AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–1097

CONSUMER INFORMATION NOTIFICATION REQUIREMENT ACT

DECEMBER 21, 2018.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. HENSARLING, from the Committee on Financial Services, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 6743]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 6743) to amend the Gramm-Leach-Bliley Act to provide a national standard for financial institution data security and breach notification on behalf of all consumers, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Consumer Information Notification Requirement Act".

SEC. 2. BREACH NOTIFICATION STANDARDS.

Section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) is amended—

(1) in subsection (b)(3) by striking the period at the end and inserting ", including through the provision of a breach notice in the event of unauthorized access that is reasonably likely to result in identity theft, fraud, or economic loss."; and

(2) by adding at the end the following:

"(c) STANDARDS WITH RESPECT TO BREACH NOTIFICATION.—Subject to section 504(a)(2) and sections 505(b) and 505(c), within 6 months after the date of enactment of this subsection, each agency or authority required to establish standards described under subsection (b)(3) with respect to the provision of a breach notice shall ensure that such standards are in compliance with subsection (b).

89–006

"(d) INSURANCE.—

"(1) ENFORCEMENT.—Notwithstanding section 505(a)(6), with respect to an entity engaged in providing insurance, the standards under subsection (b) shall be enforced—

"(A) with respect to any such standards related to data security safeguards, by—

"(i) the State insurance authority of the State in which the entity is domiciled; or

"(ii) in the case of an insurance agency or brokerage, the State insurance authority of the State in which such agency or brokerage has its principal place of business; and

"(B) with respect to any such standards related to notification of the breach of data security, by the State insurance authority of any State in which customers of the entity are affected by such a breach of data security.

"(2) NOTIFICATION BY ASSUMING INSURER.—

"(A) IN GENERAL.—Notwithstanding subsection (b), an assuming insurer that experiences a breach of data security shall only be required to notify the State insurance authority of the State in which the assuming insurer is domiciled.

"(B) ASSUMING INSURER DEFINED.—For purposes of this paragraph, the term 'assuming insurer' means an entity engaged in providing insurance that acquires an insurance obligation or risk from another entity engaged in providing insurance pursuant to a reinsurance agreement.

"(3) SAFEGUARDS FOR INSURANCE CUSTOMERS.—In carrying out subsection (b) with respect to an entity engaged in providing insurance, a State insurance authority shall establish the standards for safeguarding customer information maintained by entities engaged in activities described in section 4(k)(4)(B) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(4)(k)(4)(B)) that are the same as the standards contained in the interagency guidelines issued by the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision titled 'Interagency Guidelines Establishing Standards for Safeguarding Customer Information', published February 1, 2001 (66 Fed. Reg. 8633), and such standards shall be applied as if the entity engaged in providing insurance was a bank to the extent appropriate and practicable.".

SEC. 3. PREEMPTION WITH RESPECT TO FINANCIAL INSTITUTION SAFEGUARDS.

Section 507 of the Gramm-Leach-Bliley Act (15 U.S.C. 6807) is amended to read as follows:

"SEC. 507. RELATION TO STATE LAWS.

"(a) IN GENERAL.—This subtitle preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, with respect to a financial institution or affiliate thereof securing personal information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of data.

"(b) INSURANCE.—Subsection (a) shall not prevent a State or political subdivision of a State from establishing the standards for entities engaged in providing insurance required by sections 501(c) and 501(d), provided the standards established by such State or political subdivision do not impose any requirement that is in addition to or different from those standards, except where necessary to effectuate the purposes of this subtitle.".

PURPOSE AND SUMMARY

Introduced by Representative Blaine Luetkemeyer on September 7, 2018, H.R. 6743, the "Consumer Information Notification Requirement Act" amends the Gramm-Leach-Bliley Act (GLBA) [P.L. 106–102] to direct the federal financial regulatory agencies,[1] within six months of enactment, to establish or update a federal standard for consumer notification for covered entities in the event of unauthorized access of non-public personal information that is likely to result in identity theft, fraud, or economic loss to consumers. Covered entities include banks, credit unions, brokers, dealers, invest-

[1] Agencies includes the OCC, Federal Reserve, FDIC, NCUA, BCFP, SEC, FTC, and state insurance regulators.

ment companies, investment advisors, insurance companies, credit reporting agencies, and all other nonbank financial institutions regulated under the Federal Trade Commission's (FTC) Safeguards Rule.[2] The bill also adds explicit language that state insurance regulators have the responsibility to establish and enforce data security safeguards comparable to the 2001 *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*.[3] This bill would require the state insurance regulators to create a uniform data security and data breach standard for insurance companies.

BACKGROUND AND NEED FOR LEGISLATION

In response to competitive pressure in the financial services marketplace, as well as increased demands for convenience from consumers, financial institutions are becoming increasingly reliant on electronic storage and transmission of personal financial data. As the amount of electronically accessible data increases, so does the amount of sensitive data that is vulnerable to the risk of theft. This increased exposure to risk has also created an expectation from consumers that institutions ensure the security of personal and financial information data.

Over the last several years, numerous U.S. companies of varying sizes and from various industries have experienced major data breaches. In November and December of 2013, cybercriminals breached the data security of Target, one of the largest U.S. retail chains, stealing the personal and financial information of millions of customers. On December 19, 2013, Target confirmed that some 40 million credit and debit card account numbers had been stolen. On January 10, 2014, Target announced that personal information, including the names, addresses, phone numbers, and email addresses of up to 70 million customers, was also stolen during the data breach.[4] In September 2017, one the of three credit reporting bureaus, Equifax, announced a breach that compromised the personal and financial data of over 145 million consumers, or, nearly one-third of the U.S. population.[5] These incidents underscore the serious threats to financial privacy and data security posed by individuals and criminal syndicates—some based overseas—that seek access to personal financial data to commit fraud or identity theft.

Data breaches affect consumers in two ways. First, data breaches subject consumers to uncertainty and confusion. Consumers may lose confidence in the payments system when they hear about data breaches, even if they are not directly affected. Second, data

---

[2] The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule. Standards for Safeguarding Customer Information; Final Rule. 16 CFR § 314. 2002. Available at https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf.

[3] *See* Federal Reserve, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." (2001). Available at https://www.federalreserve.gov/boarddocs/srletters/2001/sr0115a1.pdf.

[4] Congressional Research Service, The Target and Other Financial Data Breaches: Frequently Asked Questions February 4, 2015 (R43496), N. Eric Weiss, Specialist in Financial Economics and Rena S. Miller, Specialist in Financial Economics, available at http://www.crs.gov/Reports/R43496?source=search&guid=eda354c09eb4496c9b03690e65bf5f4f&index=0.

[5] https://www.equifaxsecurity2017.com/.

breaches and the improper accessing of Personal Identifiable Information (PII) increase consumers' vulnerability to identity theft, leading to further inconvenience, potential legal issues and possible financial loss.

Protecting information and systems from major cyber threats, such as cyber theft, cyber terrorism, cyber warfare, and cyber espionage, must be a priority for Congress. Cybersecurity incidents include data breaches, in which sensitive, personal, or confidential information has potentially been viewed, stolen, or used by an individual unauthorized to do so. The financial sector is a frequent target for cyber incidents, and past incidents have shown the potential risks posed by the financial sector's interconnectedness with other major sectors of the economy.

STATE LAW GOVERNING DATA SECURITY AND DATA BREACH NOTIFICATION

Currently, only a few specific industries of the private-sector economy are required by federal law to notify consumers when a data breach may have compromised consumers' PII. These include financial institutions covered by the Gramm-Leach Bliley Act (GLBA).

Forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation to require private or governmental entities to notify individuals of security breaches of information involving PII.[6] The requirements vary by state, but most states require notification "in the most expedient time possible" or "without unreasonable delay."

Some state laws impose general data security standards as well. Seventeen states and territories permit a private right of action pertaining to data breaches or data breach notifications.

And yet, the Equifax breach has reaffirmed that data security is a national problem that requires a national solution. The patchwork of state laws that comprise the legal and regulatory data security and breach notification regime have caused both confusion and a lack of accountability as cyber criminals continue to steal valuable PII from consumers.

Data Security Standards for Financial Institutions

Despite continued data breaches, financial institutions and retailers argue that further data security legislation and regulation may be unnecessary or counterproductive. Financial institutions point out that, unlike most other sectors of the economy, they are already subject to laws and regulations that require them to safeguard confidential customer data. They also point out that they have an incentive to safeguard customer data because a data breach will damage their relationships with their customers and tarnish their brands. For these reasons, financial institutions monitor and update their security controls to reduce fraud and guard against security breaches.

As new threats develop, so to must the controls that mitigate the risks. As financial institutions are developing or reviewing their information security protocols can draw upon a variety of sources, in-

[6] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

cluding federal laws and regulations and numerous security-related guidance, in addition to several other entities that provide voluntary standards or information-gathering roles.

Financial institutions are required to institute sufficient risk management procedures to ensure their safety and soundness, and to ensure compliance with federal and state laws and regulations. The Federal Financial Institutions Examination Council (FFIEC) prescribes uniform principles, standards, and report forms for the federal examination of financial institutions and makes recommendations to promote uniformity in the supervision of financial institutions.[7] The FFIEC's members include the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Federal Reserve), the Consumer Financial Protection Bureau (BCFP), and the National Credit Union Administration (NCUA), as well as a representative state regulator.

In 2005 the FFIEC published in the *Federal Register* the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Interagency Guidance).[8] This guidance requires customer notice as the key feature of an entities response program and states:

> "every financial institution should develop and implement a response program designed to address incidents of unauthorized access to customer information maintained by the institution or its service provider. The final Guidance provides each financial institution with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations." [9]

To ensure financial institutions adhere to these principles the 2005 Interagency Guidance requires the following of breached entities:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused,
- Notifying its primary federal regulator "as soon as possible" when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information,
- Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing,
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information,
- Notifying customers when warranted and "as soon as possible", with a delay only at the directive of law enforcement agency for investigation purposes.[10]

---

[7] https://www.ffiec.gov/about.htm.
[8] https://www.gpo.gov/fdsys/pkg/FR-2005-03-29/pdf/05-5980.pdf.
[9] https://www.gpo.gov/fdsys/pkg/FR-2005-03-29/pdf/05-5980.pdf.
[10] https://www.fdic.gov/news/news/financial/2005/fil2705a.pdf.

A flexible and scalable standard guarantees that a financial institution can both notify its customers and undertake corrective action from the breached entity in the necessary and appropriate timeframes. A scalable standard does not hamper law enforcement during the course of their investigation.

Additionally the FFIEC has published an Information Security Handbook to assist examiners evaluate a financial institution's cybersecurity management.[11] The handbook provides guidance on information security risk assessment, security controls, and security monitoring. The handbook also addresses outsourced operations and requires that financial institutions exercise their security responsibilities for outsourced operations through: due diligence in selecting service providers; contractual delineation of security responsibilities, controls, and reporting; contractual provisions addressing nondisclosure of data; independent audits of the service provider's security; and coordinated incident response and notification requirements. In addition, federal statutes provide the federal financial regulators with authority to monitor third-party service providers. Banks and other covered depository institutions are examined every 12 to 18 months for compliance with the cybersecurity handbook, and may be examined more frequently at a regulator's discretion.

Title V of GLBA requires that financial institutions provide customers with notice of their privacy policies and safeguard the security and confidentiality of customer information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Section 4(k) of the Bank Holding Company Act of 1956 and accompanying regulations define financial institutions as businesses that are engaged in certain "financial activities." Such activities include traditional banking, lending, and insurance functions, along with other financial activities.

GLBA requires regulators of "financial institutions" to develop and impose upon financial institutions standards for administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. GLBA delegates enforcement and rulemaking authority to the federal banking and securities regulators and the state insurance regulators. For "financial institutions" not regulated by one of these functional regulators, the FTC imposes safeguards provided the "financial institution" is "significantly engaged in financial activities." GLBA does not set forth independent authority for the regulators. The regulators must use authority available to them under other statutes, such as their organic statutes, or, in the case of the FTC, section 5 of the Federal Trade Commission Act. There is no private right of action for failure to adhere to GLBA's privacy standards.

The federal banking agencies monitor banking companies for safety and soundness and compliance with laws and regulations by on-site examinations—at least annually and every 18 months for some community banks. Included in the examination is a comprehensive review of information technology and security. The

[11] http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

GLBA safeguards standards are integrated into the overall IT examination. In addition, since 2001, the banking agencies have issued a series of guidelines, which have the force of law, detailing how the GLBA safeguards requirements are to be put into effect. The guidelines require that financial institutions develop security programs that are tailored to the complexity of their operations. They must include board of directors' involvement; risk assessment; oversight of service providers; personnel training; systems monitoring; breach response procedures; and mitigation of incidents. Under these guidelines, when a security breach is detected, the financial institution must notify law enforcement and its supervisory agency or agencies as soon as possible; customers must be notified if a reasonable investigation shows that misuse of sensitive customer information has occurred or is reasonably possible. Measures to control the incident and mitigate its consequences must be implemented.

The security guidelines recommend implementation of a risk-based response program, including customer notification procedures, to address unauthorized access to or use of customer information maintained by a financial institution or its service provider that could result in substantial harm or inconvenience to any customer, and require disclosure of a data security breach if the covered entity concludes that "misuse of its information about a customer has occurred or is reasonably possible." Pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to "sensitive customer information."

Financial institutions must also comply with state data security breach notification laws. Retailers and merchants are not subject to GLBA or any comparable federal law. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private or government entities to provide notification of data security breaches to individuals. The requirements vary by state, but most states require notification "in the most expedient time possible" or "without unreasonable delay." Some state laws impose general data security standards.

Department of Treasury Recommendations

The United States currently does not have a national law to govern uniform notification standards. In July 2018, the Department of Treasury published a report titled the "A Financial System that Creates Economic Opportunities; Nonbank Financial, Fintech, and Innovation." The report appropriately noted the inconsistencies that a fragmented state patchwork causes by stating:

> The United States does not have a national law establishing uniform national standards for notifying consumers of data breaches, or for providing them a clear and straightforward mechanism for resolving disputes. In the absence of uniform national standards, states have been aggressive in developing their own data breach notification laws. Each state law may apply to any company located in that state or that does business with residents of that state. In practice, this means that in the event of a data breach companies could be subject to the data breach notification laws of 50 states as well as of the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands.

> State laws for data breach notification often include specific provisions regarding the number of affected individuals that will trigger notification requirements, the timing of notification, and form of notification, among other requirements. Unsurprisingly, state data breach notification laws are far from uniform. Indeed, they vary in a number of significant ways, including with respect to the most fundamental aspect, namely the scope of data covered under the definition of personal information. Other inconsistencies among states' breach notification laws can make compliance difficult for firms and entail disparate treatment for consumers. The lack of uniformity and efficiency affects both nonfinancial companies and financial institutions.[12]

The Department of Treasury recommends that Congress should enact federal standard legislation to protect consumer financial data through a technology neutral and scalable standard. H.R. 6743 responds to and fulfills the Treasury Department's recommendation.

HEARINGS

The Committee held hearings examining matters relating to H.R. 6743 on October 5 and 25, 2017, November 1, 2017, February 14, 2018, March 7, 2018, and March 15, 2018.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on September 13, 2018, and ordered H.R. 6743 to be reported favorably to the House as amended by a recorded vote of 32 yeas to 20 nays (recorded vote no. FC–208), a quorum being present. Before the motion to report was offered, the Committee adopted an amendment in the nature of a substitute offered by Mr. Luetkemeyer by voice vote. An amendment in the nature of a substitute offered by Ranking Member Waters was not agreed to by a recorded vote of 20 yeas to 32 nays (recorded vote no. FC–207).

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. An amendment in the nature of a substitute offered by Ranking Member Waters was not agreed to by a recorded vote of 20 yeas to 32 nays (recorded vote no. FC–207). A motion by Chairman Hensarling to report the bill favorably to the House as amended was agreed to by a recorded vote of 32 yeas to 20 nays (recorded vote no. FC–208), a quorum being present.

---

[12] U.S. Department of Treasury, "A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation." (Jul. 2018). Available at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities—Nonbank-Financi. . . .pdf.

Record vote no. FC-207

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Hensarling		X		Ms. Maxine Waters (CA)	X		
Mr. McHenry		X		Mrs. Carolyn B. Maloney (NY)	X		
Mr. King		X		Ms. Velázquez	X		
Mr. Royce (CA)		X		Mr. Sherman	X		
Mr. Lucas		X		Mr. Meeks			
Mr. Pearce				Mr. Capuano			
Mr. Posey		X		Mr. Clay			
Mr. Luetkemeyer		X		Mr. Lynch	X		
Mr. Huizenga		X		Mr. David Scott (GA)	X		
Mr. Duffy		X		Mr. Al Green (TX)	X		
Mr. Stivers		X		Mr. Cleaver			
Mr. Hultgren		X		Ms. Moore	X		
Mr. Ross		X		Mr. Ellison			
Mr. Pittenger				Mr. Perlmutter	X		
Mrs. Wagner		X		Mr. Himes	X		
Mr. Barr		X		Mr. Foster	X		
Mr. Rothfus		X		Mr. Kildee	X		
Mr. Messer		X		Mr. Delaney	X		
Mr. Tipton		X		Ms. Sinema	X		
Mr. Williams		X		Mrs. Beatty	X		
Mr. Poliquin		X		Mr. Heck	X		
Mrs. Love		X		Mr. Vargas	X		
Mr. Hill		X		Mr. Gottheimer			
Mr. Emmer		X		Mr. Gonzalez (TX)	X		
Mr. Zeldin		X		Mr. Crist	X		
Mr. Trott		X		Mr. Kihuen	X		
Mr. Loudermilk		X					
Mr. Mooney (WV)		X					
Mr. MacArthur		X					
Mr. Davidson		X					
Mr. Budd		X					
Mr. Kustoff (TN)		X					
Ms. Tenney		X					
Mr. Hollingsworth		X					

Record vote no. FC-208

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Hensarling	X			Ms. Maxine Waters (CA)		X	
Mr. McHenry	X			Mrs. Carolyn B. Maloney (NY)		X	
Mr. King	X			Ms. Velázquez		X	
Mr. Royce (CA)	X			Mr. Sherman		X	
Mr. Lucas	X			Mr. Meeks			
Mr. Pearce				Mr. Capuano			
Mr. Posey	X			Mr. Clay			
Mr. Luetkemeyer	X			Mr. Lynch		X	
Mr. Huizenga	X			Mr. David Scott (GA)		X	
Mr. Duffy	X			Mr. Al Green (TX)		X	
Mr. Stivers	X			Mr. Cleaver			
Mr. Hultgren	X			Ms. Moore		X	
Mr. Ross	X			Mr. Ellison			
Mr. Pittenger				Mr. Perlmutter		X	
Mrs. Wagner	X			Mr. Himes		X	
Mr. Barr	X			Mr. Foster		X	
Mr. Rothfus	X			Mr. Kildee		X	
Mr. Messer	X			Mr. Delaney		X	
Mr. Tipton	X			Ms. Sinema		X	
Mr. Williams	X			Mrs. Beatty		X	
Mr. Poliquin	X			Mr. Heck		X	
Mrs. Love	X			Mr. Vargas		X	
Mr. Hill	X			Mr. Gottheimer			
Mr. Emmer	X			Mr. Gonzalez (TX)		X	
Mr. Zeldin	X			Mr. Crist		X	
Mr. Trott	X			Mr. Kihuen		X	
Mr. Loudermilk	X						
Mr. Mooney (WV)	X						
Mr. MacArthur	X						
Mr. Davidson	X						
Mr. Budd	X						
Mr. Kustoff (TN)	X						
Ms. Tenney	X						
Mr. Hollingsworth	X						

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the findings and recommendations of the Committee based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee states that H.R. 6743 will direct the federal financial regulatory agencies to establish standards contained in the 2005 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATES

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, December 20, 2018.

Hon. JEB HENSARLING,
Chairman, Committee on Financial Services,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 6743, the Consumer Information Notification Requirement Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Stephen Rabent.

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 6743—Consumer Information Notification Requirement Act

H.R. 6743 would require several federal agencies to establish standards regarding how financial institutions provide notifications of a data breach to customers. Under the bill, State insurance authorities would be required to enforce those standards.

Under the bill, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the

National Credit Union Administration (NCUA), the Federal Reserve, the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC) would be required to create or update their standards for notifying people about a data breach. Using information from several of those affected agencies, CBO estimates that the costs to implement the bill would not be significant for any agency.

Any spending by the FTC would be subject to the availability of appropriated funds. Because the SEC is authorized under current law to collect fees sufficient to offset its annual appropriation, we estimate that the net costs to the SEC would be negligible, assuming appropriation actions consistent with that authority.

Administrative costs incurred by the FDIC, the NCUA, and the OCC are recorded in the budget as increases in direct spending, but those agencies are authorized to collect premiums and fees from insured depository institutions to cover administrative expenses. Thus, CBO expects that the net effect on direct spending would be negligible. Administrative costs to the Federal Reserve are reflected in the federal budget as a reduction in remittances to the Treasury (which are recorded in the budget as revenues).

Because enacting H.R. 6743 could affect direct spending and revenues, pay-as-you-go procedures apply. However, the net effect on direct spending and revenues would not be significant.

CBO estimates that enacting H.R. 6743 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 6743 would explicitly preempt state and local laws that require insurance providers as well as financial institutions and their affiliates to notify customers in the event of a security breach. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands would be affected. The bill also would preempt laws in at least 22 states that have enacted data security laws. These preemptions would be a mandate as defined by the Unfunded Mandates Reform Act (UMRA).

The bill also would require state insurance authorities to enforce new federal standards that would direct insurance agencies and brokerages to notify customers of a data breach. That requirement would be a mandate as defined in UMRA.

H.R. 6743 would impose private-sector mandates by requiring financial institutions and their affiliates to comply with new standards for data security and breach notifications as established by the federal government. Further, if federal regulatory agencies increase fees to offset the costs associated with implementing the bill, H.R. 6743 would increase the cost of an existing mandate on private entities required to pay those fees.

Because the various federal regulatory agencies have yet to establish the required data security and breach standards, CBO cannot determine if the cost to comply with the bill's requirements would exceed the threshold for intergovernmental and private-sector mandates established in UMRA ($80 million and $160 million in 2018, respectively, adjusted annually for inflation).

The CBO staff contacts for this estimate are Stephen Rabent (for federal costs) and Rachel Austin (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

This information is provided in accordance with section 423 of the Unfunded Mandates Reform Act of 1995.

The Committee has determined that the bill does not contain Federal mandates on the private sector. The Committee has determined that the bill does not impose a Federal intergovernmental mandate on State, local, or tribal governments.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of the section 102(b)(3) of the Congressional Accountability Act.

EARMARK IDENTIFICATION

With respect to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee has carefully reviewed the provisions of the bill and states that the provisions of the bill do not contain any congressional earmarks, limited tax benefits, or limited tariff benefits within the meaning of the rule.

DUPLICATION OF FEDERAL PROGRAMS

In compliance with clause 3(c)(5) of rule XIII of the Rules of the House of Representatives, the Committee states that no provision of the bill establishes or reauthorizes: (1) a program of the Federal Government known to be duplicative of another Federal program; (2) a program included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139; or (3) a program related to a program identified in the most recent Catalog of Federal Domestic Assistance, published pursuant to the Federal Program Information Act (Pub. L. No. 95–220, as amended by Pub. L. No. 98–169).

DISCLOSURE OF DIRECTED RULEMAKING

Pursuant to section 3(i) of H. Res. 5, (115th Congress), the following statement is made concerning directed rule makings: The Committee estimates that the bill requires no directed rule makings within the meaning of such section.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section cites H.R. 6743 as the "Consumer Information Notification Requirement Act."

Section 2. Breach notification standards

This section amends Section 501 of the Gramm-Leach-Bliley Act in order to help establish and federal standard on data security breach notifications.

Section 3. Preemption with respect to financial institution safeguards

This section amends Section 507 of the Gramm-Leach-Bliley Act to insert a preemptive requirement over state law.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

GRAMM-LEACH-BLILEY ACT

* * * * * * *

TITLE V—PRIVACY

Subtitle A—Disclosure of Nonpublic Personal Information

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) PRIVACY OBLIGATION POLICY.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a), other than the Bureau of Consumer Financial Protection, shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer[.], *including through the provision of a breach notice in the event of unauthorized access that is reasonably likely to result in identity theft, fraud, or economic loss.*

(c) STANDARDS WITH RESPECT TO BREACH NOTIFICATION.—Subject to section 504(a)(2) and sections 505(b) and 505(c), within 6 months after the date of enactment of this subsection, each agency or authority required to establish standards described under subsection (b)(3) with respect to the provision of a breach notice shall ensure that such standards are in compliance with subsection (b).

(d) INSURANCE.—

(1) ENFORCEMENT.—Notwithstanding section 505(a)(6), with respect to an entity engaged in providing insurance, the standards under subsection (b) shall be enforced—

(A) with respect to any such standards related to data security safeguards, by—

(i) the State insurance authority of the State in which the entity is domiciled; or

(ii) in the case of an insurance agency or brokerage, the State insurance authority of the State in which such agency or brokerage has its principal place of business; and

(B) with respect to any such standards related to notification of the breach of data security, by the State insurance authority of any State in which customers of the entity are affected by such a breach of data security.

(2) NOTIFICATION BY ASSUMING INSURER.—

(A) IN GENERAL.—Notwithstanding subsection (b), an assuming insurer that experiences a breach of data security shall only be required to notify the State insurance authority of the State in which the assuming insurer is domiciled.

(B) ASSUMING INSURER DEFINED.—For purposes of this paragraph, the term "assuming insurer" means an entity engaged in providing insurance that acquires an insurance obligation or risk from another entity engaged in providing insurance pursuant to a reinsurance agreement.

(3) SAFEGUARDS FOR INSURANCE CUSTOMERS.—In carrying out subsection (b) with respect to an entity engaged in providing insurance, a State insurance authority shall establish the standards for safeguarding customer information maintained by entities engaged in activities described in section 4(k)(4)(B) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(4)(k)(4)(B)) that are the same as the standards contained in the interagency guidelines issued by the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision titled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information", published February 1, 2001 (66 Fed. Reg. 8633), and such standards shall be applied as if the entity engaged in providing insurance was a bank to the extent appropriate and practicable.

* * * * * * *

[SEC. 507. RELATION TO STATE LAWS.

[(a) IN GENERAL.—This subtitle and the amendments made by this subtitle shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order,

or interpretation is inconsistent with the provisions of this subtitle, and then only to the extent of the inconsistency.

[(b) GREATER PROTECTION UNDER STATE LAW.—For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subtitle and the amendments made by this subtitle, as determined by the Bureau of Consumer Financial Protection, after consultation with the agency or authority with jurisdiction under section 505(a) of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.]

SEC. 507. RELATION TO STATE LAWS.

(a) IN GENERAL.—This subtitle preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, with respect to a financial institution or affiliate thereof securing personal information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of data.

(b) INSURANCE.—Subsection (a) shall not prevent a State or political subdivision of a State from establishing the standards for entities engaged in providing insurance required by sections 501(c) and 501(d), provided the standards established by such State or political subdivision do not impose any requirement that is in addition to or different from those standards, except where necessary to effectuate the purposes of this subtitle.

* * * * * * *

MINORITY VIEWS

One year after the Equifax data breach exposed more than 145 million Americans' personal information, H.R. 6743 would reduce the privacy, confidentiality, and security of American consumers' nonpublic personal information.

H.R. 6743 would put consumers at risk by broadly preempting state law. The bill's Federal preemption would prohibit state Attorneys General from enforcing their own laws against financial institutions that lost their customers' personal, non-public information, and prevent states from applying more stringent protections for their state residents. Thirty-two state Attorneys General warned about the danger of including sweeping Federal preemption in any Federal data security legislation, noting that:

> "States have proven themselves to be active, agile, and experienced enforcers of their consumers' data security and privacy. With the increasing threat and ever—evolving nature of data security risks, the state consumer protection laws that our Offices enforce provide vital flexibility and a vehicle by which the States can rapidly and effectively respond to protect their consumers. . . . Congress should not preempt state data security and breach notification laws." [1]

The Federal preemption provisions in H.R. 6743 go far beyond the existing provisions in the Gramm Leach Bliley Act related to the privacy and security of a financial institution's *customers' nonpublic personal information.* Instead, the bill would prohibit states from enacting and enforcing laws relating to *financial institutions and all of their affiliates with respect to securing any personal information from an unauthorized breach.* Thus, while proponents of the bill claim that it would help enhance data security, it would significantly reduce, and not strengthen, the privacy, confidentiality, and security of American consumers' nonpublic personal information.

A number of state officials, as well as state and national consumer, civil rights, civil liberties, privacy organizations echoed these concerns in their strong opposition to the bill, including the National Governors Association ("NGA"),[2] National Association of Insurance Commissioners ("NAIC"),[3] Conference of State Bank Supervisors ("CSBS"),[4] Consumers Union, U.S. PIRG, Americans for

---

[1] http://www.illinoisattorneygeneral.gov/pressroom/2018_03/20180319b.html and http://www.illinoisattorneygeneral.gov/pressroom/2018_03/Committee_Leaders_letter.pdf.

[2] https://www.nga.org/news/nga-urges-the-house-financial-services-committee-to-oppose-the-consumer-information-notification-requirement-act/.

[3] https//www.naic.org/documents/government_relations_180912_hr6743_consumer_information_notification_req_letter.pdf.

[4] https://www.csbs.org/csbs-opposes-hr-6743-consumer-information-notification-requirement-act.

Financial Reform ("AFR"), Public Citizen, NAACP, National Network to End Domestic Violence, and Patient Privacy Rights.[5]

NGA, for example, underscored that the bill "would prohibit states from imposing or enforcing any strong consumer protection standards that go above and beyond Federal standards, thereby inhibiting ongoing efforts by states to adopt data security laws and regulations that are in the best interest of consumers."

State insurance regulators voiced similar concerns, noting in their opposition letter, that the bill "assigns enforcement of its Federal data security requirements to an insurer's state of domicile, which may be far removed from the location of consumers who are harmed by a data breach. . . . It is fundamentally at odds with the state-based regulatory regime, which recognizes that those insurance regulators that have expertise and experience with a local insurance market are best positioned to protect a state's insurance consumers."

The CSBS also stated, "State regulators firmly oppose H.R. 6743 for its attempt to preempt state data breach and privacy laws. States have demonstrated their ability to spot emerging risks early and to act with agility in responding to those risks."

Unfortunately, an amendment offered by Ranking Member Waters to repeal the harmful Federal preemption provision in the bill was rejected on a party-line vote. Therefore, we oppose H.R. 6743, which would gut states' discretion and ability to protect their residents.

MAXINE WATERS.
CAROLYN B. MALONEY.
NYDIA M. VELÁZQUEZ.
WM. LACY CLAY.
MICHAEL E. CAPUANO.
CHARLIE CRIST.

○

[5] See https://uspirg.org/resources/usp/group-letter-opposing-equifax-protection-act-hr6743-luetkemeyer-prevents-state-data, https://uspirg.org/blogs/eds-blog/usp/latest-trojan-horse-data-breach-bill-hr6743-luetkemeyer-could-be-called-equifax, and https://uspirg.org/blogs/blog/usp/32-state-attorneys-general-congress-dont-replace-our-stronger-privacy-laws.