

**[DISCUSSION DRAFT]**

MARCH 12, 2015

114TH CONGRESS  
1ST SESSION**H. R.** \_\_\_\_\_

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**

\_\_\_\_\_ introduced the following bill; which was referred to the  
Committee on \_\_\_\_\_

---

**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.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE; PURPOSES.**

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

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

2 (1) protect consumers from identity theft, eco-  
3 nomic loss or economic harm, and financial fraud by  
4 establishing strong and uniform national data secu-  
5 rity and breach notification standards for electronic  
6 data in interstate commerce while minimizing State  
7 law burdens that may substantially affect interstate  
8 commerce; and

9 (2) expressly preempt any related State laws  
10 [and common law] to ensure uniformity of this  
11 Act's standards and the consistency of their applica-  
12 tion across jurisdictions.

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

14 A covered entity shall implement and maintain rea-  
15 sonable security measures and practices to protect and se-  
16 cure personal information in electronic form against unau-  
17 thorized access as appropriate for the size and complexity  
18 of such covered entity and the nature and scope of its ac-  
19 tivities.

20 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
21 **BREACH.**

22 (a) IN GENERAL.—

23 (1) IN GENERAL.—Except as otherwise pro-  
24 vided by this section, a covered entity that uses, ac-  
25 cesses, transmits, stores, disposes of, or collects per-

1       sonal information shall, following the discovery of a  
2       breach of security, conduct in good faith a reason-  
3       able and prompt investigation of the breach of secu-  
4       rity to determine whether there is a reasonable risk  
5       that the breach of security has resulted in, or will  
6       result in, identity theft, economic loss or economic  
7       harm, or financial fraud to the individuals whose  
8       personal information was subject to the breach of se-  
9       curity.

10       (2) NOTICE.—Unless there is no reasonable  
11       risk that the breach of security has resulted in, or  
12       will result in, identity theft, economic loss or eco-  
13       nomic harm, or financial fraud to the individuals  
14       whose personal information was subject to the  
15       breach of security, the covered entity shall notify any  
16       resident of the United States that has been affected  
17       by, or is reasonably believed to have been affected  
18       by, the breach of security within the time specified  
19       in subsection (c).

20       (3) LAW ENFORCEMENT.—A covered entity  
21       shall as expeditiously as possible notify the Commis-  
22       sion and the Secret Service or the Federal Bureau  
23       of Investigation of the fact that a breach of security  
24       has occurred if the number of individuals whose per-  
25       sonal information was, or there is a reasonable basis

1 to conclude was, accessed or acquired by an unau-  
2 thorized person exceeds 10,000.

3 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

4 (1) THIRD-PARTY ENTITIES.—

5 (A) IN GENERAL.—In the event of a  
6 breach of security involving personal informa-  
7 tion that is stored, processed, or maintained by  
8 a third-party entity for a covered entity, such  
9 third-party entity shall promptly notify such  
10 covered entity of the personal information that  
11 was breached. If a covered entity is acting sole-  
12 ly as a third-party entity for purposes of this  
13 paragraph, the third-party entity has no other  
14 notification obligations under this section.

15 (B) COVERED ENTITIES WHO RECEIVE NO-  
16 TICE FROM THIRD-PARTY ENTITIES.—Upon re-  
17 ceiving notification from a third-party entity  
18 under subparagraph (A), a covered entity shall  
19 provide notification as required under sub-  
20 section (a), unless it is agreed in writing that  
21 the third-party entity will provide such notifica-  
22 tion on behalf of the covered entity subject to  
23 the requirements of subsection (d)(3).

24 (C) EXCEPTION FOR SERVICE PRO-  
25 VIDERS.—A service provider shall not be consid-

1           ered a third-party entity for purposes of this  
2           paragraph.

3           (2) NON-PROFIT ORGANIZATIONS.—In the event  
4           of a breach of security involving personal informa-  
5           tion that would trigger notification under subsection  
6           (a), a non-profit organization may complete such no-  
7           tification according to the procedures set forth in  
8           subsection (d)(2).

9           (3) COORDINATION OF NOTIFICATION WITH  
10          CONSUMER REPORTING AGENCIES.—If a covered en-  
11          tity is required to provide notification to more than  
12          10,000 individuals under subsection (a), such cov-  
13          ered entity shall also notify a consumer reporting  
14          agency that compiles and maintains files on con-  
15          sumers on a nationwide basis, of the timing and dis-  
16          tribution of the notices. Such notice shall be given  
17          to such consumer reporting agencies without unrea-  
18          sonable delay and, if it will not delay notice to the  
19          affected individuals, prior to the distribution of no-  
20          tices to the affected individuals.

21          (c) TIMELINESS OF NOTIFICATION.—

22               (1) IN GENERAL.—Unless subject to a delay au-  
23               thorized under paragraph (2), a covered entity shall  
24               identify the individuals affected by a breach of secu-  
25               rity and make the notification required under sub-

1 section (a) as expeditiously as possible and without  
2 unreasonable delay, not later than 30 days after  
3 such covered entity has taken the necessary meas-  
4 ures to determine the scope of the breach of security  
5 and restore the reasonable integrity, security, and  
6 confidentiality of the data system. If a covered entity  
7 has provided the notification to individuals required  
8 under subsection (a) and after such notification dis-  
9 covers additional individuals to whom notification is  
10 required under such subsection with respect to the  
11 same breach of security, the covered entity shall  
12 make such notification to such individuals as expedi-  
13 tiously as possible and without unreasonable delay.

14 (2) DELAY OF NOTIFICATION AUTHORIZED FOR  
15 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-  
16 POSES.—Notwithstanding paragraph (1), if a Fed-  
17 eral, State, or local law enforcement agency deter-  
18 mines that the notification to individuals required  
19 under this section would impede a civil or criminal  
20 investigation or a Federal agency determines that  
21 such notification would threaten national security,  
22 such notification shall be delayed upon written re-  
23 quest of the law enforcement agency or Federal  
24 agency which the law enforcement agency or Federal  
25 agency determines is reasonably necessary and re-

1        requests in writing. A law enforcement agency or Fed-  
2        eral agency may, by a subsequent written request,  
3        revoke such delay or extend the period of time set  
4        forth in the original request made under this para-  
5        graph if further delay is necessary. If a law enforce-  
6        ment agency or Federal agency requests a delay of  
7        notification to individuals under this paragraph, the  
8        Commission shall, upon written request of the law  
9        enforcement agency or Federal agency, delay any  
10       public disclosure of a notification received by the  
11       Commission under this section relating to the same  
12       breach of security until the delay of notification to  
13       individuals is no longer in effect.

14       (d) METHOD AND CONTENT OF NOTIFICATION.—

15                (1) DIRECT NOTIFICATION.—

16                        (A) METHOD OF NOTIFICATION.—A cov-  
17        ered entity required to provide notification to  
18        an individual under subsection (a) shall be in  
19        compliance with such requirement if the covered  
20        entity provides such notice by one of the fol-  
21        lowing methods (if the selected method can rea-  
22        sonably be expected to reach the intended indi-  
23        vidual):

24                        (i) Written notification by postal mail.

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

(I) 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; and

[(II) the email or other electronic means does not contain a hyperlink.]

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

(ii) 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.



1 (iii) A telephone number, or toll-free  
2 telephone number for any covered entity  
3 that does not meet the definition of a small  
4 business concern or non-profit organiza-  
5 tion, that the individual may use to contact  
6 the covered entity to inquire about the  
7 breach of security or the information the  
8 covered entity maintained about that indi-  
9 vidual.

10 (iv) The toll-free contact telephone  
11 numbers and addresses for a consumer re-  
12 porting agency that compiles and main-  
13 tains files on consumers on a nationwide  
14 basis.

15 (v) The toll-free telephone number  
16 and Internet website address for the Com-  
17 mission whereby the individual may obtain  
18 information regarding identity theft.

19 (2) SUBSTITUTE NOTIFICATION.—

20 (A) IN GENERAL.—If, after making rea-  
21 sonable efforts to contact all individuals to  
22 whom notice is required under subsection (a),  
23 the covered entity finds that contact informa-  
24 tion for 500 or more individuals is insufficient  
25 or out-of-date, the covered entity shall also pro-

1       vide substitute notice to those individuals,  
2       which shall be reasonably calculated to reach  
3       the individuals affected by the breach of secu-  
4       rity.

5               (B) FORM OF SUBSTITUTE NOTIFICA-  
6       TION.—A covered entity may provide substitute  
7       notification by—

8               (i) email or other electronic notifica-  
9       tion to the extent that the covered entity  
10      has contact information for individuals to  
11      whom it is required to provide notification  
12      under subsection (a) [and provided such  
13      email or electronic means does not contain  
14      a hyperlink]; and

15              (ii) a conspicuous notice on the cov-  
16      ered entity's Internet website (if such cov-  
17      ered entity maintains such a website) for  
18      at least 90 days.

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

23              (3) DIRECT NOTIFICATION BY A THIRD  
24      PARTY.—Nothing in this Act shall be construed to  
25      prevent a covered entity from contracting with a

1 third party to provide the notification required under  
2 this section, provided such third party issues such  
3 notification without unreasonable delay, in accord-  
4 ance with the requirements of this section, and indi-  
5 cates to all individuals in such notification that such  
6 third party is sending such notification on behalf of  
7 the covered entity.

8 (e) REQUIREMENTS OF SERVICE PROVIDERS.—

9 (1) IN GENERAL.—If a service provider becomes  
10 aware of a breach of security involving data in elec-  
11 tronic form containing personal information that is  
12 owned or licensed by a covered entity that connects  
13 to or uses a system or network provided by the serv-  
14 ice provider for the purpose of transmitting, routing,  
15 or providing intermediate or transient storage of  
16 such data, such service provider shall notify the cov-  
17 ered entity who initiated such connection, trans-  
18 mission, routing, or storage of the data containing  
19 personal information breached, if such covered entity  
20 can be reasonably identified. If a service provider is  
21 acting solely as a service provider for purposes of  
22 this subsection, the service provider has no other no-  
23 tification obligations under this section.

24 (2) COVERED ENTITIES WHO RECEIVE NOTICE  
25 FROM SERVICE PROVIDERS.—Upon receiving notifi-

1 cation from a service provider under paragraph (1),  
2 a covered entity shall provide notification as required  
3 under this section.

4 **SEC. 4. ENFORCEMENT.**

5 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-  
6 MISSION.—

7 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
8 TICES.—A violation of section 2 or 3 shall be treated  
9 as an unfair and deceptive act or practice in viola-  
10 tion of a regulation under section 18(a)(1)(B) of the  
11 Federal Trade Commission Act (15 U.S.C.  
12 57a(a)(1)(B)) regarding unfair or deceptive acts or  
13 practices.

14 (2) POWERS OF COMMISSION.—The Commis-  
15 sion shall enforce this Act in the same manner, by  
16 the same means, and with the same jurisdiction,  
17 powers, and duties as though all applicable terms  
18 and provisions of the Federal Trade Commission Act  
19 (15 U.S.C. 41 et seq.) were incorporated into and  
20 made a part of this Act, and any covered entity who  
21 violates this Act shall be subject to the penalties and  
22 entitled to the privileges and immunities provided in  
23 the Federal Trade Commission Act (15 U.S.C. 41 et  
24 seq.), and as provided in clauses (ii) and (iii) of sec-  
25 tion 5(4)(A).

1 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
2 ERAL.—

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

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

14 (B) compel compliance with such section;  
15 or

16 (C) obtain civil penalties in the amount de-  
17 termined under paragraph (2).

18 (2) CIVIL PENALTIES.—

19 (A) CALCULATION.—

20 (i) TREATMENT OF VIOLATIONS OF  
21 SECTION 2.—For purposes of paragraph  
22 (1)(C) with regard to a violation of section  
23 2, the amount determined under this para-  
24 graph is the amount calculated by multi-  
25 plying 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 \$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) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection shall not exceed—

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

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

1 (C) ADJUSTMENT FOR INFLATION.—Be-  
2 ginning on the date that the Consumer Price  
3 Index is first published by the Bureau of Labor  
4 Statistics that is after one year after the date  
5 of enactment of this Act, and each year there-  
6 after, the amounts specified in clauses (i) and  
7 (ii) of subparagraph (A) and clauses (i) and (ii)  
8 of subparagraph (B) shall be increased by the  
9 percentage increase in the Consumer Price  
10 Index published on that date from the Con-  
11 sumer Price Index published the previous year.

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

18 (3) INTERVENTION BY THE FEDERAL TRADE  
19 COMMISSION.—

20 (A) NOTICE AND INTERVENTION.—In all  
21 cases, the State shall provide prior written no-  
22 tice of any action under paragraph (1) to the  
23 Commission and provide the Commission with a  
24 copy of its complaint, except in any case in  
25 which such prior notice is not feasible, in which

1 case the State shall serve such notice imme-  
2 diately upon instituting such action. The Com-  
3 mission shall have the right—

4 (i) to intervene in the action;

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

7 (iii) to file petitions for appeal.

8 (B) PENDING PROCEEDINGS.—If the Fed-  
9 eral Trade Commission initiates a Federal civil  
10 action for a violation of this Act, no State at-  
11 torney general may bring an action for a viola-  
12 tion of this Act that resulted from the same or  
13 related acts or omissions against a defendant  
14 named in the civil action initiated by the Fed-  
15 eral Trade Commission.

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

22 (A) conduct investigations;

23 (B) administer oaths or affirmations; or



1 (C) compel the attendance of witnesses or  
2 the production of documentary and other evi-  
3 dence.

4 (c) NO PRIVATE CAUSE OF ACTION.—Nothing in this  
5 Act shall be construed to establish a private cause of ac-  
6 tion against a person for a violation of this Act.

7 **SEC. 5. DEFINITIONS.**

8 In this Act:

9 (1) BREACH OF SECURITY.—The term “breach  
10 of security” means a compromise of the security,  
11 confidentiality, or integrity of, or loss of, data in  
12 electronic form that results in, or there is a reason-  
13 able basis to conclude has resulted in, unauthorized  
14 access to or acquisition of personal information from  
15 a covered entity.

16 (2) COMMISSION.—The term “Commission”  
17 means the Federal Trade Commission.

18 (3) CONSUMER REPORTING AGENCY THAT COM-  
19 PILES AND MAINTAINS FILES ON CONSUMERS ON A  
20 NATIONWIDE BASIS.—The term “consumer reporting  
21 agency that compiles and maintains files on con-  
22 sumers on a nationwide basis” has the meaning  
23 given that term in section 603(p) of the Fair Credit  
24 Reporting Act (15 U.S.C. 1681a(p)).

25 (4) COVERED ENTITY.—

1 (A) IN GENERAL.—The term “covered en-  
2 tity” means—

3 (i) a sole proprietorship, partnership,  
4 corporation, trust, estate, cooperative, as-  
5 sociation, or other entity in or affecting  
6 commerce that acquires, maintains, stores,  
7 sells, or otherwise uses data in electronic  
8 form that includes personal information,  
9 over which the Commission has authority  
10 pursuant to section 5(a)(2) of the Federal  
11 Trade Commission Act (15 U.S.C.  
12 45(a)(2));

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

18 (iii) notwithstanding any jurisdictional  
19 limitation of the Federal Trade Commis-  
20 sion Act (15 U.S.C. 41 et seq.), any non-  
21 profit organization.

22 (B) EXCEPTIONS.—The term “covered en-  
23 tity” does not include—

1 (i) a covered entity, as defined in sec-  
2 tion 160.103 of title 45, Code of Federal  
3 Regulations; or

4 (ii) a broker, dealer, investment com-  
5 pany, investment adviser, or person en-  
6 gaged in providing insurance that is sub-  
7 ject to title V of Public Law 106–102 (15  
8 U.S.C. 6801 et seq.).

9 (5) DATA IN ELECTRONIC FORM.—The term  
10 “data in electronic form” means any data stored  
11 electronically or digitally on any computer system or  
12 other database and includes recordable tapes and  
13 other mass storage devices.

14 (6) ENCRYPTION.—The term “encryption”—  
15 (A) means the protection of data in elec-  
16 tronic form, in storage or in transit, using an  
17 encryption technology that has been generally  
18 accepted by experts in the field of information  
19 security at the time the breach of security oc-  
20 curred that renders such data indecipherable in  
21 the absence of associated cryptographic keys  
22 necessary to enable decryption of such data;  
23 and

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

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

9 (8) PERSONAL INFORMATION.—

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

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

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

22 (II) Any two of the following:

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

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

3 (cc) Month, day, and year of  
4 birth.

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

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

22 (iv) A non-truncated social security  
23 number.

24 (v) [For any telecommunications car-  
25 rier or interconnected VoIP provider, the

1 location of, number from which and to  
2 which a call is placed, and the time and  
3 duration of such call.】

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

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

14 (ii) information obtained from a pub-  
15 licly available source, including information  
16 obtained from a news report, periodical, or  
17 other widely distributed media, or from  
18 Federal, State, or local government  
19 records.

20 (9) SERVICE PROVIDER.—The term “service  
21 provider” means a covered entity subject to the  
22 Communications Act of 1934 (47 U.S.C. 151 et  
23 seq.) that provides electronic data transmission,  
24 routing, intermediate and transient storage, or con-  
25 nection to its system or network, where such entity

1 providing such service does not select or modify the  
2 content of the electronic data, is not the sender or  
3 the intended recipient of the data, and does not dif-  
4 ferentiate personal information from other informa-  
5 tion that such entity transmits, routes, stores, or for  
6 which such entity provides connections. Any such en-  
7 tity shall be treated as a service provider under this  
8 Act only to the extent that it is engaged in the pro-  
9 vision of such transmission, routing, intermediate  
10 and transient storage, or connections.

11 (10) SMALL BUSINESS CONCERN.—The term  
12 “small business concern” has the meaning given  
13 such term under section 3 of the Small Business Act  
14 (15 U.S.C. 632).

15 (11) STATE.—The term “State” means each of  
16 the several States, the District of Columbia, the  
17 Commonwealth of Puerto Rico, Guam, American  
18 Samoa, the Virgin Islands of the United States, the  
19 Commonwealth of the Northern Mariana Islands,  
20 any other territory or possession of the United  
21 States, and each federally recognized Indian tribe.

22 **SEC. 6. EFFECT ON OTHER LAWS.**

23 (a) PREEMPTION OF STATE INFORMATION SECURITY  
24 LAWS.—No State or political subdivision of a State shall,  
25 with respect to a covered entity subject to this Act, adopt,

1 maintain, enforce, or impose or continue in effect any law,  
2 rule, regulation, duty, requirement, standard, or other  
3 provision having the force and effect of law relating to or  
4 with respect to the security of data in electronic form or  
5 notification following a breach of security.

6       **[(b) COMMON LAW.—**This section shall not exempt  
7 a covered entity from liability under common law. **【***The*  
8 *parties to this staff draft have not yet reached agreement*  
9 *on the scope of preemption and continue to discuss the*  
10 *issue.***】**

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

13           **(1) DATA SECURITY AND BREACH NOTIFICA-**  
14 **TION.—**Insofar as sections 201, 202, 222, 338, and  
15 631 of the Communications Act of 1934 (47 U.S.C.  
16 201, 202, 222, 338, and 551), and any regulations  
17 promulgated thereunder, apply to covered entities  
18 with respect to securing information in electronic  
19 form from unauthorized access, including notifica-  
20 tion of unauthorized access to data in electronic  
21 form containing personal information, such sections  
22 and regulations promulgated thereunder shall have  
23 no force or effect, unless such regulations pertain  
24 solely to 9-1-1 calls.



1           (2) RULE OF CONSTRUCTION.—【Nothing in  
2       this subsection otherwise limits the Federal Commu-  
3       nications Commission’s authority with respect to  
4       sections 201, 202, 222, 338, and 631 of the Com-  
5       munications Act of 1934 (47 U.S.C. 201, 202, 222,  
6       338, and 551).】

7       (d) PRESERVATION OF COMMISSION AUTHORITY.—  
8       Nothing in this Act may be construed in any way to limit  
9       or affect the Commission’s authority under any other pro-  
10      vision of law.

11   **SEC. 7. EFFECTIVE DATE.**

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