CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

September 29, 2016

H.R. 2205
Data Security Act of 2015

As ordered reported by the House Committee on Financial Services on December 9, 2015

H.R. 2205 would establish a new law to require businesses to take reasonable steps to protect personal information they maintain in electronic form. Further, H.R. 2205 would require those entities, in the event of a breach in their security systems, to notify individuals whose personal information has been accessed and acquired as a result of the breach. Forty-seven states have laws that govern data security; H.R. 2205 would pre-empt many of those statutes. Finally, H.R. 2205 would require the Federal Trade Commission (FTC) and many of the financial regulatory agencies to enforce the requirements of the bill.

Federal Budgetary Effects

CBO estimates that implementing H.R. 2205 would cost the FTC, the Securities and Exchange Commission, and the Commodity Futures Trading Commission about $2 million over the 2016-2021 period, assuming appropriation of the necessary amounts. CBO expects those agencies would hire additional staff, at a cost of less than $500,000 per year, on average, to carry out the new regulatory requirements because current laws that cover the businesses regulated by those agencies do not address all of the data security issues covered by H.R. 2205.

H.R. 2205 also would require the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the National Credit Union Administration, and the Federal Reserve to ensure compliance with the requirements of the bill for the depository institutions that they regulate. The costs to those regulators would be recorded in the federal budget as increases in direct spending (or as a reduction in revenues, in the case of the Federal Reserve). As a result, pay-as-you-go procedures apply to the bill. However, because provisions of the bill would deem compliance with current laws that apply to depository institutions as complying with the provisions of H.R. 2205, CBO estimates that under the bill the additional costs for those regulators would be negligible.

CBO estimates that enacting H.R. 2205 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

Intergovernmental Mandates

H.R. 2205 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) because it would explicitly preempt laws in at least 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands that require businesses to notify individuals in the event of a security breach. The bill also would preempt laws in at least 12 states that have enacted data security laws. Finally, the bill 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 compliance costs would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($77 million in 2016, adjusted annually for inflation).

Private-Sector Mandates

H.R. 2205 also contains private-sector mandates as defined in UMRA because it would impose information security and notification requirements on businesses and other entities that use or handle personal information. Specifically, the bill would require businesses and other entities to:

- Protect sensitive financial and personal information from unauthorized access by implementing and maintaining security measures that comply with the standards outlined in the bill (for example, entities would be required to designate an employee to coordinate their security programs, to periodically conduct vulnerability assessments and to adjust security programs based on those assessments); and

- Notify affected consumers, certain federal or state authorities, each consumer reporting agency, and any payment card network as appropriate whenever sensitive personal information has been compromised as a result of a breach.

In addition the bill would require:

- Businesses that have a board of directors to produce a written information security program and to report to the board annually on that status of the program; and

- Third-party service providers and Internet service providers that handle personal information on behalf of a business to notify the affected business in the event of a breach.

Entities already in compliance with the requirements under Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, or the Health Information

Technology for Economic and Clinical Health Act would be deemed to be in compliance with the bill's provisions.

The net cost of the mandates would equal the additional costs incurred, offset by any savings associated with complying with the bill's requirements. Most businesses already notify consumers in the event of a breach, so CBO expects that the bill's notification requirements would not have a substantial cost. Many of those businesses would experience a savings, because the bill would establish a uniform national standard that would preempt state laws, some of which are more stringent than the notification requirements proposed by the bill. In addition, some costs of the mandate may be mitigated because most businesses already employ data security measures and the bill would allow covered entities some flexibility to adopt security measures that are appropriate for their size, nature, and complexity of operations. However, millions of entities in the private sector may need to implement new or enhanced security measures if the bill is enacted, so that even a relatively low incremental cost per firm could amount to substantial costs in total. Consequently, CBO estimates that, in aggregate, the net cost to comply with the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($154 million in 2016, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

The CBO staff contacts for this estimate are Kim Cawley (for federal costs), Rachel Austin (for intergovernmental mandates), and Logan Smith (for private-sector mandates). The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.