CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

November 3, 2005

S. 1408
Identity Theft Protection Act

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005

SUMMARY

S. 1408 would require private companies to take certain precautions to safeguard the personal information of consumers and to notify consumers whenever there is a breach in the security of their personal information. Under the bill, consumers would have the option to freeze their credit reports in the event of a threat on their personal information. The bill also would restrict the use, display, and sale of Social Security numbers (SSNs). Under S. 1408, the Federal Trade Commission (FTC) would enforce these restrictions and requirements. Assuming appropriation of the amounts specifically authorized in the bill, CBO estimates that implementing S. 1408 would cost $1 million in 2006 and $5 million over the 2006-2010 period.

Enacting S. 1408 could increase federal revenues and direct spending as a result of the collection of additional civil and criminal penalties assessed for violations of identity theft laws. Collections of criminal penalties are recorded in the budget as revenues, deposited in the Crime Victims Fund, and later spent. CBO estimates, however, that any additional revenues and direct spending that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

S. 1408 contains several intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), including limitations on the sale, display, and use of SSNs by state and local governments, requirements that schools—many of which are public—comply with FTC regulations regarding certain personal information that they collect, and explicit preemptions of state laws regarding the treatment of that information. While the aggregate cost of complying with those mandates is uncertain, CBO estimates that such costs would exceed the threshold established in UMRA ($62 million in 2005, adjusted annually for inflation) in at least one of the first five years after the mandates go into effect.

S. 1408 would impose private-sector mandates on employers, retailers, schools, colleges, consumer-credit-reporting agencies, and other entities that acquire, maintain, or utilize sensitive personal information. While CBO cannot estimate the direct cost of complying with each mandate, certain mandates in the bill would impose security standards and notification requirements on a large number of private-sector entities, including more than five million employers. Based on this information, CBO estimates that the total direct cost of mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($123 million in 2005, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 1408 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit). CBO assumes that the bill will be enacted in calendar year 2006 and that the specified amounts will be appropriated for each year. CBO estimates that implementing the bill would cost $1 million in 2006 and $5 million over the 2006-2010 period to issue regulations and enforce the bill's new provisions restricting the use of personal information.

	By Fiscal Year, in Millions of Dollars				
	2006	2007	2008	2009	2010
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization Level	1	1	1	1	1
Estimated Outlays	1	1	1	1	1

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1408 contains several intergovernmental mandates as defined in UMRA. Specifically, the bill would:

- Limit the sale, display, and use of Social Security numbers by state, local, and tribal governments;

- Require that educational entities—many of which are public—comply with FTC regulations regarding the treatment of certain personal information that they collect;

- Explicitly preempt state laws in at least 17 states regarding the treatment of personal information; and

- Place certain notification requirements on state insurance authorities and State Attorneys General.

While there are a very large number of entities that would be required to make changes to existing systems, the aggregate cost of complying with those mandates is uncertain. Based on discussions with state and local officials, however, CBO estimates that the costs of complying with the mandates in the bill would exceed the threshold established in UMRA ($62 million in 2005, adjusted annually for inflation) in at least one of the first five years after the mandates go into effect.

CBO estimates that the prohibitions against the sale, display, and use of Social Security numbers and the requirements on educational entities would impose the most significant costs on state and local governments. The remainder of this analysis focuses on those provisions.

Social Security Numbers

While state and local governments have, in recent years, taken steps to reduce the use of SSNs on public documents, many continue to use them for a variety of purposes. The bill would restrict or prohibit governmental agencies from:

- Selling or displaying Social Security numbers that have been disclosed to the agency because of a mandatory requirement;

- Displaying SSNs on checks or check stubs;

- Placing SSNs on drivers licenses, identification cards, vehicle registrations, or employee identification cards, or coding them into magnetic strips or bar codes on those documents; and

- Allowing prisoners access to SSNs of other individuals.

The bill would allow SSNs to be sold under certain circumstances, for example, when such sale is necessary for public health, national security, or tax-law purposes, when done in compliance with certain motor vehicle laws, or consumer-reporting practices, or for nonmarket research that advances the public good.

If state and local governments do not currently have a system in place to safeguard SSNs, they would have to implement a new system for any documents issued after the regulations become effective (up to one year following enactment of the bill). If they use SSNs on checks and check-stubs as part of their recordkeeping and tracking procedures, they would have to alter those systems and remove the SSNs. Under the provisions of the bill, states would have to implement systems for removing SSNs from many documents that are available to the public. While there is some uncertainty about the extent of the requirements in this provision, CBO assumes that governmental entities would be required to remove SSNs from existing documents, a requirement that would impose significant costs on state and local governments. Further, some states may have to alter their systems for issuing driver's licenses and vehicle registrations to remove SSNs that are coded electronically onto a magnetic strip or digitized as part of a bar code. Finally, any government agency that uses SSNs would have to implement safeguards to preclude unauthorized access to SSNs and their derivatives and to protect confidentiality.

Generally, the use of SSNs by municipal governments for recordkeeping and identification is not widespread. There are over 75,000 municipal governments, however, so even small one-time costs—for example, as little as $5,000—would impose significant costs, in the aggregate, on intergovernmental entities. On the other hand, counties and states, while fewer in number (there are about 3,600 counties in the U.S.), are more dependent on SSNs for various recordkeeping and identification purposes and are thus likely to face significantly higher costs because of the complexity and scope of their recordkeeping systems. (Some counties estimate that altering their systems to use identifiers other than SSNs or to eliminate the display of SSNs would result in one-time costs ranging from $40,000 to over $1,000,000, depending on the county and the scope of the changes that would need to be made.) In total, compliance costs for all state and local entities would likely be significant.

Requirements on Schools

The bill would require elementary, secondary, and post-secondary educational institutions to:

- Develop, implement, and maintain a written program to safeguard certain personal information in accordance with FTC regulations;
- Notify affected individuals of any breach of security; and
- Refrain from using Social Security numbers as identifiers in certain circumstances.

Under current law, educational institutions that receive federal funds already are required to safeguard certain personal information and must comply with Department of Education standards. Depending on the differences between the rules promulgated by the FTC and those already required by the Department of Education, educational institutions may have to make changes to their current systems that could be costly. For example, if institutions are required to add additional systems or provide additional information, they could face added costs. Since there are over 100,000 institutions that would be affected by these changes, the total costs could be significant.

A provision that would require schools to notify affected individuals of any breach of security in which personal information may have been compromised also could be costly. The bill would cap costs for each notification to $250,000. Examples from California—where a similar law was passed in 2002—suggest that a large university could expect to incur costs of between $100,000 and $200,000 to notify individuals whose personal information may have been compromised. The California experience suggests that, because the definition of a security breach is broad, public schools likely would incur some costs to comply with this provision. Because there is a large number of educational institutions nationwide (there are over 14,000 school districts composed of about 100,000 schools and over 1,500 public institutions of higher education), total costs could be significant over time. However, CBO cannot estimate the likely frequency of such security breaches and thus cannot estimate the total costs of complying with this provision.

The bill also would prohibit educational institutions from requesting and using a Social Security number unless no other type of identifier can be used in its place. Reprograming systems that currently use SSNs as identifiers also could be costly.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1408 would impose private-sector mandates on employers, retailers, schools, colleges, consumer-credit-reporting agencies, and other entities that acquire, maintain, or utilize sensitive personal information. The legislation defines sensitive personal information as a combination of name and Social Security number, driver's license number, or credit card information. While CBO cannot determine the direct cost of complying with each mandate, certain mandates in S. 1408 would impose security standards and notification requirements on a large number of private-sector entities, including more than five million employers. Based on this information, CBO estimates that the total direct cost of mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($123 million in 2005, adjusted annually for inflation).

Security Program for the Protection of Sensitive Information

Section 2 would require covered entities to develop, implement, maintain, and enforce a written program containing administrative, technical, and physical safeguards to secure sensitive personal information. In the bill, covered entities would include businesses, employers, and educational and nonprofit institutions that acquire, maintain, and utilize sensitive personal information. The cost of this mandate depends on both the number of covered entities—more than five million—and the average cost to an entity of complying with the mandate. CBO does not have enough information to estimate the average cost to a covered entity to comply with the mandate. Because of the large number of covered entities, however, we expect that even if the average cost of writing the security program was small, the overall costs of this mandate could be significantly above the threshold established in UMRA.

Notification of Security Breach Risk

The bill would set certain procedures for notifying consumers, the FTC, and credit reporting agencies of security breaches involving personal information. In the case of a security breach, section 3(c) would require covered entities to investigate any suspected breach of security. If the breach creates a reasonable risk of identity theft, the entity would be required to notify all those individuals whose personal information was compromised and to notify the FTC and the credit-reporting agencies if the breach affects 1,000 or more individuals.

The cost of this mandate depends on the number of security breaches that occur, the average number of persons affected by a breach, and the cost per person of notification. There is very little information available on the number of breaches each year; only the largest of breaches are noticed and recorded. Nevertheless, information that is available suggests that security breaches are not rare. Although the cost to notify one person by mail may cost up to $2, the potentially large number of people in data systems maintained by some covered entities would make the cost of notification associated with one breach substantial. Furthermore, certain covered entities, such as retailers, do not maintain the mailing addresses of customers for whom they have name and credit card information. It would be costly for those entities to begin keeping that information. Based on this information, CBO expects that the cost to comply with this mandate could be large relative to UMRA's threshold for private-sector mandates.

Security Freeze

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 an authorization from the consumer. The agency also would be required to notify all other reporting agencies of the security freeze at the consumer's request. To comply with the mandates in section 4, credit-reporting agencies would have to create and operate new systems to accept, impose, and release freezes on credit reports. Further, such agencies would incur costs in terms of the lost net income from being unable to sell credit reports that they would otherwise be able to sell under current law. CBO does not have sufficient information on how such systems would be added to existing operating systems or the expected revenue from credit report sales. Therefore, CBO has no basis to determine the cost of this mandate.

Social Security Number Protection

Section 8 would prevent covered entities from soliciting any Social Security numbers from individuals unless no other identifier can be used reasonably. There are many cases in which covered entities ask individuals for their Social Security numbers. For example, employers ask their employees to provide SSNs for the purpose of sending withheld taxes to the Internal Revenue Service; in this case, no other identifier would seem possible to use. Schools, on the other hand, ask students to provide SSNs on their applications where it may be possible to use another identifier. CBO does not have sufficient information about how often covered entities could use another identifier and, if so, how much it would cost for them to switch; therefore, CBO has no basis to estimate the cost of this mandate.

This section also would prevent covered entities from displaying Social Security numbers, or any part of such a number, on any card or tag used for identification, such as student or employee identification cards. This is an increasingly rare practice; therefore, CBO estimates that the cost of this mandate would be small.

ESTIMATE PREPARED BY:

Federal Costs: Melissa Z. Petersen
Impact on State, Local, and Tribal Governments: Sarah Puro
Impact on the Private Sector: Selena Caldera and Nabeel Alsalam

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis