CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

December 7, 2009

H.R. 2221
Data Accountability and Trust Act

As ordered reported by the House Committee on Energy and Commerce on September 30, 2009

SUMMARY

H.R. 2221 would establish new requirements to protect the personal information of individuals that is collected and maintained by commercial entities. The bill would require companies to adopt procedures to protect personal information from improper access, anticipate and mitigate potential vulnerabilities in security systems intended to prevent improper access, and specify methods for disposing of data that is held in electronic and nonelectronic form. H.R. 2221 would require data brokers (entities that collect and maintain personal information for sale to others) to submit their data security policies to the Federal Trade Commission (FTC) and to establish procedures that consumers may follow to review and, if necessary, dispute the accuracy of their personal data. Finally, the bill would require entities covered by the bill to notify individuals when their personal information has been improperly accessed as the result of a breach of security. H.R. 2221 would require the FTC to develop regulations to implement and enforce the new requirements.

Assuming appropriation of the authorized amounts, CBO estimates that implementing H.R. 2221 would cost $5 million over the 2010-2014 period to develop and enforce the new regulations. Enacting H.R. 2221 could increase federal revenues from additional civil penalties assessed for violations of laws related to information security. CBO estimates that any additional revenues would not be significant because of the relatively small number of cases expected to be involved. Enacting H.R. 2221 would not affect direct spending.

H.R. 2221 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that those mandates would impose no costs on state, local, or tribal governments.

H.R. 2221 would impose several private-sector mandates as defined in UMRA by requiring certain entities engaged in interstate commerce to establish policies and procedures to keep personal information secure and to notify affected individuals in the event of a security breach. The bill also would impose new requirements on information brokers related to data collection and accuracy.

Much of the industry already complies in large part with the many of the bill's requirements. However, some of the requirements in the bill would impose new security standards and notification procedures on millions of entities in the private sector. Based on this information, 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 ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 2221 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					
	2010	2011	2012	2013	2014	2010-2014
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Authorization Level	1	1	1	1	1	5
Estimated Outlays	1	1	1	1	1	5

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted early in calendar year 2010 and that the $1 million authorized to be appropriated for each of fiscal years 2010 through 2015 will be provided for each year. CBO estimates that implementing H.R. 2221 would cost $5 million over the 2010-2014 period for the FTC to issue regulations and enforce the bill’s provisions. Enacting the legislation would not have a significant effect on revenues and would not affect direct spending.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 2221 contains intergovernmental mandates as defined in UMRA. It would preempt state and local laws that require entities that experience security breaches to notify persons whose information is comprised. The bill also would preempt state and local laws that require entities to implement security practices for handling personal information. CBO estimates that because the preemptions would only limit the application of state law, the mandate would impose no costs on state, local, or tribal governments.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 2221 would impose several private-sector mandates as defined in UMRA. It would require entities engaged in interstate commerce that own or possess personal information to implement policies and procedures to keep personal information secure, and to notify individuals when their personal information has been compromised as a result of a security breach. The bill also would require information brokers to establish procedures to verify the accuracy of the data they maintain on individuals and allow those individuals to review and correct their files.

Much of the industry already complies in large part with the many of the bill's requirements. However, this legislation would impose new information security requirements and notification procedures and practices on millions of private-sector entities. It also would broaden the definition of “personal information” and expand the circumstances under which businesses must notify individuals of a breach of their information as compared to current law. Based on information from the FTC and industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

Requirements for Information Security

Section 2 of the bill would require certain entities that own or possess personal information, that are engaged in interstate commerce, or that contract a third party to maintain such data, to establish and implement information security policies and procedures in compliance with regulations to be set by the FTC. Personal information, as defined in the bill, is an individual’s first name or initial and last name, or address, or phone number, in combination with any one or more of the following: the individual’s social security number, driver’s license number, passport number or similar identification number issued on a government document, or a financial account number or credit card number and any security or access code needed to access the account.

Covered entities would have to implement a security policy with respect to the use, sale, dissemination, and maintenance of data and conduct periodic vulnerability testing on their security programs. Additionally, those entities would have to identify an officer responsible for the oversight of the information security. Entities also would have to implement a process for disposing of obsolete electronic and non-electronic data containing personal information. Some businesses could be determined by the FTC to be in compliance with the requirements of section 2 if they are currently in compliance similar federal regulations to maintain standards and safeguards for information security.

The cost of compliance for the data privacy and security requirements would depend on the rules to be established by the FTC, the size of the entity, and the amount of personal information maintained by the entity. Most businesses are already subject to state or other federal laws regulating security policies, and it is the current practice of many businesses to use security measures to protect sensitive data. However, state laws generally use a more narrow definition of personal information than would apply under the bill. The bill's requirements would apply to varying degrees to millions businesses who own, use, or maintain personal information. Even though the incremental cost per entity of implementing the information security requirements in the bill could be small, the aggregate cost of compliance could be substantial.

Notification of Information Security Breach

Section 3 would require a covered entity that owns or possesses data in electronic form containing personal information to notify individuals and the FTC following a security breach in which such individuals' personal information was accessed or acquired by an unauthorized person. The bill also includes special notification requirements for third party agents and internet service providers.

Notification would have to be written or, in some circumstances, could be sent via email. The bill allows for substitute notification, through postings on the entity's Web site and in print and broadcast media, when the person experiencing the breach owns or possesses the data of fewer than 1,000 individuals, or when direct notification is not feasible due to excessive cost or if the contact information for the individuals is unavailable. Both forms of notification would have to include a description of the information accessed or acquired, certain relevant telephone contact numbers, and notice of the right to receive free credit monitoring services or quarterly credit reports for two years following the breach. Entities would have to provide credit reports or credit monitoring services to individuals affected by a breach at no cost to the individual, if requested.

If the breached personal information consists of an individual's name, address, or phone number in combination with a credit or debit card number and the required security code, under the legislation, breach notification would not be required. The bill also would allow an entity to be exempt from notification requirements, 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.

Should entities choose to reduce the likelihood of a data breach by encrypting personal information, the total cost could be substantial. Data encryption software can cost between $150 and $600 or more depending on the type of system used and the amount of data. If even a small portion of the millions of entities affected by this bill were to purchase this software, those costs could exceed the annual threshold.

In 2006, more than 17 million people's social security numbers were stolen or accessed in security breaches, none of which was encrypted. Since 2006, the number of individuals who have had their information accessed illegally has risen. This legislation would elevate other personally identifying information (such as driver's license numbers and passport IDs) to the level of a social security number for the purposes of data breach notification. Therefore, the number of individuals who would have to be notified about a breach could increase under the bill.

The majority of states already have data breach security laws in place; however those laws do not include provisions for mandatory credit monitoring services. The cost of bulk purchases of the credit monitoring services is approximately $60 per person, per year, according to credit industry professionals. Historically, there has been an acceptance rate of such services of about 6 percent to 8 percent. If the large number of security breaches continues, in spite of the requirements for information security programs and encryption, the cost of the notification requirements could be significant.

Special Requirements for Information Brokers

Security Systems Audit. Information Brokers (companies whose business is to collect, assemble, maintain and sell information about individuals who are not their customers) would be required to submit their information-security policies to the FTC for review upon request or accompanying notification of breach of security. As a part of their information security requirements, following a breach in security, information brokers would be required to allow the FTC to conduct a post-breach audit of their security systems, or to have an independent auditor brought in to review the system.

According to industry experts, the cost of a security audit can range from $10,000 to more than $100,000 depending on the thoroughness of the audit and the type of systems being tested. Only 26 audits were required by the FTC between 2001 and 2009. However, the scope of what constitutes a breach could be broadened under the bill, so the number of audits may increase upon enactment of this legislation.

Maintaining the Accuracy of Information. Information brokers would also be required to establish accuracy standards for the personal information they broker. The bill would require information brokers annually to provide individuals with their personal information at no cost. The individual would then have to be given the right to dispute any information held by the broker. If that information is found to be incorrect, information brokers who do not use their data for marketing purposes would be obliged to correct the inaccuracy and, in certain cases, to provide the individual with the source of the data. Information brokers who do use data for marketing purposes would be required to allow individuals to decide how their information should be used.

The cost of providing records upon request depends on the costs of gathering and distributing the information to individuals and the number of individuals requesting their information. According to information from industry sources some information brokers already correct information based on requests from individuals. Industry experts also indicate that the average cost to large information brokers that currently provide this service is about $8.50 each time a record is disclosed and information is disputed by an individual. However, the cost per record may be higher for information brokers who do not currently have systems in place to handle such disputes. Some evidence exists that many individuals' personal information housed at data brokerage firms is in part incorrect.

There were 12 million disputes that lead to investigations in 2006 and providing the means to access and dispute personal information annually could reasonably lead to an increase in the number of requests. The cost would be the incremental cost incurred by brokers as a consequence of an increase in dispute requests. According to industry leaders, there were around 30 data aggregators and 600 to 700 information brokers nationwide in 2006. Those information brokers that do not currently have the capability to resolve disputes would incur a significant cost for establishing the means to comply with this provision.

The bill would also 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. 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 personal information would be a significant enhancement of data management hardware and software for the majority of business entities. The aggregate cost of implementing such changes could be substantial.

PREVIOUS CBO ESTIMATE

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. H.R. 2221 and S. 1490 are concerned with the security of sensitive personal information and notification requirements in the event such information is disclosed to unauthorized entities. CBO estimates that implementing the provisions of S. 1490 that would require agencies to assess the security of sensitive personal information held by the government and to report to the Congress on those assessments would cost $25 million over the 2010-2014 period.

CBO determined that both H.R. 2221 and S. 1490 contain intergovernmental mandates, that would not exceed the threshold established in UMRA ($69 million in 2009, adjusted for inflation). In addition, CBO determined that both bills contain private-sector mandates that would exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, adjusted annually for inflation).

ESTIMATE PREPARED BY:

Federal Costs: Susan Willie
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