CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

April 6, 2006

H.R. 4127
Data Accountability and Trust Act (DATA)

As ordered reported by the House Committee on Energy and Commerce on March 29, 2006, with a subsequent amendment provided by the Committee on April 4, 2006

SUMMARY

H.R. 4127 would require private companies with access to consumers' personal information to take certain precautions to safeguard that information. Under the bill, private companies would be required to notify consumers and the Federal Trade Commission (FTC) whenever there is a breach in the security of a consumer's personal information. The bill also would require companies that maintain databases containing individuals' personal information to supply individuals with their personal electronic records upon request and to provide a means to correct mistakes in those records. The FTC would enforce the restrictions and requirements included in H.R. 4127 and create regulations related to the security of consumers' personal information. Assuming appropriation of the amounts specifically authorized in the bill, CBO estimates that implementing H.R. 4127 would cost less than $500,000 in 2006 and a total of $5 million over the 2006-2011 period.

Enacting H.R. 4127 could increase federal revenues as a result of the collection of additional civil penalties assessed for violations of laws related to information security. Collections of civil penalties are recorded in the budget as revenues. 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. Enacting the bill would not affect direct spending.

H.R. 4127 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates costs to state, local, and tribal governments, if any, would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 4127 would impose several private-sector mandates as defined in UMRA. It would require certain businesses and individuals engaged in interstate commerce to implement information security programs and notify individuals in the event of a security breach. It would also place new requirements on information brokers. While CBO cannot estimate the direct cost of complying with each mandate, H.R. 4127 would impose security requirements and notification procedures and practices on millions of private-sector entities. Based on information from industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 4127 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit). For this estimate, CBO assumes that the bill will be enacted before the end of 2006 and that the specified amounts will be appropriated for each year. CBO estimates that implementing H.R. 4127 would cost less than $500,000 in 2006 and about $5 million over the 2006-2011 period for the FTC to issue regulations and enforce the bill's provisions regarding the security of consumers' personal information. Enacting the legislation would not have a significant effect on revenues and would not affect direct spending.

	By Fiscal Year, in Millions of Dollars					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Authorization Level	1	1	1	1	1	0
Estimated Outlays	*	1	1	1	1	1

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 4127 contains intergovernmental mandates as defined in UMRA. Provisions in section 4 would require State Attorneys General to notify the FTC of any action taken under the bill, allow the FTC to intervene in those actions, and limit the actions that Attorneys General may take in certain circumstances. Also, provisions in section 6 would preempt state laws in about 20 states regarding the protection and use of certain personal data. Those provisions constitute intergovernmental mandates as defined in UMRA. CBO estimates that the

aggregate costs, if any, to state, local, and tribal governments of complying with the mandates in the bill would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

CBO assumes that the bill would grant no new authority to the FTC to regulate the activities of state and local governments. Under current law, the courts have ruled that the FTC does not have jurisdiction over those governments or over public universities. The provisions of the bill creating requirements to comply with FTC regulations regarding the handling of certain data, therefore, would not apply to such entities.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 4127 would impose several private-sector mandates as defined in UMRA. It would require certain businesses and individuals engaged in interstate commerce to implement information security programs and notify individuals in the event of a security breach. It also would place new requirements on information brokers. While CBO cannot estimate the direct cost of complying with each mandate, H.R. 4127 would impose security requirements and notification procedures and practices on millions of private-sector entities. Based on information from industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

Requirements for Information Security and Security Breach Notification

Section 2 would require certain businesses and individuals engaged in interstate commerce that own or possess personal information in electronic form, or that contract a third party to maintain such data, to establish and implement information security practices in compliance with regulations to be set by the FTC.

Such entities would be required to implement information security requirements that take into consideration the nature of the activities in which the entity takes part, available technology, and the cost of implementing the program. Those entities would also have to conduct periodic vulnerability testing on their programs. Additionally, those entities would have to identify an officer responsible for the oversight of the information security program. Moreover, entities may have to implement a process for disposing of obsolete data in electronic form. Some entities could be determined to be in compliance with section 2 by the FTC if those entities are currently in compliance with other federal regulations to maintain standards and safeguards for information security.

Section 3 would require those private entities to notify each U.S. citizen or resident following the discovery of a security breach in which the individual's personal information was acquired by an unauthorized person, as well as to notify the FTC. In addition, the entities would have to provide the credit reports to individuals affected by a breach at no cost to the individual, if requested, as well as a toll-free phone number by which the individual can reach the entity.

Section 3 would allow certain types of substitute notification if the private entities own or possess personal information on less than 1,000 individuals and direct notification is not feasible due to excessive cost to the entities or a lack of contact information for the individuals. Section 3 also would allow an entity to be exempt from notification requirements, however, if it determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. An allowable presumption that no risk of identity theft or fraud exists includes encryption or similar modification of data so that it is rendered unreadable.

The cost of those mandates depends on several factors. If additional security measures are implemented by the entities covered under this bill, the number of security breaches would tend to be lower over time. Conversely, if a large number of security breaches continue to occur in spite of the requirements of the information security program, entities would be required to send a large number of notifications to individuals. According to industry sources, in 2005, more than 57 million individuals' personal information was stolen or accessed in security breaches, none of which was encrypted. If private entities would be required to notify a comparative number of individuals, the notification requirements would be costly to those entities.

The mandates in section 2 and section 3 would extend to millions of private entities that use or maintain personal information. CBO estimates that even though per-entity costs of implementing the information security program or providing notification of a security breach required under the bill could be small, the aggregate cost of mandates in those sections would exceed UMRA's annual threshold in at least one of the first five years that the mandates are in effect.

Requirements for Information Brokers

Section 2 would require information brokers to disclose all personal information to individuals if requested by the individual at no cost to the individual. Additionally, if any incorrect information is contained in the information brokers' records, they would be required to change the information or provide the individual with contact information for the source from which the information broker obtained the individual's information. An information broker is defined in the bill as a commercial entity whose business is to collect, assemble, or

maintain personal information concerning individuals who are not current or former customers of such entity in order to sell or provide access to such information to any nonaffiliated third party.

The cost to information brokers of providing individuals with their personal information at no cost and having to change individuals' information could be large. Some evidence exists that many individuals' personally identifiable information housed at large information brokerage firms is in part incorrect. If a large number of individuals request data changes, CBO estimates that the time and notification costs to information brokers could be high.

Section 2 would further require information brokers to maintain an audit log of internal and external access to, or transmission of, any data in electronic form containing personal information. It would further require information brokers to submit to an audit by the FTC in the event of a security breach or if requested by the commission. CBO does not have sufficient information about industry practices to estimate the cost of this provision on the private sector.

PREVIOUS CBO ESTIMATES

CBO has provided estimates for three bills that address the security, handling, and use of certain personally identifying or sensitive data, all of which would require private companies to take certain precautions to safeguard the personal information of consumers. None of the bills would have a significant impact on direct spending or revenues. Each bill would impose private-sector mandates that exceed the threshold in UMRA ($128 million in 2006, adjusted annually for inflation) and include intergovernmental mandates as defined in UMRA; all would preempt state and local laws. The bills we have previously reviewed are:

- H.R. 3997, the Financial Data Protection Act of 2006, as ordered reported by the House Committee on Financial Services on March 16, 2006. CBO transmitted a cost estimate for this bill on March 30, 2006. H.R. 3997 includes a provision to allow consumers to place a security freeze on their credit report.

- S. 1326, the Notification of Risk to Personal Data Act, as reported by the Senate Committee on the Judiciary on October 20, 2005. CBO transmitted a cost estimate for this bill on March 10, 2006. In addition to requirements on private-sector companies, S. 1326 would require government agencies at the federal, state, and local level to take certain precautions to safeguard the personal information that they possess. S. 1326 contains intergovernmental mandates that exceed the threshold in UMRA ($64 million in 2006, adjusted annually for inflation).

- S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005. CBO transmitted a cost estimate for this bill on November 3, 2005. S. 1408 includes a provision to allow consumers to place a security freeze on their credit report. The bill also contains intergovernmental mandates that would exceed the threshold in UMRA ($64 million in 2006, adjusted annually for inflation).

ESTIMATE PREPARED BY:

Federal Costs: Melissa Z. Petersen
Impact on State, Local, and Tribal Governments: Sarah Puro
Impact on the Private Sector: Tyler Kruzich

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis