CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

April 20, 2015

H.R. 1770
Data Security and Breach Notification Act of 2015

As ordered reported by the House Committee on Energy and Commerce on April 15, 2015

SUMMARY

H.R. 1770 would establish a new law to require businesses to take reasonable steps to protect personal information they maintain in electronic form. Further, H.R. 1770 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. 1770 would pre-empt many of those statutes. The bill would direct the Federal Trade Commission (FTC) to enforce the rules and authorize the agency to collect civil penalties if those rules are violated.

CBO estimates that implementing H.R. 1770 would cost $1 million over the 2015-2020 period, assuming appropriation of the necessary amounts. In addition, CBO estimates that enacting the bill would increase revenues by $9 million over the 2015-2025 period from the collection of civil penalties; therefore pay-as-you-go procedures would apply. Enacting H.R. 1770 would not affect direct spending.

H.R. 1770 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the mandates would be small and would not exceed the threshold established in UMRA ($77 million in 2015, adjusted annually for inflation).

H.R. 1770 would impose private-sector mandates as defined in UMRA on businesses and non-profits that possess or manage sensitive personal information and on Internet service providers (ISPs). Because most of those businesses already comply with similar requirements in state laws, CBO estimates that the incremental cost to comply with the mandates in the bill would probably fall below the annual threshold established in UMRA for private-sector mandates ($154 million in 2015, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary effect of H.R. 1770 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											
	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2016-2020	2016-2025
CHANGES IN REVENUES												
Estimated Revenues	*	1	1	1	1	1	1	1	1	1	4	9

Notes: * = less than $500,000.

CBO estimates that implementing H.R. 1770 would cost $1 million over the 2015-2020 period, assuming appropriation of the necessary amounts.

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted near the end of fiscal year 2015, that the necessary amounts will be appropriated each year, and that spending will follow historical patterns for similar activities.

Spending Subject to Appropriation

H.R. 1770 would direct the FTC to enforce new federal regulations that would require certain businesses and nonprofits to:

- Establish security measures to protect personal information maintained in electronic form, and

- Notify individuals if a breach of security measures creates a reasonable risk that they would be exposed to identity theft or economic harm because of the breach.

Based on information from the FTC, CBO estimates that implementing H.R. 1770 would cost about $1 million over the 2015-2020 period, assuming appropriation of the necessary amounts. CBO expects the agency would hire 2 additional staff, at a cost of $260,000 per year, on average, to carry out the new regulatory requirements.

Revenues

Under current law, the FTC has authority under the Federal Trade Commission Act to bring enforcement actions against companies for deceptive and unfair practices that can involve consumers' privacy and personal information. However, the FTC can currently assess civil monetary penalties as part of those actions only in certain privacy related cases, such as for violations of rules established by the Children's Online Privacy Protection Act and the Fair Credit Reporting Act.

Under H.R. 1770, the FTC could assess civil penalties in a broader set of privacy related cases. Based on information provided by the FTC, CBO estimates that enacting H.R. 1770 would increase revenues from civil penalties by about $1 million per year and by $9 million over the 2016-2025 period. Those payments of civil penalties would come primarily from covered entities that violate requirements to implement and maintain reasonable security measures to protect personal information.

PAY-AS-YOU-GO CONSIDERATIONS

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. The net changes revenues that are subject to those pay-as-you-go procedures are shown in the following table.

CBO Estimate of Pay-As-You-Go Effects for H.R. 1770, as ordered reported by the House Committee on Energy and Commerce on April 15, 2015

	By Fiscal Year, in Millions of Dollars												
	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2015-2020	2015-2025
	NET DECREASE (-) IN THE DEFICIT												
Statutory Pay-As-You-Go Impact	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-4	-9

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 1770 contains intergovernmental mandates as defined in UMRA. The bill 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 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 the costs of the mandates would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($77 million in 2015, adjusted annually for inflation).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 1770 would impose private-sector mandates as defined in UMRA on businesses and non-profits that possess or manage sensitive personal information and on ISPs. Because most of those businesses already comply with similar requirements in state laws, CBO estimates that the incremental cost to comply with the mandates in the bill would probably fall below the annual threshold established in UMRA for private-sector mandates ($154 million in 2015, adjusted annually for inflation).

Requirements for Information Security

The bill would require businesses to implement and maintain reasonable security measures to protect personal information maintained in electronic form from unauthorized access. The bill stipulates that such security measures must be appropriate for the size, complexity, and general nature and scope of the activities of the business entity. According to the FTC, it is already enforcing such requirements for businesses covered under the Federal Trade Commission Act. Other businesses covered by the bill that are not currently under FTC's jurisdiction, including telecommunications carriers and non-profits, are currently subject to similar enforcement by the FCC or applicable state agencies under certain state laws. As a result, CBO expects that the incremental cost to comply with this provision would be minimal.

Notification of Security Breaches

The bill would require businesses engaged in Interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personal information to notify any individuals whose information has been or may have been unlawfully accessed as a result of a breach. In the event of a breach, businesses would be required to conduct an investigation to determine if there is a reasonable risk the breach resulted in, or could result in, identity theft, economic loss or harm, or financial fraud to individuals whose personal information was compromised. Upon determining there was sufficient risk, businesses would be required to notify individuals in the United States affected by the breach using written letters, or email. Notifications would be required to include certain information about the breach, as well as toll-free numbers for the affected business, consumer reporting agencies, and the FTC. If a breach requires notification of over 10,000 individuals, businesses would have to notify consumer reporting agencies, the FTC and either the Secret Service or the Federal Bureau of Investigation.

After a business has made reasonable efforts to contact all individuals affected by a breach, and determines that the contact information of at least 500 such individuals is insufficient or out-of-date, the bill would require such businesses to attempt to contact the individuals through either email (if it was not the primary method of contact), or by posting a conspicuous notice detailing information about the breach on the business's website for at least 90 days.

The bill also would impose requirements on ISPs. Should an ISP become aware of a breach affecting personal information that is owned or licensed by a business that connects to the ISP's networks, it must notify the affected business, if the business can be reasonably identified. The ISP would have no further notification requirements upon notifying the affected business under the bill, provided their relationship with the affected business was strictly for the purpose of transmitting, routing, or providing intermediate transient storage of data.

Nearly all states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most businesses to notify individuals if a security breach occurs. Therefore, CBO expects that the incremental costs incurred by businesses to comply with the notification requirements in the bill would not be substantial.

ESTIMATE PREPARED BY:

Federal Costs: Susan Willie
Federal Revenues: Nathaniel Frentz
Impact on State, Local, and Tribal Governments: Melissa Merrell
Impact on the Private Sector: Logan Smith

ESTIMATE APPROVED BY:

Theresa Gullo
Assistant Director for Budget Analysis