

.....
(Original Signature of Member)

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

Mrs. BLACKBURN (for herself, Mr. WELCH, Mr. BURGESS, and Mr. LOEBSACK) 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 to
10 ensure uniformity of this Act's standards and the
11 consistency of their application across jurisdictions.

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

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

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

21 (a) IN GENERAL.—

22 (1) RESTORING SECURITY.—Except as other-
23 wise provided by this section, a covered entity that
24 uses, accesses, transmits, stores, disposes of, or col-
25 lects personal information shall, following the dis-

1 covery of a breach of security restore the reasonable
2 integrity, security, and confidentiality of the data
3 system.

4 (2) INVESTIGATION.—A covered entity or
5 breached covered entity shall conduct in good faith
6 a reasonable and prompt investigation of the breach
7 of security to determine whether there is a reason-
8 able risk that the breach of security has resulted in,
9 or will result in, identity theft, economic loss or eco-
10 nomic harm, or financial fraud to the individuals
11 whose personal information was subject to the
12 breach of security.

13 (3) NOTIFICATION TO INDIVIDUALS RE-
14 QUIRED.—Unless there is no reasonable risk that
15 the breach of security has resulted in, or will result
16 in, identity theft, economic loss or economic harm,
17 or financial fraud to the individuals whose personal
18 information was affected by the breach of security,
19 the covered entity, breached covered entity, or non-
20 breached covered entity, as the case may be, shall
21 notify any resident of the United States that has
22 been affected by the breach of security within the
23 time specified in subsection (c).

24 (4) NON-BREACHED COVERED ENTITY ELEC-
25 TION NOTICE.—

1 (A) NOTICE TO NON-BREACHED COVERED
2 ENTITY REQUIRED.—Subject to the require-
3 ments of this paragraph, in the event of a
4 breach of security that presents a reasonable
5 risk that the breach of security has resulted in,
6 or will result in, identity theft, economic loss or
7 economic harm, or financial fraud to individuals
8 whose personal information or record is de-
9 scribed in the notice provided under this para-
10 graph the breached covered entity shall, as ex-
11 peditiously as possible and without unreason-
12 able delay within 10 days after fulfilling the re-
13 quirements described in paragraph (1), notify
14 in writing each non-breached covered entity of
15 the breach of security.

16 (B) CONTENTS OF NOTICE.—The breached
17 covered entity shall include in the notice de-
18 scribed in subparagraph (A)—

19 (i) the elements of personal informa-
20 tion reasonably believed to be affected by
21 the breach of security;

22 (ii) an identification of the records re-
23 ceived from the non-breached entity that
24 have been, or are reasonably believed to

1 have been, affected by the breach of secu-
2 rity; and

3 (iii) whether there is a reasonable risk
4 that the breach of security relating to such
5 information and records has resulted in, or
6 will result in, identity theft, economic loss
7 or economic harm, or financial fraud.

8 (C) ELECTION BY NON-BREACHED COV-
9 ERED ENTITY AFTER RECEIVING NOTICE FROM
10 A BREACHED COVERED ENTITY.—In the case of
11 a breached covered entity that is a party to a
12 written contract with a non-breached covered
13 entity in which the breached covered entity
14 maintains, stores, transmits, or processes data
15 in electronic form containing personal informa-
16 tion identified in subparagraph (B), not later
17 than 10 days after receipt of the notice de-
18 scribed in subparagraph (A), the non-breached
19 covered entity may elect, in writing to the
20 breached covered entity, to provide notification
21 required by paragraph (3) to the individuals de-
22 scribed in the notice. Such election relieves the
23 breached covered entity of the requirements
24 under paragraph (3) with respect to the individ-
25 uals described in the notice.

1 (D) OBLIGATION AFTER ELECTION.—

2 (i) BREACHED COVERED ENTITY CO-
3 OPERATION.—If a non-breached covered
4 entity elects under subparagraph (C) to
5 provide notice under paragraph (3), the
6 breached covered entity shall cooperate in
7 all reasonable respects with the non-
8 breached covered entity so that the notifi-
9 cation to such individuals is made as re-
10 quired under this section. Not later than
11 10 business days after the non-breached
12 covered entity submits a written request
13 for necessary information to the breached
14 covered entity, the breached covered entity
15 shall provide such information.

16 (ii) NON-BREACHED COVERED ENTITY
17 COOPERATION.—If a non-breached covered
18 entity does not elect to provide notice to
19 individuals under subparagraph (C), the
20 non-breached covered entity shall provide
21 all required information about such indi-
22 viduals to, and cooperate in all reasonable
23 respects with, the breached covered entity
24 so that the notification to such individuals
25 is made as required under this section. Not

1 later than 10 business days after the
2 breached covered entity submits a written
3 request for necessary information to the
4 non-breached covered entity, the non-
5 breached covered entity shall provide such
6 information.

7 (5) LAW ENFORCEMENT.—A covered entity
8 shall as expeditiously as possible notify the Commis-
9 sion and the Secret Service or the Federal Bureau
10 of Investigation of the fact that a breach of security
11 has occurred if the number of individuals whose per-
12 sonal information was, or there is a reasonable basis
13 to conclude was, accessed or acquired by an unau-
14 thorized person exceeds 10,000. Any notification
15 provided to the Secret Service or the Federal Bu-
16 reau of Investigation pursuant to this paragraph
17 shall be provided not less than 10 days before notifi-
18 cation is provided to individuals pursuant to para-
19 graph (3).

20 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

21 (1) NON-PROFIT ORGANIZATIONS.—In the event
22 of a breach of security involving personal informa-
23 tion that would trigger notification under subsection
24 (a), a non-profit organization may complete such no-

1 tification according to the procedures set forth in
2 subsection (d)(2).

3 (2) COORDINATION OF NOTIFICATION WITH
4 CONSUMER REPORTING AGENCIES.—If a covered en-
5 tity is required to provide notification to more than
6 10,000 individuals under subsection (a), such cov-
7 ered entity shall also notify a consumer reporting
8 agency that compiles and maintains files on con-
9 sumers on a nationwide basis, of the timing and dis-
10 tribution of the notices. Such notice shall be given
11 to such consumer reporting agencies without unrea-
12 sonable delay and, if it will not delay notice to the
13 affected individuals, prior to the distribution of no-
14 tices to the affected individuals.

15 (c) TIMELINESS OF NOTIFICATION.—

16 (1) IN GENERAL.—Unless subject to a delay au-
17 thorized under paragraph (2), a breached covered
18 entity shall make the notification required under
19 subsection (a)(3) within 25 days after the non-
20 breached covered entity declines or fails to exercise
21 the election under subsection (a)(4)(C), a non-
22 breached covered entity shall make the notification
23 required under subsection (a)(3) within 25 days
24 after exercising the election under subsection
25 (a)(4)(C), and any other covered entity shall identify

1 the individuals affected by a breach of security and
2 make the notification required under subsection (a)
3 as expeditiously as possible and without unreason-
4 able delay, not later than 30 days after completing
5 the requirements of subsection (a)(1). If a covered
6 entity has provided the notification to individuals re-
7 quired under subsection (a) and after such notifica-
8 tion discovers additional individuals to whom notifi-
9 cation is required under such subsection with respect
10 to the same breach of security, the covered entity
11 shall make such notification to such individuals as
12 expeditiously as possible and without unreasonable
13 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 quests 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.

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

3 (I) the covered entity's primary
4 method of communication with the in-
5 dividual is by email or such other elec-
6 tronic means or the individual has
7 consented to receive such notification;
8 and

9 (II) the email or other electronic
10 means does not contain a hyperlink.

11 (B) CONTENT OF NOTIFICATION.—Regard-
12 less of the method by which notification is pro-
13 vided to an individual under subparagraph (A)
14 with respect to a breach of security, such notifi-
15 cation shall include each of the following:

16 (i) The identity of the covered entity
17 that suffered the breach and, if such cov-
18 ered entity is also a breached covered enti-
19 ty providing notice under section 3(b)(1),
20 the identity of each non-breached covered
21 entity that did not elect to notify affected
22 individuals pursuant to section 3(b)(1)(B)
23 sufficient to show the breached covered en-
24 tity's commercial relationship to the indi-
25 vidual receiving notice.

1 (ii) A description of the personal in-
2 formation that was, or there is a reason-
3 able basis to conclude was, acquired or
4 accessed by an unauthorized person.

5 (iii) The date range of the breach of
6 security, or an approximate date range of
7 the breach of security if a specific date
8 range is unknown based on the information
9 available at the time of the notification.

10 (iv) A telephone number, or toll-free
11 telephone number for any covered entity
12 that does not meet the definition of a small
13 business concern or non-profit organiza-
14 tion, that the individual may use to contact
15 the covered entity to inquire about the
16 breach of security or the information the
17 covered entity maintained about that indi-
18 vidual.

19 (v) The toll-free contact telephone
20 numbers and addresses for a consumer re-
21 porting agency that compiles and main-
22 tains files on consumers on a nationwide
23 basis.

24 (vi) The toll-free telephone number
25 and Internet website address for the Com-

1 mission whereby the individual may obtain
2 information regarding identity theft.

3 (2) SUBSTITUTE NOTIFICATION.—

4 (A) IN GENERAL.—If, after making rea-
5 sonable efforts to contact all individuals to
6 whom notice is required under subsection (a),
7 the covered entity finds that contact informa-
8 tion for 500 or more individuals is insufficient
9 or out-of-date, the covered entity shall also pro-
10 vide substitute notice to those individuals,
11 which shall be reasonably calculated to reach
12 the individuals affected by the breach of secu-
13 rity.

14 (B) FORM OF SUBSTITUTE NOTIFICA-
15 TION.—A covered entity may provide substitute
16 notification by—

17 (i) email or other electronic notifica-
18 tion to the extent that the covered entity
19 has contact information for individuals to
20 whom it is required to provide notification
21 under subsection (a) and provided such
22 email or electronic means does not contain
23 a hyperlink; and

24 (ii) a conspicuous notice on the cov-
25 ered entity's Internet website (if such cov-

1 ered entity maintains such a website) for
2 at least 90 days.

3 (C) CONTENT OF SUBSTITUTE NOTICE.—

4 Each form of substitute notice under clauses (i)
5 and (ii) of subparagraph (B) shall include the
6 information required under paragraph (1)(B).

7 (3) DIRECT NOTIFICATION BY A THIRD
8 PARTY.—Nothing in this Act shall be construed to
9 prevent a covered entity from contracting with a
10 third party to provide the notification required under
11 this section, provided such third party issues such
12 notification without unreasonable delay, in accord-
13 ance with the requirements of this section, and indi-
14 cates to all individuals in such notification that such
15 third party is sending such notification on behalf of
16 the covered entity.

17 (e) REQUIREMENTS OF SERVICE PROVIDERS.—

18 (1) IN GENERAL.—If a service provider becomes
19 aware of a breach of security involving data in elec-
20 tronic form containing personal information that is
21 owned or licensed by a covered entity that connects
22 to or uses a system or network provided by the serv-
23 ice provider for the purpose of transmitting, routing,
24 or providing intermediate or transient storage of
25 such data, such service provider shall notify the cov-

1 ered entity who initiated such connection, trans-
2 mission, routing, or storage of the data containing
3 personal information breached, if such covered entity
4 can be reasonably identified. If a service provider is
5 acting solely as a service provider for purposes of
6 this subsection, the service provider has no other no-
7 tification obligations under this section.

8 (2) COVERED ENTITIES WHO RECEIVE NOTICE
9 FROM SERVICE PROVIDERS.—Upon receiving notifi-
10 cation from a service provider under paragraph (1),
11 a covered entity shall provide notification as required
12 under this section.

13 **SEC. 4. ENFORCEMENT.**

14 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
15 MISSION.—

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

23 (2) POWERS OF COMMISSION.—The Commis-
24 sion shall enforce this Act in the same manner, by
25 the same means, and with the same jurisdiction,

1 powers, and duties as though all applicable terms
2 and provisions of the Federal Trade Commission Act
3 (15 U.S.C. 41 et seq.) were incorporated into and
4 made a part of this Act, and any covered entity who
5 violates this Act shall be subject to the penalties and
6 entitled to the privileges and immunities provided in
7 the Federal Trade Commission Act (15 U.S.C. 41 et
8 seq.), and as provided in clauses (ii) and (iii) of sec-
9 tion 5(4)(A).

10 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
11 ERAL.—

12 (1) CIVIL ACTION.—In any case in which the
13 attorney general of a State has reason to believe
14 that an interest of the residents of that State has
15 been or is threatened or adversely affected by any
16 covered entity who violates section 2 or 3 of this
17 Act, the attorney general of the State, as *parens*
18 *patriae*, may bring a civil action on behalf of the
19 residents of the State in a district court of the
20 United States of appropriate jurisdiction to—

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

23 (B) compel compliance with such section;

24 or

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

3 (2) CIVIL PENALTIES.—

4 (A) CALCULATION.—

5 (i) TREATMENT OF VIOLATIONS OF
6 SECTION 2.—For purposes of paragraph
7 (1)(C) with regard to a violation of section
8 2, the amount determined under this para-
9 graph is the amount calculated by multi-
10 plying the number of days that a covered
11 entity is not in compliance with such sec-
12 tion by an amount not greater than
13 \$11,000.

14 (ii) TREATMENT OF VIOLATIONS OF
15 SECTION 3.—For purposes of paragraph
16 (1)(C) with regard to a violation of section
17 3, the amount determined under this para-
18 graph is the amount calculated by multi-
19 plying the number of violations of such
20 section by an amount not greater than
21 \$11,000. Each failure to send notification
22 as required under section 3 to a resident of
23 the State shall be treated as a separate
24 violation.

1 (B) MAXIMUM TOTAL LIABILITY.—Not-
2 withstanding the number of actions which may
3 be brought against a covered entity under this
4 subsection, the maximum civil penalty for which
5 any covered entity may be liable under this sub-
6 section shall not exceed—

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

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

12 (C) ADJUSTMENT FOR INFLATION.—Be-
13 ginning on the date that the Consumer Price
14 Index is first published by the Bureau of Labor
15 Statistics that is after one year after the date
16 of enactment of this Act, and each year there-
17 after, the amounts specified in clauses (i) and
18 (ii) of subparagraph (A) and clauses (i) and (ii)
19 of subparagraph (B) shall be increased by the
20 percentage increase in the Consumer Price
21 Index published on that date from the Con-
22 sumer Price Index published the previous year.

23 (D) PENALTY FACTORS.—In determining
24 the amount of such a civil penalty, the degree
25 of culpability, any history of prior such conduct,

1 ability to pay, effect on ability to continue to do
2 business, and such other matters as justice may
3 require shall be taken into account.

4 (3) INTERVENTION BY THE FEDERAL TRADE
5 COMMISSION.—

6 (A) NOTICE AND INTERVENTION.—In all
7 cases, the State shall provide prior written no-
8 tice of any action under paragraph (1) to the
9 Commission and provide the Commission with a
10 copy of its complaint, except in any case in
11 which such prior notice is not feasible, in which
12 case the State shall serve such notice imme-
13 diately upon instituting such action. The Com-
14 mission shall have the right—

15 (i) to intervene in the action;

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

18 (iii) to file petitions for appeal.

19 (B) PENDING PROCEEDINGS.—If the Fed-
20 eral Trade Commission initiates a Federal civil
21 action for a violation of this Act, no State at-
22 torney general may bring an action for a viola-
23 tion of this Act that resulted from the same or
24 related acts or omissions against a defendant

1 named in the civil action initiated by the Fed-
2 eral Trade Commission.

3 (4) CONSTRUCTION.—For purposes of bringing
4 any civil action under paragraph (1), nothing in this
5 Act shall be construed to prevent an attorney gen-
6 eral of a State from exercising the powers conferred
7 on the attorney general by the laws of that State
8 to—

9 (A) conduct investigations;

10 (B) administer oaths or affirmations; or

11 (C) compel the attendance of witnesses or
12 the production of documentary and other evi-
13 dence.

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

17 **SEC. 5. DEFINITIONS.**

18 In this Act:

19 (1) BREACH OF SECURITY.—The term “breach
20 of security”—

21 (A) means a compromise of the security,
22 confidentiality, or integrity of, or loss of, data
23 in electronic form that results in, or there is a
24 reasonable basis to conclude has resulted in,

1 unauthorized access to or acquisition of per-
2 sonal information from a covered entity; and

3 (B) does not include the good faith acquisi-
4 tion of personal information by an employee or
5 agent of the covered entity for the purposes of
6 the covered entity, if the personal information is
7 not used or subject to further unauthorized dis-
8 closure.

9 (2) BREACHED COVERED ENTITY.—The term
10 “breached covered entity” means a covered entity
11 that has incurred a breach of security affecting data
12 in electronic form containing personal information of
13 a non-breached covered entity that has directly con-
14 tracted the breached covered entity to maintain,
15 store, or process data in electronic form containing
16 personal information on behalf of such non-breached
17 covered entity. For purposes of this definition, the
18 term “breached covered entity” shall not include a
19 service provider.

20 (3) COMMISSION.—The term “Commission”
21 means the Federal Trade Commission.

22 (4) CONSUMER REPORTING AGENCY THAT COM-
23 PILES AND MAINTAINS FILES ON CONSUMERS ON A
24 NATIONWIDE BASIS.—The term “consumer reporting
25 agency that compiles and maintains files on con-

1 sumers on a nationwide basis” has the meaning
2 given that term in section 603(p) of the Fair Credit
3 Reporting Act (15 U.S.C. 1681a(p)).

4 (5) COVERED ENTITY.—

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

7 (i) a sole proprietorship, partnership,
8 corporation, trust, estate, cooperative, as-
9 sociation, or other entity in or affecting
10 commerce that acquires, maintains, stores,
11 sells, or otherwise uses data in electronic
12 form that includes personal information,
13 over which the Commission has authority
14 pursuant to section 5(a)(2) of the Federal
15 Trade Commission Act (15 U.S.C.
16 45(a)(2));

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

22 (iii) notwithstanding any jurisdictional
23 limitation of the Federal Trade Commis-
24 sion Act (15 U.S.C. 41 et seq.), any non-
25 profit organization.

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

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

6 (ii) a business associate, as defined in
7 section 160.103 of title 45, Code of Fed-
8 eral Regulations, acting in its capacity as
9 a business associate;

10 (iii) if a covered entity, as defined in
11 section 160.103 of title 45, Code of Fed-
12 eral Regulations, is a hybrid entity, as de-
13 fined in section 164.105 of title 45, Code
14 of Federal Regulations, then the health
15 care component of such hybrid entity;

16 (iv) a broker, dealer, investment ad-
17 viser, or person engaged in providing in-
18 surance that is subject to title V of Public
19 Law 106-102 (15 U.S.C. 6801 et seq.); or

20 (v) a State-chartered credit union, as
21 defined in section 101(6) of the Federal
22 Credit Union Act (12 U.S.C. 1752(6)),
23 that is not an insured credit union as de-
24 fined in section 101(7) of such Act (12
25 U.S.C. 1752(7)).

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

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

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

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

20 (8) NON-BREACHED COVERED ENTITY.—The
21 term “non-breached covered entity” means a covered
22 entity that has not incurred the breach of security
23 involving data in electronic form containing personal
24 information that it owns or licenses but whose data
25 has been affected by the breach of security incurred

1 by a breached covered entity it directly contracts to
2 maintain, store, or process data in electronic form
3 containing personal information on behalf of the
4 non-breached covered entity.

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

10 (10) PERSONAL INFORMATION.—

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

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

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

23 (II) Any two of the following:

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

20 (11) 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 (12) **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 (13) **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 security breach of such data.

6 (b) COMMON LAW.—This section shall not exempt a
7 covered entity from liability under common law.

8 (c) CERTAIN FTC ENFORCEMENT LIMITED TO DATA
9 SECURITY AND BREACH NOTIFICATION.—

10 (1) DATA SECURITY AND BREACH NOTIFICA-
11 TION.—Insofar as sections 201, 202, 222, 338, and
12 631 of the Communications Act of 1934 (47 U.S.C.
13 201, 202, 222, 338, and 551), and any regulations
14 promulgated thereunder, apply to covered entities
15 with respect to securing information in electronic
16 form from unauthorized access, including notifica-
17 tion of unauthorized access to data in electronic
18 form containing personal information, such sections
19 and regulations promulgated thereunder shall have
20 no force or effect, unless such regulations pertain
21 solely to 9–1–1 calls.

22 (2) RULE OF CONSTRUCTION.—Nothing in this
23 subsection otherwise limits the Federal Communica-
24 tions Commission’s authority with respect to sec-
25 tions 201, 202, 222, 338, and 631 of the Commu-

