AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. ____

OFFERED BY MS. ESHOO OF CALIFORNIA

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Data Security and Breach Notification Act of 2015''.

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations in accordance with section 553 of title 5, United States Code, that contain requirements applicable to covered entities with respect to the security of personal information that are consistent with the requirements of section 1798.81.5 of the California Civil Code (as in effect on the date of the enactment of this Act). In promulgating such regulations, the Commission shall make such modifications to such requirements as are necessary to adapt such requirements for application throughout the United States as a whole.

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations in accordance with section 553 of title 5, United States Code, that contain requirements applicable to covered entities with respect to notification after a breach of security that are consistent with the requirements of section 1798.82 of the California Civil Code (as in effect on the date of the enactment of this Act). In promulgating such regulations, the Commission shall make such modifications to such requirements as are necessary to adapt such requirements for application throughout the United States as a whole.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of the regulations promulgated under 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 the regulations promulgated under

sections 2 and 3 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 such regulations 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 subparagraphs (B) and (C) of section 5(3).

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—If the chief law enforcement officer of a State, or an official or agency designated by a State, has reason to believe that any covered entity has violated or is violating the regulations promulgated under section 2 or 3, the attorney general, official, or agency of the State, in addition to any authority it may have to bring an action in State court under its consumer protection law, may bring a civil action in an appropriate State court or an appropriate district court of the United States to—

(A) enjoin further such violation by the defendant;

(B) enforce compliance with such regulations;

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

(D) obtain damages, restitution, or other compensation on behalf of residents of the State.

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF REGULATIONS UNDER SECTION 2.—For purposes of paragraph (1)(C) with regard to a violation of the regulations promulgated under section 2, 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 regulations by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF REGULATIONS UNDER SECTION 3.—For purposes of paragraph (1)(C) with regard to a violation of the regulations promulgated under section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such regulations by an amount not greater than $11,000. Each failure to send notification as required under such regulations to a resident of the United States 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 clauses (i) and (ii) 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) PRIVATE RIGHT OF ACTION.—

(1) IN GENERAL.—A person injured by an act or practice in violation of the regulations promulgated under section 2 or 3 may bring in an appropriate State court or an appropriate district court of the United States—

(A) an action to enjoin the violation;

(B) an action to recover damages for actual monetary loss from the violation; or

(C) both such actions.

(2) WILLFUL OR KNOWING VIOLATIONS.—If the court finds that the defendant acted willfully or knowingly in committing a violation described in paragraph (1), the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under paragraph (1)(B).

(3) COSTS AND ATTORNEY'S FEES.—The court shall award to a prevailing plaintiff in an action under this subsection the costs of such action and reasonable attorney's fees, as determined by the court.

(4) LIMITATION.—An action may be commenced under this subsection not later than 2 years after the date on which the person first discovered or had a reasonable opportunity to discover the violation.

(5) NONEXCLUSIVE REMEDY.—The remedy provided by this subsection shall be in addition to any other remedies available to the person.

SEC. 5. DEFINITIONS.

In this Act:

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

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

(3) COVERED ENTITY.—The term ''covered entity'' means—

(A) any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture 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));

(B) 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

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of

1986 that is exempt from taxation under section 501(a) of such Code.

(4) 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.

(5) 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.

(6) HEALTH INSURANCE INFORMATION.—The term ‘‘health insurance information’’ means an individual’s health insurance policy number or subscriber identification number, any unique identifier

used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(7) MEDICAL INFORMATION.—The term ''medical information'' means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(8) PERSONAL INFORMATION.—

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

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

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

(II) Any two of the following:

(aa) Home address or telephone number.

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

(cc) 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) For any telecommunications carrier or interconnected VoIP provider, the location of, number from which and to which a call is placed, and the time and duration of such call.

(vi) Health insurance information.

(vii) Medical information.

(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.

(9) 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).

(10) 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. RELATIONSHIP TO OTHER LAW.

(a) EFFECT ON STATE BREACH NOTIFICATION LAWS.—A covered entity that is in compliance with the regulations promulgated under section 3 shall be deemed to have provided appropriate notice as required by any State law that requires notification to individuals in the event of a breach of security of personal information.

(b) EFFECT ON OTHER STATE LAWS.—Nothing in this Act shall be construed to—

(1) preempt or limit any provision of any other law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, including any State consumer protection law, any State law relating to acts of fraud or deception, and any State trespass, contract, or tort law;

(2) prevent or limit the attorney general of a State from exercising the powers conferred upon the attorney general by the laws of the State, including

conducting investigations, administering oaths or affirmations, or compelling the attendance of witnesses or the production of documentary and other evidence; or

(3) preempt or limit any provision of any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State with respect to any person that is not a covered entity.

(c) RELATIONSHIP TO OTHER FEDERAL LAW.—A covered entity that is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a breach of security shall be deemed to be in compliance with the regulations promulgated under section 3 with respect to activities and information covered under such Federal law.

(d) PRESERVATION OF AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the authority under any other provision of law of the Commission, the Federal Communications Commission, or the Consumer Financial Protection Bureau.

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.

⊠