I

115TH CONGRESS
1ST SESSION

H. R. 3816

To require notification following a breach of security of a system containing personal information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 21, 2017

Mr. RUSH introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To require notification following a breach of security of a system containing personal 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. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NATIONWIDE NOTIFICATION.—Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information shall, following the discovery of a breach of security of the system maintained by such person that contains such data—

(1) notify each individual who is a citizen or resident of the United States whose personal information was acquired or accessed as a result of such a breach of security;

(2) notify the Commission; and

(3) notify the Bureau.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY AGENTS.—In the event of a breach of security by any third-party entity that has been contracted to maintain or process data in electronic form containing personal information on behalf of any other person who owns or possesses such data, such third-party entity shall be required to notify such person of the breach of security. Upon receiving such notification from such third party, such person shall provide the notification required under subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another person 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 be re-

quired to notify of such a breach of security only the person who initiated such connection, transmission, routing, or storage if such person can be reasonably identified. Upon receiving such notification from a service provider, such person shall provide the notification required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CONSUMER REPORTING AGENCIES.—If a person is required to provide notification to more than 1,000 individuals under subsection (a)(1), the person shall also notify the major consumer reporting agencies of the timing and distribution of the notices. Such notice shall be given to the 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) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) shall be made not later than 30 days following the discovery of a breach of security, unless the person providing notice can show that providing notice within such a timeframe is not feasible due to extraordinary circumstances necessary to prevent further breach or unauthorized disclo-

sures, and reasonably restore the integrity of the data system, in which case such notification shall be made as promptly as possible.

(2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) LAW ENFORCEMENT.—If a Federal, State, or local law enforcement agency determines that the notification required under this section would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for 30 days or such lesser period of time which the law enforcement agency determines is reasonably necessary and requests in writing. A law enforcement 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.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be de-

layed for a period of time which the national security agency or homeland security agency determines is reasonably necessary and requests in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) shall be in compliance with such requirement if the person provides conspicuous and clearly identified notification by one of the following methods (provided the selected method can reasonably be expected to reach the intended individual):

(i) Written notification.

(ii) Notification by email or other electronic means, if—

(I) the person's primary method of communication with the individual

is by email or such other electronic means; or

(II) the individual has consented to receive such notification and the notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A), such notification shall include—

(i) a description of the personal information that was acquired or accessed by an unauthorized person;

(ii) a telephone number that the individual may use, at no cost to such individual, to contact the person to inquire about the breach of security or the information the person maintained about that individual;

(iii) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 5 years, credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 10 years, and instructions to the individual on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(iv) the toll-free contact telephone numbers and addresses for the major consumer reporting agencies;

(v) a toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft; and

(vi) a toll-free telephone number and Internet website address for the Bureau

whereby the individual may obtain information regarding identity theft and credit reports.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) may provide substitute notification in lieu of the direct notification required by paragraph (1) if the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals and such direct notification is not feasible due to—

(i) excessive cost to the person required to provide such notification relative to the resources of such person, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A); or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(1);

(ii) a conspicuous notice on the Internet website of the person (if such person maintains such a website); and

(iii) notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under this paragraph shall include—

(i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individuals, consumer credit reports on a quarterly basis for a period of 5 years, credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 10 years, and instructions on requesting such reports or service from the

person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code; and

(ii) a telephone number by which an individual can, at no cost to such individual, learn whether that individual's personal information is included in the breach of security.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining circumstances under which substitute notification may be provided under paragraph (2), including criteria for determining if notification under paragraph (1) is not feasible due to excessive costs to the person required to provide such notification relative to 5 the resources of such person. Such regulations may also identify other circumstances

where substitute notification would be appropriate for any person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this subsection. Such guidance shall include—

(i) a description of written or email notification that complies with the requirements of paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—A person required to provide notification under subsection (a) shall, upon request of an individual whose personal information was included in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(A) consumer credit reports from at least one of the major consumer reporting agencies

beginning not later than 30 days following the individual's request and continuing on a quarterly basis for a period of 10 years thereafter; or

(B) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 30 days following the individual's request and continuing for a period of 10 years.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (d)(3), the Commission shall determine the circumstances under which a person required to provide notification under subsection (a)(1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(4) BREACH OF CONSUMER REPORTING AGENCY.—In the event of a breach of security of a consumer reporting agency, that agency shall provide

any consumer credit report required under paragraph (1)(A) from another consumer reporting agency.

(f) EXEMPTION.—

(1) GENERAL EXEMPTION.—A person shall be exempt from the requirements under this section if, following a breach of security, such person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTION.—

(A) IN GENERAL.—If the data in electronic form containing personal information is rendered unusable, unreadable, or indecipherable through encryption or other security technology or methodology (if the method of encryption or such other technology or methodology is generally accepted by experts in the information security field), there shall be a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption or other security technologies or methodologies in a specific case, have been or are reasonably likely to be compromised.

(B) METHODOLOGIES OR TECHNOLOGIES.—Not later than 1 year after the date of the enactment of this Act and biannually thereafter, the Commission shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies which render data in electronic form unusable, unreadable, or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such methodology or technology in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

(3) FTC GUIDANCE.—Not later than 1 year after the date of the enactment of this Act the Commission shall issue guidance regarding the application of the exemption in paragraph (1).

(g) WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(2), finds that notification of such a breach of security via the Commission's Internet website would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet website.

(h) WEBSITE NOTICE OF CONSUMER FINANCIAL PROTECTION BUREAU.—If the Bureau, upon receiving notification of any breach of security that is reported to the Bureau under subsection (a)(2), finds that notification of such a breach of security via the Bureau's Internet website would be in the public interest or for the protection of consumers, the Bureau shall place such a notice in a clear and conspicuous location on its Internet website.

(i) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission, in consultation with the Bureau, shall conduct a study on the practicality and cost effectiveness of requiring the notification required by subsection (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(j) GENERAL RULEMAKING AUTHORITY.—The Commission and Bureau may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

(k) TREATMENT OF PERSONS GOVERNED BY OTHER LAW.—A person who is in compliance with any other Federal law that requires such person to provide notification to individuals following a breach of security, and that, taken as a whole, provides protections substantially similar to, or greater than, those required under this section, as the Commission shall determine by rule (under section 553 of title 5, United States Code), shall be deemed to be in compliance with this section.

SEC. 2. APPLICATION AND ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 1 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. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(3) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency 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 person who violates section 1 of this Act, the attorney general, official, or agency 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—

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

(B) to compel compliance with such section; or

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

(2) CIVIL PENALTIES.—

(A) CALCULATION.—For purposes of paragraph (1)(C) with regard to a violation of section 1, 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 $11,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clause (i) of subparagraph (A) 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.

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

(i) $5,000,000 for each violation of section 2; and

(ii) $5,000,000 for all violations of section 3 resulting from a single breach of security.

(3) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—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) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(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) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 1.—

(1) IN GENERAL.—It shall be an affirmative defense to an enforcement action brought under subsection (a), or a civil action brought under subsection (b), based on a violation of section 1, that all of the personal information contained in the data in electronic form that was acquired or accessed as a result of a breach of security of the defendant is public record information that is lawfully made available to the general public from Federal, State, or local government records and was acquired by the defendant from such records.

(2) NO EFFECT ON OTHER REQUIREMENTS.—Nothing in this subsection shall be construed to exempt any person from the requirement to notify the Commission of a breach of security as required under section 3(a).

SEC. 3. PROHIBITION ON CERTAIN CONTRACT CLAUSES.

(a) UNLAWFUL CONDUCT.—It shall be unlawful for any person to include a clause in a contract that—

(1) prohibits an individual described in section (1)(a)(1) from pursuing civil action related to the breach; or

(2) requires mandatory arbitration related to the breach.

(b) VIOLATION OF RULE.—A violation of subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(c) POWERS OF COMMISSION.—The Commission shall enforce this section 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. Any person who violates subsection (a) shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

SEC. 4. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term ''breach of security'' means the unauthorized acquisition of data in electronic form containing personal information.

(2) BUREAU.—The term ''Bureau'' means the Consumer Financial Protection Bureau.

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

(4) CONSUMER REPORTING AGENCY.—The term ''consumer reporting agency'' has the meaning given the term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(5) 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.

(6) ENCRYPTION.—The term ''encryption'' means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management and safeguards of such keys to protect the integrity of the encryption.

(7) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personal information for the purpose of engag-

ing in commercial transactions under the name of such other person.

(8) NON-PUBLIC INFORMATION.—The term ''non-public information'' means information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

(9) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means any information or compilation of information that includes any of the following:

(i) An individual's first name or initial and last name in combination with any or more of the following data elements for that individuals:

(I) Home address or telephone number.

(II) Mother's maiden name.

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

(IV) User name or electronic mail address.

(ii) Driver's license number, passport number, military identification number,

alien registration number, or other similar number issued on a government document used to verify identity.

(iii) Unique account identifier, including a financial account number, credit or debit card number, electronic identification number, user name, or routing code.

(iv) Partial or complete Social Security number.

(v) Unique biometric or genetic data such as a fingerprint, voice print, a retina or iris image, or any other unique physical representations.

(vi) Information that could be used to access an individual's account, such as user name and password or email address and password.

(vii) Any two or more of the following data elements:

(I) An individual's first and last name or first initial and last name.

(II) A unique account identifier, including a financial account number or credit or debit card number, elec-

tronic identification number, user name, or routing code.

(III) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(viii) Information generated or derived from the operation or use of an electronic communications device that is sufficient to identify the street name and name of the city or town in which the device is located.

(ix) Any information regarding an individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional, or the provision of health care to the individual, including health information provided to a website or mobile application.

(x) A health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual, or any information in an individual's health insurance application and claims history, including any appeals records.

(xi) Digitized or other electronic signature.

(xii) Nonpublic communications or other user-created content such as emails, photographs, or videos.

(xiii) Any record or information concerning payroll, income, financial accounts, mortgages, loans, lines of credit, utility bills, accumulated purchases, or any other information regarding financial assets, obligations, or spending habits.

(xiv) Any additional element the Commission defines as personal information.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, modify the definition of ''personal information'' under subparagraph (A).

(10) PUBLIC RECORD INFORMATION.—The term ''public record information'' means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

(11) SERVICE PROVIDER.—The term ''service provider'' means an entity that provides to a user transmission, routing, intermediate and transient storage, or connections to its system or network, for electronic communications, between or among points specified by such user of material of the user's choosing, without modification to the content of the material as sent or received. 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) STATE.—The term ''State'' means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, the Commonwealth of the Northern Mariana Islands, any other territory or possession of the United States, and each federally recognized Indian Tribe.

SEC. 5. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly requires

notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 2(b) may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—This subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) other State laws to the extent that those laws relate to acts of fraud.

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

SEC. 6. EFFECTIVE DATE.

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

SEC. 7. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to the Commission $1,000,000 for each of fiscal years 2018 through 2023 to carry out this Act.

○