114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
114–908

DATA SECURITY AND BREACH NOTIFICATION ACT OF 2015

JANUARY 3, 2017.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. UPTON, from the Committee on Energy and Commerce, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 1770]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 1770) to require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

69–006

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; PURPOSES.

(a) SHORT TITLE.—This Act may be cited as the "Data Security and Breach Notification Act of 2015".

(b) PURPOSES.—The purposes of this Act are to—

(1) protect consumers from identity theft, economic loss or economic harm, and financial fraud by establishing strong and uniform national data security and breach notification standards for electronic data in interstate commerce while minimizing State law burdens that may substantially affect interstate commerce; and

(2) expressly preempt any related State laws to ensure uniformity of this Act's standards and the consistency of their application across jurisdictions.

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

A covered entity shall implement and maintain reasonable security measures and practices to protect and secure personal information in electronic form against unauthorized access and acquisition as appropriate for the size and complexity of such covered entity and the nature and scope of its activities.

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) IN GENERAL.—

(1) RESTORING SECURITY.—Except as otherwise provided by this section, a covered entity that uses, accesses, transmits, stores, disposes of, or collects personal information shall, following the discovery of a breach of security restore the reasonable integrity, security, and confidentiality of the data system and identify the impact of the breach pursuant to paragraph (2).

(2) INVESTIGATION.—A covered entity shall conduct in good faith a reasonable and prompt investigation of the breach of security to determine whether there is a reasonable risk that the breach of security has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud to the individuals whose personal information was subject to the breach of security.

(3) NOTIFICATION TO INDIVIDUALS REQUIRED.—

(A) TRIGGER.—Unless there is no reasonable risk that the breach of security has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud to the individuals whose personal information was affected by the breach of security, the covered entity shall notify any resident of the United States that has been affected by the breach of security pursuant to this section.

(B) NOTIFICATION DUTY.—Unless subject to a delay authorized under subsection (c)—

(i) a breached covered entity shall notify any individual for whom an election was not made under paragraph (4)(C) not later than 25 days after the non-breached covered entity declines or fails to exercise the election under paragraph (4)(C);

(ii) a non-breached covered entity shall notify any individual for whom the non-breached covered entity provided personal information to the breached covered entity, and such personal information was affected by the breach of security, not later than 25 days after exercising the election under paragraph (4)(C); and

(iii) any other covered entity shall identify the individuals affected by a breach of security and make the notification required under this subsection as expeditiously as possible, without unreasonable delay, and not later than 30 days after completing the requirements of paragraph (1).

(C) NOTIFICATION REQUIRED UPON DISCOVERY OF ADDITIONAL INDIVIDUALS AFFECTED.—If a covered entity, breached covered entity, or non-breached covered entity has provided the notification to individuals required under this subsection and after such notification discovers additional individuals to whom notification is required under this subsection with respect to the same breach of security, the covered entity, breached covered entity, or non-breached covered entity shall make such notification to such individuals as expeditiously as possible and without unreasonable delay.

(4) NON-BREACHED COVERED ENTITY ELECTION NOTICE.—

(A) NOTICE TO NON-BREACHED COVERED ENTITY REQUIRED.—Subject to the requirements of this paragraph, unless there is no reasonable risk that the breach of security has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud related to the personal information provided by the non-breached covered entity to the breached covered entity, the breached covered entity shall, as expeditiously as possible and without unreasonable delay within 10 days after fulfilling the requirements described in paragraph (1), notify in writing each non-breached covered entity of the breach of security.

(B) CONTENTS OF NOTICE.—The breached covered entity shall include in the notice described in subparagraph (A) the elements of personal information received from the non-breached covered entity pursuant to the contract described in subparagraph (C) reasonably believed to be affected by the breach of security.

(C) ELECTION BY NON-BREACHED COVERED ENTITY AFTER RECEIVING NOTICE FROM A BREACHED COVERED ENTITY.—In the case of a breached covered entity that is a party to a written contract with a non-breached covered entity in which the breached covered entity maintains, stores, transmits, or processes data in electronic form containing personal information, not later than 10 days after receipt of the notice described in subparagraph (A), the non-breached covered entity may elect, in writing to the breached covered entity, to provide notification required by paragraph (3) all individuals whose personal information was provided by the non-breached covered entity to the breached covered entity and was affected by the breach of security. Such election relieves the breached covered entity of the requirements under paragraph (3) with respect to such individuals.

(D) OBLIGATION AFTER ELECTION.—

(i) BREACHED COVERED ENTITY COOPERATION.—If a non-breached covered entity elects under subparagraph (C) to provide notice under paragraph (3), the breached covered entity shall cooperate in all reasonable respects with the non-breached covered entity and provide any of the information the breached covered entity possesses that is described under subsection (d)(1)(B) and provide all personal information received from the non-breached covered entity that was affected by the breach of security so that the notification to such individuals is made as required under this section. Not later than 10 business days after the non-breached covered entity submits a written request for information requested under this subsection to the breached covered entity, the breached covered entity shall provide such information.

(ii) NON-BREACHED COVERED ENTITY COOPERATION.—If a non-breached covered entity does not elect to provide notice to individuals under subparagraph (C), the non-breached covered entity shall provide any of the information the non-breached covered entity possesses that is described under subsection (d)(1)(B) for any individual whose personal information was received from the non-breached covered entity that was affected by the breach of security, and cooperate in all reasonable respects with, the breached covered entity so that the notification to such individuals is made as required under this section. Not later than 10 business days after the breached covered entity submits a written request for information requested under this subsection to the non-breached covered entity, the non-breached covered entity shall provide such information.

(5) LAW ENFORCEMENT.—A covered entity shall as expeditiously as possible notify the Commission and the Secret Service or the Federal Bureau of Investigation of the fact that a breach of security has occurred if the number of individuals whose personal information was, or there is a reasonable basis to conclude was, accessed and acquired by an unauthorized person exceeds 10,000. Any notification provided to the Secret Service or the Federal Bureau of Investigation pursuant to this paragraph shall be provided not less than 10 days before notification is provided to individuals pursuant to paragraph (3).

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) NON-PROFIT ORGANIZATIONS.—In the event of a breach of security involving personal information that would trigger notification under subsection (a), a non-profit organization may complete such notification according to the procedures set forth in subsection (d)(2).

(2) COORDINATION OF NOTIFICATION WITH CONSUMER REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 10,000 individuals under subsection (a), such covered entity shall also notify a consumer

reporting agency that compiles and maintains files on consumers on a nationwide basis, of the timing and distribution of the notices. Such notice shall be given to such consumer reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—Notwithstanding paragraph (1), if a Federal, State, or local law enforcement agency determines that the notification to individuals required under this section would impede a civil or criminal investigation or a Federal agency determines that such notification would threaten national security, such notification shall be delayed upon written request of the law enforcement agency or Federal agency which the law enforcement agency or Federal agency determines is reasonably necessary and requests in writing. A law enforcement agency or Federal agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary. If a law enforcement agency or Federal agency requests a delay of notification to individuals under this paragraph, the Commission shall, upon written request of the law enforcement agency or Federal agency, delay any public disclosure of a notification received by the Commission under this section relating to the same breach of security until the delay of notification to individuals is no longer in effect.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods (if the selected method can reasonably be expected to reach the intended individual):

(i) Written notification by postal mail.

(ii) Notification by email or other electronic means, if the covered entity's primary method of communication with the individual is by email or such other electronic means or the individual has consented to receive such notification.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a breach of security, such notification shall include each of the following:

(i) The identity of the covered entity that suffered the breach and, if such covered entity is also a breached covered entity providing notice under section 3(b)(1), the identity of each non-breached covered entity that did not elect to notify affected individuals pursuant to section 3(b)(1)(B) sufficient to show the breached covered entity's commercial relationship to the individual receiving notice.

(ii) A description of the personal information that was, or there is a reasonable basis to conclude was, acquired and accessed by an unauthorized person.

(iii) The date range of the breach of security, or an approximate date range of the breach of security if a specific date range is unknown based on the information available at the time of the notification.

(iv) A telephone number, or toll-free telephone number for any covered entity that does not meet the definition of a small business concern or non-profit organization, that the individual may use to contact the covered entity to inquire about the breach of security or the information the covered entity maintained about that individual.

(v) The toll-free contact telephone numbers and addresses for a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.

(vi) The toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft.

(2) SUBSTITUTE NOTIFICATION.—

(A) IN GENERAL.—If, after making reasonable efforts to contact all individuals to whom notice is required under subsection (a), the covered entity finds that contact information for 500 or more individuals is insufficient or out-of-date, the covered entity shall also provide substitute notice to those individuals, which shall be reasonably calculated to reach the individuals affected by the breach of security.

(B) FORM OF SUBSTITUTE NOTIFICATION.—A covered entity may provide substitute notification by—

(i) email or other electronic notification to the extent that the covered entity has contact information for individuals to whom it is required to provide notification under subsection (a); and

(ii) a conspicuous notice on the covered entity's Internet website (if such covered entity maintains such a website) for at least 90 days.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under clauses (i) and (ii) of subparagraph (B) shall include the information required under paragraph (1)(B).

(3) DIRECT NOTIFICATION BY A THIRD PARTY.—Nothing in this Act shall be construed to prevent a covered entity from contracting with a third party to provide the notification required under this section, provided such third party issues such notification without unreasonable delay, in accordance with the requirements of this section, and indicates to all individuals in such notification that such third party is sending such notification on behalf of the covered entity.

(e) REQUIREMENTS OF SERVICE PROVIDERS.—

(1) IN GENERAL.—If a service provider becomes aware of a breach of security involving data in electronic form containing personal information that is owned or licensed by a covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage of the data containing personal information breached, if such covered entity can be reasonably identified. If a service provider is acting solely as a service provider for purposes of this subsection, the service provider has no other notification obligations under this section.

(2) COVERED ENTITIES WHO RECEIVE NOTICE FROM SERVICE PROVIDERS.—Upon receiving notification from a service provider under paragraph (1), a covered entity shall provide notification as required under this section.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, and any covered entity who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.), and as provided in clauses (ii) and (iii) of section 5(5)(A). Notwithstanding section 5(m) of the Federal Trade Commission Act, the Commission may impose civil penalties for violations of section 3 in an amount not greater than $1,000 per violation. Each failure to send notification as required under section 3 to a resident of the United States shall be treated as a separate violation.

(3) MAXIMUM TOTAL LIABILITY FOR FIRST-TIME VIOLATION OF SECTION 2.—The maximum total civil penalty for which any covered entity is liable under this subsection for all violations of section 2 resulting from the same related act or omission may not exceed $8,760,000, if such act or omission constitutes the covered entity's first violation of section 2.

(4) MAXIMUM TOTAL LIABILITY FOR FIRST-TIME VIOLATION OF SECTION 3.—The maximum total civil penalty for which any covered entity is liable under this subsection for all violations of section 3 resulting from the same related act or omission may not exceed $17,520,000, if such act or omission constitutes the covered entity's first violation of section 3.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity who violates section 2 or 3 of this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin further violation of such section by the defendant;

(B) compel compliance with such section; or

(C) obtain civil penalties in the amount determined under paragraph (2).

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 2.—For purposes of paragraph (1)(C) with regard to all violations of section 2 resulting from the same related act or omission, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such section by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph (1)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $1,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation.

(B) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection shall not exceed—

(i) $2,500,000 for each violation of section 2; and

(ii) $2,500,000 for all violations of section 3 resulting from a single breach of security.

(C) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after one year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) and clauses (i) and (ii) of subparagraph (B) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(D) PENALTY FACTORS.—In determining the amount of such a civil penalty, the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require shall be taken into account.

(3) INTERVENTION BY THE FEDERAL TRADE COMMISSION.—

(A) NOTICE AND INTERVENTION.—In all cases, the State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) PENDING PROCEEDINGS.—If the Federal Trade Commission initiates a Federal civil action for a violation of this Act, no State attorney general may bring an action for a violation of this Act that resulted from the same or related acts or omissions against a defendant named in the civil action initiated by the Federal Trade Commission.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(c) NO PRIVATE CAUSE OF ACTION.—Nothing in this Act shall be construed to establish a private cause of action against a person for a violation of this Act.

SEC. 5. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term "breach of security"—

(A) means a compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to and acquisition of personal information from a covered entity; and

(B) does not include the good faith acquisition of personal information by an employee or agent of the covered entity for the purposes of the covered entity, if the personal information is not used or subject to further unauthorized disclosure.

(2) BREACHED COVERED ENTITY.—The term "breached covered entity" means a covered entity that has incurred a breach of security affecting data in electronic form containing personal information of a non-breached covered entity that has directly contracted the breached covered entity to maintain, store, or process data in electronic form containing personal information on behalf of such non-breached covered entity. For purposes of this definition, the term "breached covered entity" shall not include a service provider that is subject to section 3(e).

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" has the meaning given that term in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(5) COVERED ENTITY.—

(A) IN GENERAL.—The term "covered entity" means—

(i) a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other entity in or affecting commerce that acquires, maintains, stores, sells, or otherwise uses data in electronic form that includes personal information, over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(ii) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and

(iii) notwithstanding any jurisdictional limitation of the Federal Trade Commission Act (15 U.S.C. 41 et seq.), any non-profit organization.

(B) EXCEPTIONS.—The term "covered entity" does not include—

(i) a covered entity, as defined in section 160.103 of title 45, Code of Federal Regulations;

(ii) a business associate, as defined in section 160.103 of title 45, Code of Federal Regulations, acting in its capacity as a business associate;

(iii) if a covered entity, as defined in section 160.103 of title 45, Code of Federal Regulations, is a hybrid entity, as defined in section 164.105 of title 45, Code of Federal Regulations, then the health care component of such hybrid entity;

(iv) a broker, dealer, investment adviser, futures commission merchant, special purpose vehicle, finance company, or person engaged in providing insurance that is subject to title V of Public Law 106-102 (15 U.S.C. 6801 et seq.);

(v) a State-chartered credit union, as defined in section 101(6) of the Federal Credit Union Act (12 U.S.C. 1752(6)), that is not an insured credit union as defined in section 101(7) of such Act (12 U.S.C. 1752(7)); or

(vi) a credit union service organization as outlined in section 106(7)(I) of the Federal Credit Union Act (12 U.S.C. 1757(7)(I)).

(6) DATA IN ELECTRONIC FORM.—The term "data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(7) ENCRYPTED.—The term "encrypted", used with respect to data in electronic form, in storage or in transit—

(A) means the data is protected using an encryption technology that has been generally accepted by experts in the field of information security at the time the breach of security occurred that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys in order to protect the integrity of the encryption.

(8) NON-BREACHED COVERED ENTITY.—The term "non-breached covered entity" means a covered entity that has not incurred the breach of security involving data in electronic form containing personal information that it owns or licenses but whose data has been affected by the breach of security incurred by a breached covered entity it directly contracts to maintain, store, or process data in electronic form containing personal information on behalf of the non-breached covered entity.

(9) NON-PROFIT ORGANIZATION.—The term "non-profit organization" means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code.

(10) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term "personal information" means any information or compilation of information in electronic form that includes the following:

(i) An individual's first and last name or first initial and last name in combination with all of the following:

(I) Home address or telephone number.

(II) Mother's maiden name, if identified as such.

(III) Month, day, and year of birth.

(ii) A financial account number or credit or debit card number or other identifier, in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

(iii) A unique account identifier (other than for an account described in clause (ii)), electronic identification number, biometric data unique to an individual, user name, or routing code in combination with any associated security code, access code, biometric data unique to an individual, or password that is required for an individual to obtain money, or purchase goods, services, or any other thing of value.

(iv) A non-truncated social security number.

(v) Any information that pertains to the transmission of specific calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(vi) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(vii) A driver's license number, passport number, or alien registration number or other government-issued unique identification number.

(B) EXCEPTIONS.—The term "personal information" does not include—

(i) information that is encrypted or rendered unusable, unreadable, or indecipherable through data security technology or methodology that is generally accepted by experts in the field of information security at the time the breach of security occurred, such as redaction or access controls; or

(ii) information available in a publicly available source, including information obtained from a news report, periodical, or other widely distributed media, or from Federal, State, or local government records.

(11) SERVICE PROVIDER.—The term "service provider" means a covered entity subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) that provides electronic data transmission, routing, intermediate and transient storage, or connection to its system or network, where such entity providing such service does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such entity transmits, routes, stores, or for which such entity provides connections. Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

(12) SMALL BUSINESS CONCERN.—The term "small business concern" has the meaning given such term under section 3 of the Small Business Act (15 U.S.C. 632).

(13) STATE.—The term "State" means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Virgin Islands of the United States, the Commonwealth of the Northern Mariana Islands, any other territory or possession of the United States, and each federally recognized Indian tribe.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—No State or political subdivision of a State shall, with respect to a covered entity subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a security breach of such data.

(b) COMMON LAW.—This section shall not exempt a covered entity from liability under common law.

(c) CERTAIN FTC ENFORCEMENT LIMITED TO DATA SECURITY AND BREACH NOTIFICATION.—

(1) DATA SECURITY AND BREACH NOTIFICATION.—Insofar as sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551), and any regulations promulgated thereunder, apply to covered entities with respect to securing information in electronic form from unauthorized access and acquisition, including notification of unauthorized access and acquisition to data in electronic form containing personal information, such sections and regulations promulgated thereunder shall have no force or effect, unless such regulations pertain solely to 9–1–1 calls.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection otherwise limits the Federal Communications Commission's authority with respect to sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551).

(d) PRESERVATION OF COMMISSION AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 7. EDUCATION AND OUTREACH FOR SMALL BUSINESSES.

The Commission shall conduct education and outreach for small business concerns on data security practices and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such small business concerns.

SEC. 8. WEBSITE ON DATA SECURITY BEST PRACTICES.

The Commission shall establish and maintain an Internet website containing nonbinding best practices for businesses regarding data security and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such businesses.

SEC. 9. EFFECTIVE DATE.

This Act shall take effect 1 year after the date of enactment of this Act.

PURPOSE AND SUMMARY

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

Consumers face an increasing risk of identity theft and financial fraud created by criminals with varying motivations, but a common goal: to steal personal information for financial gain.

Currently, there are forty-seven different State laws dealing with data breach notification and twelve State laws governing commercial data security. This patchwork of State laws creates confusion for consumers looking for consistency and predictability in breach notices, as well as complex compliance issues for businesses as they secure their systems after a breach. Moreover, this patchwork has not always resulted in better consumer protections and may lead to additional opportunities for cyber criminals to exploit vulnerable individuals with phishing attacks or other schemes because there is no consistent standard for data security or breach notification. Following a breach, consumers must take steps to protect their accounts and their credit by replacing their cards, updating accounts, and monitoring their credit with existing tools. In addition, consumers ultimately bear the costs of the breach through higher fees and prices.

H.R. 1770 addresses the growing problem of identity theft and payment fraud by requiring covered entities to implement reasonable security measures for the type of personal information that

criminals use for identity theft and payment fraud and to notify individuals in the case of a breach of security for such personal information. H.R. 1770 would establish a single Federal regime enforced by the Federal Trade Commission (FTC) and subject to civil penalties. Additionally, State attorneys general would be authorized to enjoin violations, compel compliance, or seek civil penalties for violations of the Act. H.R. 1770 is limited in scope to address those categories of information that result in identity theft and payment fraud. The bill neither addresses privacy issues nor preempts existing privacy laws.

HEARINGS

The Subcommittee on Commerce, Manufacturing, and Trade held a hearing on the discussion draft, H.R. ____, the Data Security and Breach Notification Act of 2015 on March 18, 2015. The Subcommittee received testimony from:

- Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission;
- Clete Johnson, Chief Counsel for Cybersecurity, Public Safety and Homeland Security Bureau, Federal Communications Commission;
- Mallory Duncan, Senior Vice President and General Counsel, National Retail Federation;
- Jon Leibowitz, Partner, David Polk & Wardwell LLP, Co-Chairman of, and on behalf of, the 21st Century Privacy Coalition;
- Laura Moy, Senior Policy Council, Open Technology Institute, New America;
- Yael Weinman, Vice President, Global Privacy Policy and General Counsel, Information Technology Industry Council; and,
- Sara Cable, Assistant Attorney General, Office of the Massachusetts Attorney General.

COMMITTEE CONSIDERATION

On March 25, 2015, the Subcommittee on Commerce, Manufacturing, and Trade met in open markup session and forwarded H.R. ____, Data Security and Breach Notification Act of 2015 to the full Committee, as amended, by a voice vote. On April 14, 2015, Rep. Blackburn, Rep. Welch, Rep. Burgess, and Rep. Upton introduced H.R. 1770, which was substantially similar to the bill approved by the Subcommittee. On April 15, 2015, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 1770, Data Security and Breach Notification Act of 2015, reported to the House, as amended, by a record vote of 29 yeas and 20 nays.

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. A motion by Mr. Upton to order H.R. 1770 reported to the House, as amended, was agreed to by a record vote of 29 ayes and 20 nays. The following reflects the record votes taken during the Committee consideration:

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 3

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: An amendment offered by Mr. Rush, No. 2, to strike all language following the enacting clause and insert the "Data Accountability and Trust Act."

DISPOSITION: NOT AGREED TO, by a roll call vote of 23 yeas and 28 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton		X		Mr. Pallone	X		
Mr. Barton	X			Mr. Rush	X		
Mr. Whitfield		X		Ms. Eshoo	X		
Mr. Shimkus		X		Mr. Engel	X		
Mr. Pitts		X		Mr. Green			
Mr. Walden		X		Ms. DeGette			
Mr. Murphy		X		Ms. Capps	X		
Mr. Burgess		X		Mr. Doyle	X		
Mrs. Blackburn		X		Ms. Schakowsky	X		
Mr. Scalise		X		Mr. Butterfield	X		
Mr. Latta		X		Ms. Matsui	X		
Mrs. McMorris Rodgers		X		Ms. Castor	X		
Mr. Harper		X		Mr. Sarbanes	X		
Mr. Lance	X			Mr. McNerney	X		
Mr. Guthrie				Mr. Welch	X		
Mr. Olson		X		Mr. Lujan	X		
Mr. McKinley		X		Mr. Tonko	X		
Mr. Pompeo		X		Mr. Yarmuth	X		
Mr. Kinzinger		X		Ms. Clarke	X		
Mr. Griffith		X		Mr. Loebsack	X		
Mr. Bilirakis		X		Mr. Schrader	X		
Mr. Johnson		X		Mr. Kennedy	X		
Mr. Long		X		Mr. Cardenas	X		
Mrs. Ellmers		X					
Mr. Bucshon		X					
Mr. Flores		X					
Mrs. Brooks		X					
Mr. Mullin		X					
Mr. Hudson		X					
Mr. Collins		X					
Mr. Cramer		X					

04/15/2015

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 4

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: An amendment offered by Mr. Olson, No. 3, to cap the Federal Trade Commission's (FTC) civil penalty authority for first-time violations under sections 2 and 3 of this bill, to cap the FTC's civil penalty authority for violations of section 3, and to lower the civil penalty maximums per violation of section 3 for State Attorney's General.

DISPOSITION: AGREED TO, by a roll call vote of 30 yeas and 20 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton	X			Mr. Pallone		X	
Mr. Barton		X		Mr. Rush		X	
Mr. Whitfield	X			Ms. Eshoo		X	
Mr. Shimkus	X			Mr. Engel			
Mr. Pitts	X			Mr. Green			
Mr. Walden	X			Ms. DeGette			
Mr. Murphy	X			Ms. Capps		X	
Mr. Burgess	X			Mr. Doyle		X	
Mrs. Blackburn	X			Ms. Schakowsky		X	
Mr. Scalise				Mr. Butterfield		X	
Mr. Latta	X			Ms. Matsui		X	
Mrs. McMorris Rodgers	X			Ms. Castor		X	
Mr. Harper	X			Mr. Sarbanes		X	
Mr. Lance	X			Mr. McNerney		X	
Mr. Guthrie	X			Mr. Welch		X	
Mr. Olson	X			Mr. Lujan		X	
Mr. McKinley	X			Mr. Tonko		X	
Mr. Pompeo	X			Mr. Yarmuth		X	
Mr. Kinzinger	X			Ms. Clarke		X	
Mr. Griffith	X			Mr. Loebsack		X	
Mr. Bilirakis	X			Mr. Schrader	X		
Mr. Johnson	X			Mr. Kennedy		X	
Mr. Long	X			Mr. Cardenas		X	
Mrs. Ellmers	X						
Mr. Bucshon	X						
Mr. Flores	X						
Mrs. Brooks	X						
Mr. Mullin	X						
Mr. Hudson	X						
Mr. Collins	X						
Mr. Cramer	X						

04/15/2015

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 5

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: An amendment in the nature of a substitute offered by Ms. Eshoo, No. 4, to grant APA rulemaking authority for the Federal Trade Commission (FTC) to define both security standards and breach notification standards that are consistent with California Civil Code sections 1798.81.5 and 1798.82, to grant enforcement jurisdiction to the FTC keeping in place enforcement authority for the Federal Communications Commission and the Consumer Financial Protection Bureau, to grant a private right of action, and to add health insurance information and medical information as personal information.

DISPOSITION: NOT AGREED TO, by a roll call vote of 20 yeas and 30 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton		X		Mr. Pallone	X		
Mr. Barton		X		Mr. Rush	X		
Mr. Whitfield		X		Ms. Eshoo	X		
Mr. Shimkus		X		Mr. Engel			
Mr. Pitts		X		Mr. Green			
Mr. Walden		X		Ms. DeGette			
Mr. Murphy		X		Ms. Capps	X		
Mr. Burgess		X		Mr. Doyle	X		
Mrs. Blackburn		X		Ms. Schakowsky	X		
Mr. Scalise				Mr. Butterfield	X		
Mr. Latta		X		Ms. Matsui	X		
Mrs. McMorris Rodgers		X		Ms. Castor	X		
Mr. Harper		X		Mr. Sarbanes	X		
Mr. Lance		X		Mr. McNerney	X		
Mr. Guthrie		X		Mr. Welch	X		
Mr. Olson		X		Mr. Lujan	X		
Mr. McKinley		X		Mr. Tonko	X		
Mr. Pompeo		X		Mr. Yarmuth	X		
Mr. Kinzinger		X		Ms. Clarke	X		
Mr. Griffith		X		Mr. Loebsack	X		
Mr. Bilirakis		X		Mr. Schrader	X		
Mr. Johnson		X		Mr. Kennedy	X		
Mr. Long		X		Mr. Cardenas	X		
Mrs. Ellmers		X					
Mr. Bucshon		X					
Mr. Flores		X					
Mrs. Brooks		X					
Mr. Mullin		X					
Mr. Hudson		X					
Mr. Collins		X					
Mr. Cramer		X					

04/15/2015

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 6

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: An amendment offered by Mr. Kennedy, No. 9, to amend preemption language by allowing States to continue to bring State law-based unfair or deceptive acts or practices including claims relating to an individual's written communication's related to financial or legal matters, data security, or breach notification.

DISPOSITION: NOT AGREED TO, by a roll call vote of 19 yeas and 26 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton		X		Mr. Pallone	X		
Mr. Barton	X			Mr. Rush	X		
Mr. Whitfield	X			Ms. Eshoo	X		
Mr. Shimkus		X		Mr. Engel			
Mr. Pitts		X		Mr. Green			
Mr. Walden		X		Ms. DeGette			
Mr. Murphy		X		Ms. Capps	X		
Mr. Burgess		X		Mr. Doyle	X		
Mrs. Blackburn		X		Ms. Schakowsky	X		
Mr. Scalise				Mr. Butterfield			
Mr. Latta		X		Ms. Matsui	X		
Mrs. McMorris Rodgers				Ms. Castor	X		
Mr. Harper		X		Mr. Sarbanes	X		
Mr. Lance		X		Mr. McNerney	X		
Mr. Guthrie		X		Mr. Welch	X		
Mr. Olson		X		Mr. Lujan	X		
Mr. McKinley		X		Mr. Tonko	X		
Mr. Pompeo		X		Mr. Yarmuth	X		
Mr. Kinzinger		X		Ms. Clarke			
Mr. Griffith		X		Mr. Loebsack			
Mr. Bilirakis		X		Mr. Schrader	X		
Mr. Johnson		X		Mr. Kennedy	X		
Mr. Long		X		Mr. Cardenas	X		
Mrs. Ellmers		X					
Mr. Bucshon		X					
Mr. Flores							
Mrs. Brooks		X					
Mr. Mullin		X					
Mr. Hudson		X					
Mr. Collins		X					
Mr. Cramer		X					

04/15/2015

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 7

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: An amendment offered by Mr. Kennedy, No. 10, to insert a non-exhaustive list of permissible common law claims in the section that excludes common law claims from the preemption of State data security and breach notification laws.

DISPOSITION: NOT AGREED TO, by a roll call vote of 19 yeas and 27 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton		X		Mr. Pallone	X		
Mr. Barton		X		Mr. Rush	X		
Mr. Whitfield		X		Ms. Eshoo	X		
Mr. Shimkus		X		Mr. Engel			
Mr. Pitts		X		Mr. Green			
Mr. Walden		X		Ms. DeGette	X		
Mr. Murphy				Ms. Capps	X		
Mr. Burgess		X		Mr. Doyle	X		
Mrs. Blackburn		X		Ms. Schakowsky	X		
Mr. Scalise				Mr. Butterfield			
Mr. Latta		X		Ms. Matsui	X		
Mrs. McMorris Rodgers				Ms. Castor	X		
Mr. Harper		X		Mr. Sarbanes	X		
Mr. Lance		X		Mr. McNerney	X		
Mr. Guthrie		X		Mr. Welch	X		
Mr. Olson		X		Mr. Lujan	X		
Mr. McKinley		X		Mr. Tonko	X		
Mr. Pompeo		X		Mr. Yarmuth	X		
Mr. Kinzinger		X		Ms. Clarke			
Mr. Griffith		X		Mr. Loebsack	X		
Mr. Bilirakis		X		Mr. Schrader	X		
Mr. Johnson		X		Mr. Kennedy	X		
Mr. Long		X		Mr. Cardenas	X		
Mrs. Ellmers		X					
Mr. Bucshon		X					
Mr. Flores							
Mrs. Brooks		X					
Mr. Mullin		X					
Mr. Hudson		X					
Mr. Collins		X					
Mr. Cramer		X					

04/15/2015

COMMITTEE ON ENERGY AND COMMERCE -- 114TH CONGRESS
ROLL CALL VOTE # 8

BILL: H.R. 1770, the "Data Security and Breach Notification Act of 2015"

AMENDMENT: A motion by Mr. Upton to order H.R. 1770 favorably reported to the House, as amended. (Final Passage)

DISPOSITION: AGREED TO, by a roll call vote of 29 yeas and 20 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Upton	X			Mr. Pallone		X	
Mr. Barton	X			Mr. Rush		X	
Mr. Whitfield	X			Ms. Eshoo		X	
Mr. Shimkus	X			Mr. Engel			
Mr. Pitts	X			Mr. Green			
Mr. Walden	X			Ms. DeGette		X	
Mr. Murphy				Ms. Capps		X	
Mr. Burgess	X			Mr. Doyle		X	
Mrs. Blackburn	X			Ms. Schakowsky		X	
Mr. Scalise	X			Mr. Butterfield		X	
Mr. Latta	X			Ms. Matsui		X	
Mrs. McMorris Rodgers	X			Ms. Castor		X	
Mr. Harper	X			Mr. Sarbanes		X	
Mr. Lance	X			Mr. McNerney			
Mr. Guthrie	X			Mr. Welch		X	
Mr. Olson	X			Mr. Lujan		X	
Mr. McKinley	X			Mr. Tonko		X	
Mr. Pompeo	X			Mr. Yarmuth		X	
Mr. Kinzinger	X			Ms. Clarke		X	
Mr. Griffith	X			Mr. Loebsack		X	
Mr. Bilirakis	X			Mr. Schrader		X	
Mr. Johnson	X			Mr. Kennedy		X	
Mr. Long	X			Mr. Cardenas		X	
Mrs. Ellmers	X						
Mr. Bucshon	X						
Mr. Flores							
Mrs. Brooks	X						
Mr. Mullin	X						
Mr. Hudson	X						
Mr. Collins	X						
Mr. Cramer	X						

04/15/2015

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a hearing and made findings that are reflected in this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goal of H.R. 1770 is to protect consumers from identity theft, economic loss or economic harm, of financial fraud by establishing strong and uniform national data security and breach notification standards for electronic data in interstate commerce while minimizing State law burdens that may substantially affect interstate commerce, and expressly preempt any related State laws to ensure uniformity of this Act's standards and the consistency of their application across jurisdictions.

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 finds that H.R. 1770, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

EARMARK, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with clause 9(e), 9(f), and 9(g) of rule XXI of the Rules of the House of Representatives, the Committee finds that H.R. 1770 contains no earmarks, limited tax benefits, or limited tariff benefits.

COMMITTEE COST ESTIMATE

The Committee adopts as its own 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 ESTIMATE

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, April 20, 2015.

Hon. FRED UPTON,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1770, the Data Security and Breach Notification Act of 2015.

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

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 1770—Data Security and Breach Notification Act of 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-tree 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.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATION OF FEDERAL PROGRAMS

No provision of H.R. 1770 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that enacting H.R. 1770 specifically directs to be completed no rule making within the meaning of 5 U.S.C. 551.

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 section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title; purposes

Section 1 provides that the Act may be cited as the "Data Security and Breach Notification Act of 2015," and that its purpose is to protect consumers from identity theft, economic loss or economic harm, and financial fraud by establishing uniform national data security and breach notification standards for electronic data in interstate commerce.

Section 2. Requirements for information security

This section requires covered entities to implement and maintain reasonable security measures and practices that are appropriate to the size and complexity of the entity and the nature and scope of its activities, and to protect and secure electronic personal information against unauthorized access and acquisition.

Section 3. Notification of information security breach

Following a breach of security, this section requires a covered entity that uses, accesses, transmits, stores, disposes of, or collects personal information to restore the reasonable integrity, security, and confidentiality of the data system, and conduct a reasonable and prompt investigation of the breach to determine whether there is a reasonable risk that the breach has resulted in, or will result in, identity theft, economic loss or economic harm, or financial fraud.

This section requires covered entities to notify individuals affected by, or reasonably believed to have been affected by, the breach of security unless there is no reasonable risk that the breach has resulted in, or will result in identity theft, economic loss or economic harm, or financial fraud. A breached covered entity shall notify any individual for whom an election was not made under this section not later than twenty-five days after the non-breached covered entity declines or fails to make an election. A non-breached covered entity shall notify any individual for whom it provided personal information to the breached covered entity that was affected by the breach of security within twenty-five days after exercising the election under this section. Any other covered entity shall identify the individuals affected by the breach of security and notify them within thirty days after restoring the reasonable integrity, security, and confidentiality of the data system and identifying the impact of the breach of security pursuant to this section.

If a covered entity, breached covered entity, or non-breached covered entity discovers additional individuals to whom notification is required after providing notice under this section, the covered entity shall notify such individuals as expeditiously as possible and without unreasonable delay.

This section requires breached covered entities to notify in writing a non-breached covered entity of a breach of security within ten days after restoring the reasonable integrity, security, and confidentiality of the data system and identifying the impact of the breach pursuant to this section. The breached covered entity shall include in the notice information about the elements of personal information received from the non-breached covered entity pursuant to their contract reasonably believed to be affected by the breach of security. A non-breached covered entity may elect in writing to provide notice to all individuals included in the notice whose personal information was affected by the breach of security within ten days of receiving the notice. Such election relieves the breached covered entity of its notification obligation under this section for those individuals. After an election by a non-breached covered entity, the breached covered entity shall cooperate in all reasonable respects with the non-breached covered entity and provide any of the information the breached covered entity possesses that is described

in the notice to individuals so that notification to individuals is made in compliance with this section. A breached covered entity shall reply within ten business days to a request for such information by a non-breached covered entity. If a non-breached covered entity declines or fails to elect, it shall cooperate in all respects with the breached covered entity and provide any information it possesses that is described in the notice to individuals so that notification to individuals is made in compliance with this section. A non-breached covered entity shall reply within 10 business days to a request for such information by a breached covered entity.

This section requires a covered entity to also notify the FTC and the Secret Service or Federal Bureau of Investigation of a breach of security if more than 10,000 individuals' personal information was, or there is reasonable basis to conclude was, accessed and acquired by an unauthorized person. This section allows Federal, State, or local law enforcement to delay notification to affected individuals if it would impede a civil or criminal investigation.

This section provides certain accommodations for non-profits or where there is limited contact information for an individual. This section requires covered entities to notify a consumer reporting agency of a breach of security affecting more than 10,000 individuals.

This section requires that any notice to affected individuals about a breach of security must include: 1) a description of the personal information that was, or reasonably believed to be, accessed and acquired by an unauthorized person; 2) the date range or approximate date range of the breach; 3) a telephone number or toll-free number (if the covered entity does not meet the definition of a small business concern or non-profit organization) that an affected individual may use to inquire about the breach; 4) the toll-free contact telephone number and addresses for a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis; and 5) the toll-free telephone number and Internet website for the FTC where individuals can get more information about identity theft.

A covered entity may contract out its notice obligation as long it is clear that the notice is sent on behalf of the covered entity.

This section requires a service provider to notify a covered entity if it becomes aware of a breach of security involving electronic data containing personal information and can reasonably identify the sender.

Section 4. Enforcement

This section establishes that a violation of this Act will be treated as an unfair or deceptive act or practice under the Federal Trade Commission Act and violations will be enforced by the FTC. Any covered entity that violates this Act shall be subject to the penalties and immunities provided in the Federal Trade Commission Act and as extended by this Act to common carriers and nonprofit organizations. Notwithstanding section 5(m) of the FTC Act, the Commission may impose civil penalties for violations of section 3 in an amount not greater than $1,000 per violation and each failure to send a notification shall be a separate violation.

This section sets a maximum total liability for first-time violations of section 2 resulting from the same related act or omission

at $8,760,000, and for first-time violations of section 3 resulting from the same related act or omission at $17,520,000.

This section allows for State attorneys general to bring enforcement actions for violations of either the security or notification requirements of this draft. They may bring civil penalties of up to $11,000 per violation of section 2 and $1,000 per violation of section 3.

This section establishes a maximum civil penalty of $2.5 million in cases filed by a State attorney general. Civil penalties will be annually adjusted for inflation.

This section requires that the covered entity's degree of culpability, history of prior conduct, ability to pay, effect on ability to continue to do business, and any other matters must be taken into account in determining the amount of a civil penalty.

This section provides certain process requirements so that there is not redundant enforcement between State attorneys general and the FTC.

This section also provides that nothing in this Act establishes a private cause of action against a person for a violation of this Act.

Section 5. Definitions

This section provides definitions for the following terms: breach of security, breached covered entity, Commission, consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, covered entity, data in electronic form, encrypted, non-breached covered entity, non-profit organization, personal information, service provider, small business concern, and State.

Section 6. Effect on other laws

This section prevents States from adopting, maintaining, enforcing, or imposing or continuing in effect any law, rule, regulation, duty, requirement, standard, or other provision related to the security of data in electronic form or notification following a breach of security with respect to a covered entity.

This section would not exempt a covered entity from liability under common law.

This section provides that any regulations in sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 that pertain to information security or breach notification practices of covered entities are superseded by this Act.

This section provides that nothing in this subsection otherwise limits the Federal Communications Commission's authority with respect to sections 201, 202, 222, 338, and 631 of the Communications Act of 1934.

This section also provides that nothing in this Act should be construed in any way to limit or affect the FTC's authority under any other provision of law.

Section 7. Education and outreach for small businesses

This section requires the Commission to conduct education and outreach for small business concerns on data security practices and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such small business concerns.

Section 8. Website on data security best practices

This section requires the Commission to establish and maintain a website with non-binding best practices for businesses regarding data security and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such small businesses.

Section 9. Effective date

This section provides that the Act will take effect one year after the date of enactment of this Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

DISSENTING VIEWS

We agree that there is a need for legislation requiring entities that hold and collect consumer information be required to secure such information and provide notice to consumers in the case of a breach of security of that information. Unfortunately, we cannot support H.R. 1770, the Data Security and Breach Notification Act of 2015, as reported by the Committee on Energy and Commerce on April 15, 2015. This bill does not enhance consumer protections. And it many ways, it puts consumers in a worse place with regard to data security and breach notification than they are today.

Our views on specific provisions in H.R. 1770 and the Committee's consideration of the bill are set forth below.

I. H.R. 1770, AS REPORTED

H.R. 1770 fails to meet the dual purposes of reducing breaches and mitigating their adverse effects. Federal data breach legislation should enhance protections against data breaches and provide consumers with relevant information following a breach. Instead, H.R. 1770 weakens existing consumer protections by preempting often stronger state and territorial data breach laws without an adequate replacement for those provisions.

H.R. 1770 fails to require sufficient protections of consumers' personal information. Robust data security is critical to any data breach bill. Federal legislation cannot be foolproof, but it should be focused on stopping breaches from happening, before consumers' personal information is compromised and before consumers see the negative effects.

H.R. 1770 also fails to provide strong data breach notification to consumers whose data has been subject to a breach. Many of the 51 state and territorial breach notification laws provide greater protections for consumers. Thirty-eight of those state laws require notice of a breach to be provided in more circumstances than H.R. 1770, thereby allowing consumers to prevent harms instead of waiting for harms to occur before taking action. In contrast, H.R. 1770 requires a financial harm analysis before notification is required to be provided to consumers. Consumers should know when their personal information has been hacked, and have the ability to decide whether a breach of their personal information may cause them harm and react as they see fit. Consumers have not reported confusion because of the variation in notice requirements in the state laws.

In addition, H.R. 1770 is narrow in scope, providing a limited and inflexible definition of personal information. Although the bill purports to focus on personal information that leads to financial harms, the definition of personal information does not include some types of personal information that could lead directly to financial harm, such as payroll information. Moreover, it does not cover any

other types of personal information that indirectly lead to financial harm through phishing scams or other fraud schemes. Nor does H.R. 1770 cover the types of personal information that lead to other harms, such as physical or emotional harms. Many state laws that would be preempted by this bill cover broader personal information, such as an individual's medical history or health insurance information. These types of information are not covered by H.R. 1770.

Moreover, H.R. 1770 limits the civil penalties that can be sought by the Federal Trade Commission (FTC) and the state attorneys general in enforcing the provisions of this bill, again limiting consumer protections available under current law. Both the FTC and the state attorneys general need the ability to match the scope of these breaches with adequate penalties. The FTC and state attorneys general should have the flexibility to seek fair penalties that are commensurate with the damage that has been done. This bill caps total fine the FTC can impose for first offenses at $8,760,000 for violations of the security requirements and at $17,520,000 for violations of breach notification requirements. The bill also caps the total fine state attorneys general, collectively, can impose in all cases at $2.5 million of the security requirements and at $2.5 million for violations of breach notification requirements. Under the maximum penalty provision for state attorneys general, therefore, if one state attorney general collects $2.5 million from an entity for a violation of the breach notification provision, no other state attorney general will be permitted to impose a fine at all, even if a breach affected millions of consumers in his or her state.

Further, while this bill provides state attorneys general with the ability to bring civil actions against companies that violate the act, it does not provide that they receive any notification of a breach. There is simply no good reason to delay, and perhaps prevent, the facts of a data breach from reaching state attorneys general, who often have relationships and connections in states that are critical to disseminating information to consumers and businesses quickly. And while the FTC, which also has authority to enforce the provisions of this bill, does receive notification of a breach so that it can respond effectively, it is not notified unless there is a very high threshold of affected consumers.

Finally, H.R. 1770 preempts provisions of the Communications Act regarding telecommunications, cable, and satellite services, as well as the regulations promulgated thereunder, to the extent they apply to information security practices and breach notification. And because data security is inextricably linked to privacy and competition, the ability of the Federal Communications Commission (FCC) to protect consumers in those areas also would be adversely affected. H.R. 1770 only requires the reasonable securing of personal information as the bill defines personal information, i.e., narrowly. The bill then preempts the Communications Act broadly, with regard to all information. Since H.R. 1770's breach notification is exclusively linked to financial harm, notifications currently required under the Communication Act also would become void and unenforceable. The bill moves jurisdiction over these communications services for data security and breach notification from the FCC to the FTC. The FTC has expertise in general data breach issues.

But, as primarily an enforcement agency, the FTC lacks the tools to effectively handle the unique data security, breach notification, and privacy issues of communications services. Under H.R. 1770, these services will no longer be subject to the before-the-fact security and privacy requirements under the Communications Act and its associated regulations. Instead, they will only be subject to after-the-fact enforcement. This system does not adequately protect consumers' valuable communications-related personal information, such as telecommunications subscribers' customer proprietary network information (CPNI), which includes virtually all information about a customer's use of the service, or cable or satellite subscribers' viewing histories.

II. COMMITTEE CONSIDERATION

A. Amendments Offered in Subcommittee

Four amendments were adopted at the Subcommittee markup. A manager's amendment offered by Representatives Burgess and Welch made minor changes to the definition of encryption and made broader an exception to the definition of covered entities for entities subject to GLB. The change to the GLB exception was mostly reversed in the bill considered by the full committee. An amendment offered by Representative Pompeo and Welch established procedures for breached covered entities and non-breached covered entities to provide notice to individuals. The language added by this amendment was also significantly changed in the bill considered by the full committee. Two amendments offered by Representatives Cardenas and Blackburn were adopted at the Subcommittee markup adding sections 7 and 8 to the bill regarding education and outreach for small businesses through the FTC.

In addition, five amendments were offered by other minority members, all of which were voted down along party lines. Representative Clarke offered an amendment to give the FTC rulemaking authority to change the definition of personal information as necessary. Representative Rush offered two amendments to address concerns with the preemption of the Communications Act. The first amendment struck the preemption language entirely. The second amendment was intended to transfer as much enforcement authority from the Federal Communications Commission (FCC) to the FTC as the FCC loses in the underlying bill text. Representative Kennedy offered two amendments intended to address state preemption and the conflict in the common law preemption language.

B. Amendments Offered in Full Committee

On April 14–15, 2015, the full Committee on Energy and Commerce voted in favor of H.R. 1770, the Data Security and Breach Notification Act of 2015, strictly along party lines. Four amendments were adopted at full Committee. An amendment offered by Representative Kinzinger slightly expanded the definition of personal information to include a user name or email address in combination with password or security question and answer. Representative Barton offered an amendment making a minor technical correction to a reference to notification by breached or non-

breached covered entities. Representative Olson offered an amendment that lowered the per-violation fine from $11,000 to $1,000 for a violation of the notice requirements in section 3. The Olson amendment also placed limits on the total penalties for first-time violations of section 2 at $8,760,000 and for first-time violations of section 3 at $17,520,000. These limits on first-time penalties only apply to enforcement by the FTC.

An amendment offered by Representative Blackburn further weakened the consumer protections afforded by this bill. The amendment, among other things, limited the definition of breach of security to relate to information that was accessed and acquired instead of accessed or acquired; added a requirement that a covered entity suffering a breach identify the impact of the breach as part of its required investigation into the breach (which would occur before notice is given to consumers); and changed the requirement that to be considered personal information a name must be connected with all three (not two of three) of the following: (1) home address and telephone number, (2) mother's maiden name, (3) birthday. The Blackburn amendment also made changes to the notification duties that a breached covered entity has with respect to a non-breached covered entity and changed the definition of call information that is considered personal information.

In addition, five amendments were offered by minority members, four of which were voted down along party lines. An amendment in the nature of a substitute offered by Representatives Rush and Schakowsky, which was intended to protect consumers without overburdening businesses, received bipartisan support but failed to get enough votes to be adopted. The amendment would have provided a strong security standard with needed specificity, while ensuring that it is technology-neutral and allows for flexibility for businesses to implement appropriate security procedures. It also would have given the FTC rulemaking authority to flesh out the needed details and allowed those details to change overtime as criminals get more and more creative. This amendment would not have a financial harm trigger for notification to consumers but would have added to the definition of personal information because unauthorized access to all kinds of personal information can harm people whose information is stolen. Additionally, it would have given the FTC authority to change the definition of personal information. This amendment also acknowledges the important role of the states and would have eliminated the limitations on state enforcement that are in the underlying bill by requiring notice to state attorneys general and removing the caps on civil penalties that can be sought by state attorneys general. Moreover, the amendment would have preempted state laws, replacing them with strong security and breach notification standards, to avoid burdening businesses with a 51 law with which they must comply. Furthermore, the amendment would have preserved the FCC's authority to regulate the privacy, data security, and breach notification with regard to telecommunications, satellite, cable, and broadband services.

Representative Eshoo also offered an amendment in the nature of a substitute, which, among other things, would have directed the FTC to promulgate a rule creating security standards consistent

with California state security standards, making the California standards the floor for the nation. The bill would have preempted state breach notification laws that failed to meet the California standards, would have allowed states to innovate by passing stronger state laws. The amendment provides an expanded definition of personal information compared to the underlying bill, including health and medical information. It also eliminates the cap on the ability of state attorneys general to seek civil penalties. It would have ensured notice to consumers of a breach whether or not there is financial harm and gives consumers a private right of action for violations of the security or breach notification requirements. The amendment would have also preserved the FCC's authority to regulate the privacy, data security, and breach notification with regard to telecommunications, satellite, cable, and broadband services.

Representative McNerney offered an amendment that would have provided that in the event of a breach that affects 500 consumers or more, a covered entity must provide notice to the state attorneys general of those states whose resident were affected. Representative Kennedy offered two amendments intended to protect states' abilities to use their unfair and deceptive practices authority and address the conflict in the common law preemption language.

For the reasons stated above, we dissent from the views contained in the Committee's report.

FRANK PALLONE, JR.,
Ranking Member, Committee on Energy and Commerce.
JAN SCHAKOWSKY,
Ranking Member, Subcommittee on Commerce, Manufacturing and Trade.

○