

114TH CONGRESS
1ST SESSION

S. 961

To protect information relating to consumers, to require notice of security breaches, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 15, 2015

Mr. CARPER (for himself and Mr. BLUNT) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To protect information relating to consumers, to require notice of security breaches, 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.**

4 This Act may be cited as the “Data Security Act of
5 2015”.

6 **SEC. 2. PURPOSES.**

7 The purposes of this Act are—

8 (1) to establish strong and uniform national
9 data security and breach notification standards for
10 electronic data; and

1 (2) to expressly preempt any related State laws
2 in order to provide the Federal Trade Commission
3 with authority to enforce such standards for entities
4 covered under this Act.

5 **SEC. 3. DEFINITIONS.**

6 For purposes of this Act, the following definitions
7 shall apply:

8 (1) AFFILIATE.—The term “affiliate” means
9 any company that controls, is controlled by, or is
10 under common control with another company.

11 (2) AGENCY.—The term “agency” has the same
12 meaning as in section 551(1) of title 5, United
13 States Code.

14 (3) BREACH OF DATA SECURITY.—

15 (A) IN GENERAL.—The term “breach of
16 data security” means the unauthorized acqui-
17 sition of sensitive account information or sen-
18 sitive personal information.

19 (B) EXCEPTION FOR DATA THAT IS NOT IN
20 USABLE FORM.—The term “breach of data se-
21 curity” does not include the unauthorized ac-
22 quisition of sensitive account information or
23 sensitive personal information that is encrypted,
24 redacted, or otherwise protected by another
25 method that renders the information unreadable

1 and unusable if the encryption, redaction, or
2 protection process or key is not also acquired
3 without authorization.

4 (4) CARRIER.—The term “carrier” means any
5 entity that—

6 (A) provides electronic data transmission,
7 routing, intermediate, and transient storage, or
8 connections to its system or network;

9 (B) does not select or modify the content
10 of the electronic data;

11 (C) is not the sender or the intended re-
12 cipient of the data; and

13 (D) does not differentiate sensitive account
14 information or sensitive personal information
15 from other information that the entity trans-
16 mits, routes, stores in intermediate or transient
17 storage, or for which such entity provides con-
18 nections.

19 (5) COMMISSION.—The term “Commission”
20 means the Federal Trade Commission.

21 (6) CONSUMER.—The term “consumer” means
22 an individual.

23 (7) CONSUMER REPORTING AGENCY THAT COM-
24 PILES AND MAINTAINS FILES ON CONSUMERS ON A
25 NATIONWIDE BASIS.—The term “consumer reporting

1 agency that compiles and maintains files on con-
2 sumers on a nationwide basis” has the same mean-
3 ing as in section 603(p) of the Fair Credit Report-
4 ing Act (15 U.S.C. 1681a(p)).

5 (8) COVERED ENTITY.—

6 (A) IN GENERAL.—The term “covered en-
7 tity” means any individual, partnership, cor-
8 poration, trust, estate, cooperative, association
9 or entity that accesses, maintains, commu-
10 nicates, or handles sensitive account informa-
11 tion or sensitive personal information.

12 (B) EXCEPTION.—The term “covered enti-
13 ty” does not include any agency or any other
14 unit of Federal, State, or local government or
15 any subdivision of the unit.

16 (9) FINANCIAL INSTITUTION.—The term “fi-
17 nancial institution” has the same meaning as in sec-
18 tion 509(3) of the Gramm-Leach-Bliley Act (15
19 U.S.C. 6809(3)).

20 (10) INFORMATION SECURITY PROGRAM.—The
21 term “information security program” means the ad-
22 ministrative, technical, or physical safeguards that a
23 covered entity uses to access, collect, distribute,
24 process, protect, store, use, transmit, dispose of, or

1 otherwise handle sensitive account information and
 2 sensitive personal information.

3 (11) SENSITIVE ACCOUNT INFORMATION.—The
 4 term “sensitive account information” means a finan-
 5 cial account number relating to a consumer, includ-
 6 ing a credit card number or debit card number, in
 7 combination with any security code, access code,
 8 password, or other personal identification informa-
 9 tion required to access the financial account.

10 (12) SENSITIVE PERSONAL INFORMATION.—

11 (A) IN GENERAL.—The term “sensitive
 12 personal information” means—

13 (i) a Social Security number; or

14 (ii) the first and last name of a con-
 15 sumer in combination with—

16 (I) the consumer’s driver’s li-
 17 cense number, passport number, mili-
 18 tary identification number, or other
 19 similar number issued on a govern-
 20 ment document used to verify identity;

21 (II) information that could be
 22 used to access a consumer’s account,
 23 such as a user name and password or
 24 e-mail and password; or

1 (III) biometric data of the con-
2 sumer used to gain access to financial
3 accounts of the consumer.

4 (B) EXCEPTION.—The term “sensitive per-
5 sonal information” does not include publicly
6 available information that is lawfully made
7 available to the general public and obtained
8 from—

9 (i) Federal, State, or local government
10 records; or

11 (ii) widely distributed media.

12 (13) SUBSTANTIAL HARM OR INCONVEN-
13 IENCE.—The term “substantial harm or inconven-
14 ience” means—

15 (A) identity theft; or

16 (B) fraudulent transactions on financial
17 accounts.

18 (14) THIRD-PARTY SERVICE PROVIDER.—The
19 term “third-party service provider” means any per-
20 son that maintains, processes, or otherwise is per-
21 mitted access to sensitive account information or
22 sensitive personal information in connection with
23 providing services to a covered entity.

1 **SEC. 4. PROTECTION OF INFORMATION AND SECURITY**

2 **BREACH NOTIFICATION.**

3 (a) SECURITY PROCEDURES REQUIRED.—

4 (1) IN GENERAL.—Each covered entity shall de-
5 velop, implement, and maintain a comprehensive in-
6 formation security program that contains adminis-
7 trative, technical, and physical safeguards that are
8 reasonably designed to achieve the objectives in
9 paragraph (2).

10 (2) OBJECTIVES.—The objectives of this sub-
11 section are to—

12 (A) ensure the security and confidentiality
13 of sensitive account information and sensitive
14 personal information;

15 (B) protect against any anticipated threats
16 or hazards to the security or integrity of such
17 information; and

18 (C) protect against unauthorized acqui-
19 sition of such information that could result in
20 substantial harm to the individuals to whom
21 such information relates.

22 (3) LIMITATION.—A covered entity's informa-
23 tion security program under paragraph (1) shall be
24 appropriate to—

25 (A) the size and complexity of the covered
26 entity;

1 (B) the nature and scope of the activities
2 of the covered entity; and

3 (C) the sensitivity of the consumer infor-
4 mation to be protected.

5 (4) ELEMENTS.—In order to develop, imple-
6 ment, and maintain its information security pro-
7 gram, a covered entity shall—

8 (A) designate an employee or employees to
9 coordinate the information security program;

10 (B) identify reasonably foreseeable internal
11 and external risks to the security, confiden-
12 tiality, and integrity of sensitive account infor-
13 mation and sensitive personal information and
14 assess the sufficiency of any safeguards in place
15 to control these risks, including consideration of
16 risks in each relevant area of the covered enti-
17 ty's operations, including—

18 (i) employee training and manage-
19 ment;

20 (ii) information systems, including
21 network and software design, as well as in-
22 formation processing, storage, trans-
23 mission, and disposal; and

1 (iii) detecting, preventing and re-
2 sponding to attacks, intrusions, or other
3 systems failures;

4 (C) design and implement information
5 safeguards to control the risks identified in its
6 risk assessment, and regularly assess the effec-
7 tiveness of the safeguards' key controls, sys-
8 tems, and procedures;

9 (D) oversee service providers by—

10 (i) taking reasonable steps to select
11 and retain service providers that are capa-
12 ble of maintaining appropriate safeguards
13 for the sensitive account information or
14 sensitive personal information at issue;

15 (ii) requiring service providers by con-
16 tract to implement and maintain such safe-
17 guards; and

18 (iii) reasonably oversee or obtain an
19 assessment of the service provider's compli-
20 ance with contractual obligations, where
21 appropriate in light of the covered entity's
22 risk assessment; and

23 (E) evaluate and adjust the information
24 security program in light of the results of the
25 risk assessments and testing and monitoring re-

1 quired by subparagraphs (C) and (D) and any
2 material changes to the covered entity's oper-
3 ations or business arrangements, or any other
4 circumstances that the covered entity knows or
5 has reason to know may have a material impact
6 on its information security program.

7 (5) SECURITY CONTROLS.—Each covered entity
8 shall—

9 (A) consider whether the following security
10 measures are appropriate for the covered entity
11 and, if so, adopt those measures that the cov-
12 ered entity concludes are appropriate—

13 (i) access controls on information sys-
14 tems, including controls to authenticate
15 and permit access only to authorized indi-
16 viduals and controls to prevent employees
17 from providing sensitive account informa-
18 tion or sensitive personal information to
19 unauthorized individuals who may seek to
20 obtain this information through fraudulent
21 means;

22 (ii) access restrictions at physical lo-
23 cations containing sensitive account infor-
24 mation or sensitive personal information,
25 such as buildings, computer facilities, and

1 records storage facilities, to permit access
2 only to authorized individuals;

3 (iii) encryption of electronic sensitive
4 account information or sensitive personal
5 information, including while in transit or
6 in storage on networks or systems to which
7 unauthorized individuals may have access;

8 (iv) procedures designed to ensure
9 that information system modifications are
10 consistent with the covered entity's infor-
11 mation security program;

12 (v) dual control procedures, segrega-
13 tion of duties, and employee background
14 checks for employees with responsibilities
15 for, or access to, sensitive account informa-
16 tion or sensitive personal information;

17 (vi) monitoring systems and proce-
18 dures to detect actual and attempted at-
19 tacks on, or intrusions into, information
20 systems;

21 (vii) response programs that specify
22 actions to be taken when the covered entity
23 suspects or detects that unauthorized indi-
24 viduals have gained access to information
25 systems; and

(viii) measures to protect against destruction, loss, or damage of sensitive account information or sensitive personal information due to potential environmental hazards, such as fire and water damage or technological failures;

(B) develop, implement, and maintain appropriate measures to properly dispose of sensitive account information and sensitive personal information; and

(C) train staff to implement the covered entity's information security program.

(6) ADMINISTRATIVE REQUIREMENTS.—

(A) BOARD OVERSIGHT.—If a covered entity has a board of directors, the covered entity's board of directors or an appropriate committee of the board shall—

(i) approve the covered entity's written information security program; and

(ii) oversee the development, implementation, and maintenance of the covered entity's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

1 (B) REPORT TO THE BOARD.—If a covered
2 entity has a board of directors, the covered enti-
3 ty shall report to its board or an appropriate
4 committee of the board at least annually, in-
5 cluding describing—

6 (i) the overall status of the informa-
7 tion security program and the covered enti-
8 ty's compliance with this Act; and

9 (ii) material matters related to its
10 program, addressing issues such as risk as-
11 sessment, risk management and control de-
12 cisions, service provider arrangements, re-
13 sults of testing, security breaches or viola-
14 tions and management's responses, and
15 recommendations for changes in the infor-
16 mation security program.

17 (b) INVESTIGATION REQUIRED.—

18 (1) IN GENERAL.—If a covered entity believes
19 that a breach of data security has or may have oc-
20 curred in relation to sensitive account information or
21 sensitive personal information that is maintained,
22 communicated, or otherwise handled by, or on behalf
23 of, the covered entity, the covered entity shall con-
24 duct an investigation to—

1 (A) assess the nature and scope of the in-
2 cident;

3 (B) identify any sensitive account informa-
4 tion or sensitive personal information that may
5 have been involved in the incident;

6 (C) determine if the sensitive account in-
7 formation or sensitive personal information has
8 been acquired without authorization; and

9 (D) take reasonable measures to restore
10 the security and confidentiality of the systems
11 compromised in the breach.

12 (c) NOTICE REQUIRED.—If a covered entity deter-
13 mines under subsection (b)(1)(C) that the unauthorized
14 acquisition of sensitive account information or sensitive
15 personal information involved in a breach of data security
16 is reasonably likely to cause substantial harm to the con-
17 sumers to whom the information relates, the covered enti-
18 ty, or a third party acting on behalf of the covered entity,
19 shall—

20 (1) notify, without unreasonable delay—

21 (A) an appropriate Federal law enforce-
22 ment agency;

23 (B) the appropriate agency or authority
24 identified in section 5;

1 (C) any relevant payment card network, if
2 the breach involves a breach of payment card
3 numbers;

4 (D) each consumer reporting agency that
5 compiles and maintains files on consumers on a
6 nationwide basis, if the breach involves sensitive
7 personal information or sensitive account infor-
8 mation relating to 5,000 or more consumers;
9 and

10 (E) all consumers to whom the sensitive
11 account information or sensitive personal infor-
12 mation relates;

13 (2) provide notice to consumers by—

14 (A) written notification sent to the postal
15 address of the consumer in the records of the
16 covered entity;

17 (B) telephonic notification to the number
18 of the consumer in the records of the covered
19 entity;

20 (C) e-mail of the consumer or other elec-
21 tronic means in the records of the covered enti-
22 ty; or

23 (D) substitute notification in print and to
24 broadcast media where the individual whose
25 personal information was acquired resides, if

1 providing written or e-mail notification is not
2 feasible due to—

3 (i) lack of sufficient contact informa-
4 tion for the consumers that must be noti-
5 fied;

6 (ii) excessive cost to the covered enti-
7 ty; or

8 (iii) exigent circumstances; and

9 (3) provide notice that includes—

10 (A) a description of the type of sensitive
11 account information or sensitive personal infor-
12 mation involved in the breach of data security;

13 (B) a general description of the actions
14 taken by the covered entity to restore the secu-
15 rity and confidentiality of the sensitive account
16 information or sensitive personal information
17 involved in the breach of data security; and

18 (C) a summary of rights of victims of iden-
19 tity theft prepared by the Commission under
20 section 609(d) of the Fair Credit Reporting Act
21 (15 U.S.C. 1681g(d)), if the breach of data se-
22 curity involves sensitive personal information.

23 (d) CLARIFICATION.—A financial institution shall
24 have no obligation under this Act for a breach of security
25 at another covered entity involving sensitive account infor-

1 mation relating to an account owned by the financial insti-
 2 tution.

3 (e) SPECIAL NOTIFICATION REQUIREMENTS.—

4 (1) THIRD-PARTY SERVICE PROVIDERS.—In the
 5 event of a breach of data security of a system main-
 6 tained by a third-party entity that has been con-
 7 tracted to maintain, store, or process data in elec-
 8 tronic form containing sensitive account information
 9 or sensitive personal information on behalf of a cov-
 10 ered entity who owns or possesses such data, such
 11 third-party shall—

12 (A) notify the covered entity; and

13 (B) notify consumers if it is agreed in
 14 writing that the third-party service provider will
 15 provide such notification on behalf of the cov-
 16 ered entity.

17 (2) CARRIER OBLIGATIONS.—

18 (A) IN GENERAL.—If a carrier becomes
 19 aware of a breach of data security involving
 20 data in electronic form containing sensitive ac-
 21 count information or sensitive personal informa-
 22 tion that is owned or licensed by a covered enti-
 23 ty that connects to or uses a system or network
 24 provided by the carrier for the purpose of trans-
 25 mitting, routing, or providing intermediate or

transient storage of such data, such carrier shall notify the covered entity who initiated such connection, transmission, routing, or storage of the data containing sensitive account information or sensitive personal information, if such covered entity can be reasonably identified. If a service provider is acting solely as a service provider for purposes of this subsection, the service provider has no other notification obligations under this section.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM CARRIERS.—Upon receiving notification from a service provider under paragraph (1), a covered entity shall provide notification as required under this section.

(3) COMMUNICATIONS WITH ACCOUNT HOLDERS.—If a covered entity that is not a financial institution experiences a breach of data security involving sensitive account information, a financial institution that issues an account to which the sensitive account information relates may communicate with the account holder regarding the breach, including—

(A) an explanation that the financial institution was not breached, and that the breach

1 occurred at a third-party that had access to the
2 consumer's sensitive account information; or

3 (B) identify the covered entity that experi-
4 enced the breach after the covered entity has
5 provided notice consistent with this Act.

6 (f) COMPLIANCE.—

7 (1) IN GENERAL.—An entity shall be deemed to
8 be in compliance with—

9 (A) in the case of a financial institution—

10 (i) subsection (a), if the financial in-
11 stitution maintains policies and procedures
12 to protect the confidentiality and security
13 of sensitive account information and sen-
14 sitive personal information that are con-
15 sistent with the policies and procedures of
16 the financial institution that are designed
17 to comply with the requirements of section
18 501(b) of the Gramm-Leach-Bliley Act (15
19 U.S.C. 6801(b)) and any regulations or
20 guidance prescribed under that section
21 that are applicable to the financial institu-
22 tion; and

23 (ii) subsections (b) and (c), if the fi-
24 nancial institution—

1 (I)(aa) maintains policies and
2 procedures to investigate and provide
3 notice to consumers of breaches of
4 data security that are consistent with
5 the policies and procedures of the fi-
6 nancial institution that are designed
7 to comply with the investigation and
8 notice requirements established by
9 regulations or guidance under section
10 501(b) of the Gramm-Leach-Bliley
11 Act (15 U.S.C. 6801(b)) that are ap-
12 plicable to the financial institution;

13 (bb) is an affiliate of a bank
14 holding company that maintains poli-
15 cies and procedures to investigate and
16 provide notice to consumers of
17 breaches of data security that are con-
18 sistent with the policies and proce-
19 dures of a bank that is an affiliate of
20 the financial institution, and the poli-
21 cies and procedures of the bank are
22 designed to comply with the investiga-
23 tion and notice requirements estab-
24 lished by any regulations or guidance
25 under section 501(b) of the Gramm-

1 Leach-Bliley Act (15 U.S.C. 6801(b))
2 that are applicable to the bank; or

3 (cc)(AA) is an affiliate of a sav-
4 ings and loan holding company that
5 maintains policies and procedures to
6 investigate and provide notice to con-
7 sumers of data breaches of data secu-
8 rity that are consistent with the poli-
9 cies and procedures of a savings asso-
10 ciation that is an affiliate of the fi-
11 nancial institution; and

12 (BB) the policies and procedures
13 of the savings association are designed
14 to comply with the investigation and
15 notice requirements established by any
16 regulations or guidelines under section
17 501(b) of the Gramm-Leach-Bliley
18 Act (15 U.S. 6801(b)) that are appli-
19 cable to savings associations; and

20 (II) provides for notice to the en-
21 tities described under subparagraphs
22 (B), (C), and (D) of subsection (c)(1),
23 if notice is provided to consumers pur-
24 suant to the policies and procedures

1 of the financial institution described
 2 in subclause (I); and

3 (B) subsections (a), (b), and (c)—

4 (i) if the entity is a covered entity for
 5 purposes of the regulations promulgated
 6 under section 264(c) of the Health Insur-
 7 ance Portability and Accountability Act of
 8 1996 (42 U.S.C. 1320d-2 note), to the ex-
 9 tent that the entity is in compliance with
 10 such regulations; or

11 (ii) if the entity is in compliance with
 12 sections 13402 and 13407 of the HITECH
 13 Act (42 U.S.C. 17932 and 17937).

14 (2) DEFINITIONS.—In this subsection—

15 (A) the terms “bank holding company”
 16 and “bank” have the meanings given the terms
 17 in section 2 of the Bank Holding Company Act
 18 of 1956 (12 U.S.C. 1841);

19 (B) the term “savings and loan holding
 20 company” has the meaning given the term in
 21 section 10 of the Home Owners’ Loan Act (12
 22 U.S.C. 1467a); and

23 (C) the term “savings association” has the
 24 meaning given the term in section 2 of the
 25 Home Owners’ Loan Act (12 U.S.C. 1462).

1 **SEC. 5. ADMINISTRATIVE ENFORCEMENT.**

2 (a) IN GENERAL.—Notwithstanding any other provi-
3 sion of law section 4 shall be enforced exclusively under—

4 (1) section 8 of the Federal Deposit Insurance
5 Act (12 U.S.C. 1818), in the case of—

6 (A) a national bank, a Federal branch or
7 Federal agency of a foreign bank, or any sub-
8 sidiary thereof (other than a broker, dealer,
9 person providing insurance, investment com-
10 pany, or investment adviser), or a savings asso-
11 ciation, the deposits of which are insured by the
12 Federal Deposit Insurance Corporation, or any
13 subsidiary thereof (other than a broker, dealer,
14 person providing insurance, investment com-
15 pany, or investment adviser), by the Office of
16 the Comptroller of the Currency;

17 (B) a member bank of the Federal Reserve
18 System (other than a national bank), a branch
19 or agency of a foreign bank (other than a Fed-
20 eral branch, Federal agency, or insured State
21 branch of a foreign bank), a commercial lending
22 company owned or controlled by a foreign bank,
23 an organization operating under section 25 or
24 25A of the Federal Reserve Act (12 U.S.C.
25 601, 611), or a bank holding company and its
26 nonbank subsidiary or affiliate (other than a

1 broker, dealer, person providing insurance, in-
2 vestment company, or investment adviser), by
3 the Board of Governors of the Federal Reserve
4 System; and

5 (C) a bank, the deposits of which are in-
6 sured by the Federal Deposit Insurance Cor-
7 poration (other than a member of the Federal
8 Reserve System), an insured State branch of a
9 foreign bank, or any subsidiary thereof (other
10 than a broker, dealer, person providing insur-
11 ance, investment company, or investment ad-
12 viser), by the Board of Directors of the Federal
13 Deposit Insurance Corporation;

14 (2) the Federal Credit Union Act (12 U.S.C.
15 1751 et seq.), by the National Credit Union Admin-
16 istration Board with respect to any federally insured
17 credit union;

18 (3) the Securities Exchange Act of 1934 (15
19 U.S.C. 78a et seq.), by the Securities and Exchange
20 Commission with respect to any broker or dealer;

21 (4) the Investment Company Act of 1940 (15
22 U.S.C. 80a–1 et seq.), by the Securities and Ex-
23 change Commission with respect to any investment
24 company;

1 (5) the Investment Advisers Act of 1940 (15
2 U.S.C. 80b–1 et seq.), by the Securities and Ex-
3 change Commission with respect to any investment
4 adviser registered with the Securities and Exchange
5 Commission under that Act;

6 (6) the Commodity Exchange Act (7 U.S.C. 1
7 et seq.), by the Commodity Futures Trading Com-
8 mission with respect to any futures commission mer-
9 chant, commodity trading advisor, commodity pool
10 operator, or introducing broker;

11 (7) the provisions of title XIII of the Housing
12 and Community Development Act of 1992 (12
13 U.S.C. 4501 et seq.), by the Director of Federal
14 Housing Enterprise Oversight (and any successor to
15 the functional regulatory agency) with respect to the
16 Federal National Mortgage Association, the Federal
17 Home Loan Mortgage Corporation, and any other
18 entity or enterprise (as defined in that title) subject
19 to the jurisdiction of the functional regulatory agen-
20 cy under that title, including any affiliate of any the
21 enterprise;

22 (8) State insurance law, in the case of any per-
23 son engaged in providing insurance, by the applica-
24 ble State insurance authority of the State in which
25 the person is domiciled; and

(9) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8), including—

(A) 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.);

(B) notwithstanding the Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.), include the authority to enforce compliance by air carriers and foreign air carriers; and

(C) notwithstanding the Packers and Stockyards Act (7 U.S.C. 181 et seq.), include the authority to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—

(1) DATA SECURITY AND BREACH NOTIFICATION.—Sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551), and any regulations promul-

1 gated in accordance with those sections, shall not
2 apply with respect to the information security prac-
3 tices, including practices relating to the notification
4 of unauthorized access to data in electronic form, of
5 any covered entity otherwise subject to those sec-
6 tions.

7 (2) RULE OF CONSTRUCTION.—Nothing in this
8 subsection otherwise limits authority of the Federal
9 Communication Commission with respect to sections
10 201, 202, 222, 338, and 631 of the Communications
11 Act of 1934 (47 U.S.C. 201, 202, 222, 338, and
12 551).

13 (c) NO PRIVATE RIGHT OF ACTION.—

14 (1) IN GENERAL.—This Act may not be con-
15 strued to provide a private right of action, including
16 a class action with respect to any Act or practice
17 regulated under this Act.

18 (2) EXCEPTION.—A consumer or entity that
19 suffers financial harm as a result of a covered enti-
20 ty's violation of this Act may bring an action in a
21 district court of the United States for the judicial
22 district in which the consumer or entity suffered the
23 harm against the covered entity to recover—

24 (A) in the case of a negligent violation of
25 this Act, actual financial damages, court costs

1 allowed by the rules of the court, and reason-
2 able attorney's fees; and

3 (B) in the case of a knowing violation of
4 this Act, the damages, costs, and attorney's fees
5 described in subparagraph (A) of this sub-
6 section and punitive damages.

7 **SEC. 6. RELATION TO STATE LAW.**

8 No requirement or prohibition may be imposed under
9 the laws of any State with respect to the responsibilities
10 of any person to—

11 (1) protect the security of information relating
12 to consumers that is maintained, communicated, or
13 otherwise handled by, or on behalf of, the person;

14 (2) safeguard information relating to consumers
15 from—

16 (A) unauthorized access; and

17 (B) unauthorized acquisition;

18 (3) investigate or provide notice of the unau-
19 thorized acquisition of, or access to, information re-
20 lating to consumers, or the potential misuse of the
21 information, for fraudulent, illegal, or other pur-
22 poses; or

23 (4) mitigate any potential or actual loss or
24 harm resulting from the unauthorized acquisition of,
25 or access to, information relating to consumers.

1 **SEC. 7. DELAYED EFFECTIVE DATE FOR CERTAIN PROVI-**
2 **SIONS.**

3 Sections 4 and 6 shall take effect 1 year after the
4 date of enactment of this Act.

