Union Calendar No. 719

114TH CONGRESS
2D SESSION

H. R. 1770

[Report No. 114–908]

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.

IN THE HOUSE OF REPRESENTATIVES

APRIL 14, 2015

Mrs. BLACKBURN (for herself, Mr. WELCH, Mr. BURGESS, and Mr. UPTON) introduced the following bill; which was referred to the Committee on Energy and Commerce

JANUARY 3, 2017

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on April 14, 2015]

A BILL

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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 na-

tionwide 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 sub-

section, 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 nonprofit 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, inter-

mediate 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 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 businesses.

SEC. 9. EFFECTIVE DATE.

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

Union Calendar No. 719

114TH CONGRESS
2D SESSION

H. R. 1770

[Report No. 114–908]

A BILL

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.

JANUARY 3, 2017

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed