

**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:

**1 SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Data Security and  
3 Breach Notification Act of 2015”.

**4 SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.**

5       Not later than 1 year after the date of the enactment  
6 of this Act, the Commission shall promulgate regulations  
7 in accordance with section 553 of title 5, United States  
8 Code, that contain requirements applicable to covered en-  
9 tities with respect to the security of personal information  
10 that are consistent with the requirements of section  
11 1798.81.5 of the California Civil Code (as in effect on the  
12 date of the enactment of this Act). In promulgating such  
13 regulations, the Commission shall make such modifica-  
14 tions to such requirements as are necessary to adapt such  
15 requirements for application throughout the United States  
16 as a whole.

1 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
2 **BREACH.**

3 Not later than 1 year after the date of the enactment  
4 of this Act, the Commission shall promulgate regulations  
5 in accordance with section 553 of title 5, United States  
6 Code, that contain requirements applicable to covered en-  
7 tities with respect to notification after a breach of security  
8 that are consistent with the requirements of section  
9 1798.82 of the California Civil Code (as in effect on the  
10 date of the enactment of this Act). In promulgating such  
11 regulations, the Commission shall make such modifica-  
12 tions to such requirements as are necessary to adapt such  
13 requirements for application throughout the United States  
14 as a whole.

15 **SEC. 4. ENFORCEMENT.**

16 (a) **ENFORCEMENT BY THE FEDERAL TRADE COM-**  
17 **MISSION.—**

18 (1) **UNFAIR OR DECEPTIVE ACTS OR PRAC-**  
19 **TICES.—**A violation of the regulations promulgated  
20 under section 2 or 3 shall be treated as an unfair  
21 and deceptive act or practice in violation of a regula-  
22 tion under section 18(a)(1)(B) of the Federal Trade  
23 Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding  
24 unfair or deceptive acts or practices.

25 (2) **POWERS OF COMMISSION.—**The Commis-  
26 sion shall enforce the regulations promulgated under

1 sections 2 and 3 in the same manner, by the same  
2 means, and with the same jurisdiction, powers, and  
3 duties as though all applicable terms and provisions  
4 of the Federal Trade Commission Act (15 U.S.C. 41  
5 et seq.) were incorporated into and made a part of  
6 this Act, and any covered entity who violates such  
7 regulations shall be subject to the penalties and enti-  
8 tled to the privileges and immunities provided in the  
9 Federal Trade Commission Act (15 U.S.C. 41 et  
10 seq.), and as provided in subparagraphs (B) and (C)  
11 of section 5(3).

12 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
13 ERAL.—

14 (1) IN GENERAL.—If the chief law enforcement  
15 officer of a State, or an official or agency designated  
16 by a State, has reason to believe that any covered  
17 entity has violated or is violating the regulations  
18 promulgated under section 2 or 3, the attorney gen-  
19 eral, official, or agency of the State, in addition to  
20 any authority it may have to bring an action in  
21 State court under its consumer protection law, may  
22 bring a civil action in an appropriate State court or  
23 an appropriate district court of the United States  
24 to—

1 (A) enjoin further such violation by the de-  
2 fendant;

3 (B) enforce compliance with such regula-  
4 tions;

5 (C) obtain civil penalties in the amount de-  
6 termined under paragraph (2); or

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

10 (2) CIVIL PENALTIES.—

11 (A) CALCULATION.—

12 (i) TREATMENT OF VIOLATIONS OF  
13 REGULATIONS UNDER SECTION 2.—For  
14 purposes of paragraph (1)(C) with regard  
15 to a violation of the regulations promul-  
16 gated under section 2, the amount deter-  
17 mined under this paragraph is the amount  
18 calculated by multiplying the number of  
19 days that a covered entity is not in compli-  
20 ance with such regulations by an amount  
21 not greater than \$11,000.

22 (ii) TREATMENT OF VIOLATIONS OF  
23 REGULATIONS UNDER SECTION 3.—For  
24 purposes of paragraph (1)(C) with regard  
25 to a violation of the regulations promul-

1 gated under section 3, the amount deter-  
2 mined under this paragraph is the amount  
3 calculated by multiplying the number of  
4 violations of such regulations by an  
5 amount not greater than \$11,000. Each  
6 failure to send notification as required  
7 under such regulations to a resident of the  
8 United States shall be treated as a sepa-  
9 rate violation.

10 (B) ADJUSTMENT FOR INFLATION.—Be-  
11 ginning on the date that the Consumer Price  
12 Index is first published by the Bureau of Labor  
13 Statistics that is after 1 year after the date of  
14 enactment of this Act, and each year thereafter,  
15 the amounts specified in clauses (i) and (ii) of  
16 subparagraph (A) shall be increased by the per-  
17 centage increase in the Consumer Price Index  
18 published on that date from the Consumer  
19 Price Index published the previous year.

20 (c) PRIVATE RIGHT OF ACTION.—

21 (1) IN GENERAL.—A person injured by an act  
22 or practice in violation of the regulations promul-  
23 gated under section 2 or 3 may bring in an appro-  
24 priate State court or an appropriate district court of  
25 the United States—

- 1 (A) an action to enjoin the violation;  
2 (B) an action to recover damages for ac-  
3 tual monetary loss from the violation; or  
4 (C) both such actions.

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

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

17 (4) LIMITATION.—An action may be com-  
18 menced under this subsection not later than 2 years  
19 after the date on which the person first discovered  
20 or had a reasonable opportunity to discover the vio-  
21 lation.

22 (5) NONEXCLUSIVE REMEDY.—The remedy pro-  
23 vided by this subsection shall be in addition to any  
24 other remedies available to the person.

1 **SEC. 5. DEFINITIONS.**

2 In this Act:

3 (1) **BREACH OF SECURITY.**—The term “breach  
4 of security” means unauthorized access to, acquisi-  
5 tion of, or use of data in electronic form containing  
6 personal information.

7 (2) **COMMISSION.**—The term “Commission”  
8 means the Federal Trade Commission.

9 (3) **COVERED ENTITY.**—The term “covered en-  
10 tity” means—

11 (A) any organization, corporation, trust,  
12 partnership, sole proprietorship, unincorporated  
13 association, or venture over which the Commis-  
14 sion has authority pursuant to section 5(a)(2)  
15 of the Federal Trade Commission Act (15  
16 U.S.C. 45(a)(2));

17 (B) notwithstanding section 5(a)(2) of the  
18 Federal Trade Commission Act (15 U.S.C.  
19 45(a)(2)), common carriers subject to the Com-  
20 munications Act of 1934 (47 U.S.C. 151 et  
21 seq.); and

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

1           1986 that is exempt from taxation under sec-  
2           tion 501(a) of such Code.

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

8           (5) ENCRYPTED.—The term “encrypted”, used  
9           with respect to data in electronic form, in storage or  
10          in transit—

11           (A) means the data is protected using an  
12           encryption technology that has been generally  
13           accepted by experts in the field of information  
14           security at the time the breach of security oc-  
15           curred that renders such data indecipherable in  
16           the absence of associated cryptographic keys  
17           necessary to enable decryption of such data;  
18           and

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

22           (6) HEALTH INSURANCE INFORMATION.—The  
23           term “health insurance information” means an indi-  
24           vidual’s health insurance policy number or sub-  
25           scriber identification number, any unique identifier



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

4           (7) MEDICAL INFORMATION.—The term “med-  
5       ical information” means any information regarding  
6       an individual's medical history, mental or physical  
7       condition, or medical treatment or diagnosis by a  
8       health care professional.

9           (8) PERSONAL INFORMATION.—

10           (A) IN GENERAL.—The term “personal in-  
11       formation” means any information or compila-  
12       tion of information that includes the following:

13           (i) An individual's first and last name  
14       or first initial and last name in combina-  
15       tion with any one of the following data ele-  
16       ments:

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

21           (II) Any two of the following:

22           (aa) Home address or tele-  
23       phone number.

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

1 (cc) Month, day, and year of  
2 birth.

3 (ii) A financial account number or  
4 credit or debit card number or other iden-  
5 tifier, in combination with any security  
6 code, access code, or password that is re-  
7 quired for an individual to obtain credit,  
8 withdraw funds, or engage in a financial  
9 transaction.

10 (iii) A unique account identifier (other  
11 than for an account described in clause  
12 (ii)), electronic identification number, bio-  
13 metric data unique to an individual, user  
14 name, or routing code in combination with  
15 any associated security code, access code,  
16 biometric data unique to an individual, or  
17 password that is required for an individual  
18 to obtain money, or purchase goods, serv-  
19 ices, or any other thing of value.

20 (iv) A non-truncated social security  
21 number.

22 (v) For any telecommunications car-  
23 rier or interconnected VoIP provider, the  
24 location of, number from which and to

1 which a call is placed, and the time and  
2 duration of such call.

3 (vi) Health insurance information.

4 (vii) Medical information.

5 (B) EXCEPTIONS.—The term “personal in-  
6 formation” does not include—

7 (i) information that is encrypted or  
8 rendered unusable, unreadable, or indeci-  
9 pherable through data security technology  
10 or methodology that is generally accepted  
11 by experts in the field of information secu-  
12 rity at the time the breach of security oc-  
13 curred, such as redaction or access con-  
14 trols; or

15 (ii) information available in a publicly  
16 available source, including information ob-  
17 tained from a news report, periodical, or  
18 other widely distributed media, or from  
19 Federal, State, or local government  
20 records.

21 (9) SMALL BUSINESS CONCERN.—The term  
22 “small business concern” has the meaning given  
23 such term under section 3 of the Small Business Act  
24 (15 U.S.C. 632).

1           (10) STATE.—The term “State” means each of  
2       the several States, the District of Columbia, the  
3       Commonwealth of Puerto Rico, Guam, American  
4       Samoa, the Virgin Islands of the United States, the  
5       Commonwealth of the Northern Mariana Islands,  
6       any other territory or possession of the United  
7       States, and each federally recognized Indian tribe.

8   **SEC. 6. RELATIONSHIP TO OTHER LAW.**

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

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

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

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

1 conducting investigations, administering oaths or af-  
2 firmations, or compelling the attendance of witnesses  
3 or the production of documentary and other evi-  
4 dence; or

5 (3) preempt or limit any provision of any law,  
6 rule, regulation, requirement, standard, or other pro-  
7 vision having the force and effect of law of any State  
8 with respect to any person that is not a covered enti-  
9 ty.

10 (c) RELATIONSHIP TO OTHER FEDERAL LAW.—A  
11 covered entity that is in compliance with any other Federal  
12 law that requires such covered entity to provide notifica-  
13 tion to individuals following a breach of security shall be  
14 deemed to be in compliance with the regulations promul-  
15 gated under section 3 with respect to activities and infor-  
16 mation covered under such Federal law.

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

22 **SEC. 7. EDUCATION AND OUTREACH FOR SMALL BUSI-**  
23 **NESSES.**

24 The Commission shall conduct education and out-  
25 reach for small business concerns on data security prac-

1 tices and how to prevent hacking and other unauthorized  
2 access to, acquisition of, or use of data maintained by such  
3 small business concerns.

4 **SEC. 8. WEBSITE ON DATA SECURITY BEST PRACTICES.**

5 The Commission shall establish and maintain an  
6 Internet website containing non-binding best practices for  
7 businesses regarding data security and how to prevent  
8 hacking and other unauthorized access to, acquisition of,  
9 or use of data maintained by such businesses.

10 **SEC. 9. EFFECTIVE DATE.**

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

