

114TH CONGRESS  
1ST SESSION

# H. R. 2205

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

---

## IN THE HOUSE OF REPRESENTATIVES

MAY 1, 2015

Mr. NEUGEBAUER (for himself and Mr. CARNEY) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To protect financial 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—

1           (1) to establish strong and uniform national  
2 data security and breach notification standards for  
3 electronic data; and

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

8 **SEC. 3. DEFINITIONS.**

9           For purposes of this Act, the following definitions  
10 shall apply:

11           (1) **AFFILIATE.**—The term “affiliate” means  
12 any company that controls, is controlled by, or is  
13 under common control with another company.

14           (2) **AGENCY.**—The term “agency” has the same  
15 meaning as in section 551(1) of title 5, United  
16 States Code.

17           (3) **BREACH OF DATA SECURITY.**—

18           (A) **IN GENERAL.**—The term “breach of  
19 data security” means the unauthorized acquisi-  
20 tion of sensitive financial account information  
21 or sensitive personal information.

22           (B) **EXCEPTION FOR DATA THAT IS NOT IN**  
23 **USABLE FORM.**—The term “breach of data se-  
24 curity” does not include the unauthorized ac-  
25 quisition of sensitive financial account informa-

1           tion or sensitive personal information that is  
2           encrypted, redacted, or otherwise protected by  
3           another method that renders the information  
4           unreadable and unusable if the encryption, re-  
5           daction, or protection process or key is not also  
6           acquired without authorization.

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

9                   (A) provides electronic data transmission,  
10                  routing, intermediate, and transient storage, or  
11                  connections to its system or network;

12                  (B) does not select or modify the content  
13                  of the electronic data;

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

16                  (D) does not differentiate sensitive finan-  
17                  cial account information or sensitive personal  
18                  information from other information that the en-  
19                  tity transmits, routes, stores in intermediate or  
20                  transient storage, or for which such entity pro-  
21                  vides connections.

22           (5) COMMISSION.—The term “Commission”  
23           means the Federal Trade Commission.

24           (6) CONSUMER.—The term “consumer” means  
25           an individual.

1           (7) CONSUMER REPORTING AGENCY THAT COM-  
2           PILES AND MAINTAINS FILES ON CONSUMERS ON A  
3           NATIONWIDE BASIS.—The term “consumer reporting  
4           agency that compiles and maintains files on con-  
5           sumers on a nationwide basis” has the same mean-  
6           ing as in section 603(p) of the Fair Credit Report-  
7           ing Act (15 U.S.C. 1681a(p)).

8           (8) COVERED ENTITY.—

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

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

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

23          (10) INFORMATION SECURITY PROGRAM.—The  
24          term “information security program” means the ad-  
25          ministrative, technical, or physical safeguards that a

1 covered entity uses to access, collect, distribute,  
2 process, protect, store, use, transmit, dispose of, or  
3 otherwise handle sensitive financial account informa-  
4 tion and sensitive personal information.

5 (11) SENSITIVE FINANCIAL ACCOUNT INFORMA-  
6 TION.—The term “sensitive financial account infor-  
7 mation” means a financial account number relating  
8 to a consumer, including a credit card number or  
9 debit card number, in combination with any security  
10 code, access code, password, or other personal identi-  
11 fication information required to access the financial  
12 account.

13 (12) SENSITIVE PERSONAL INFORMATION.—

14 (A) IN GENERAL.—The term “sensitive  
15 personal information” includes—

16 (i) a Social Security number; and

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

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

24 (II) information that could be  
25 used to access a consumer’s account,

1 such as a user name and password or  
2 e-mail and password; or

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

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

11 (i) Federal, State, or local government  
12 records; or

13 (ii) widely distributed media.

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

17 (A) identity theft; or

18 (B) fraudulent transactions on financial  
19 accounts.

20 (14) THIRD-PARTY SERVICE PROVIDER.—The  
21 term “third-party service provider” means any per-  
22 son that maintains, processes, or otherwise is per-  
23 mitted access to sensitive financial account informa-  
24 tion or sensitive personal information in connection  
25 with 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 financial account information and  
14 sensitive 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 acquisi-  
19 tion 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, maintain, and enforce its information security  
7 program, 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 financial ac-  
13 count information and sensitive personal infor-  
14 mation and assess the sufficiency of any safe-  
15 guards in place to control these risks, including  
16 consideration of risks in each relevant area of  
17 the covered entity'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 third-party service providers  
10 by—

11 (i) taking reasonable steps to select  
12 and retain third-party service providers  
13 that are capable of maintaining appro-  
14 priate safeguards for the sensitive financial  
15 account information or sensitive personal  
16 information at issue;

17 (ii) requiring third-party service pro-  
18 viders by contract to implement and main-  
19 tain such safeguards; and

20 (iii) reasonably oversee or obtain an  
21 assessment of the third-party service pro-  
22 vider's compliance with contractual obliga-  
23 tions, where appropriate in light of the  
24 covered entity's risk assessment; and

1           (E) evaluate and adjust the information  
2 security program in light of the results of the  
3 risk assessments and testing and monitoring re-  
4 quired by subparagraphs (C) and (D) and any  
5 material changes to the covered entity's oper-  
6 ations or business arrangements, or any other  
7 circumstances that the covered entity knows or  
8 has reason to know may have a material impact  
9 on its information security program.

10           (5) SECURITY CONTROLS.—Each covered entity  
11 shall—

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

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

1           (ii) access restrictions at physical lo-  
2 cations containing sensitive financial ac-  
3 count information or sensitive personal in-  
4 formation, such as buildings, computer fa-  
5 cilities, and records storage facilities, to  
6 permit access only to authorized individ-  
7 uals;

8           (iii) encryption of electronic sensitive  
9 financial account information or sensitive  
10 personal information, including while in  
11 transit or in storage on networks or sys-  
12 tems to which unauthorized individuals  
13 may have access;

14           (iv) procedures designed to ensure  
15 that information system modifications are  
16 consistent with the covered entity's infor-  
17 mation security program;

18           (v) dual control procedures, segrega-  
19 tion of duties, and employee background  
20 checks for employees with responsibilities  
21 for, or access to, sensitive financial account  
22 information or sensitive personal informa-  
23 tion;

24           (vi) monitoring systems and proce-  
25 dures to detect actual and attempted at-

1 tacks on, or intrusions into, information  
2 systems;

3 (vii) response programs that specify  
4 actions to be taken when the covered entity  
5 suspects or detects that unauthorized indi-  
6 viduals have gained access to information  
7 systems; and

8 (viii) measures to protect against de-  
9 struction, loss, or damage of sensitive fi-  
10 nancial account information or sensitive  
11 personal information due to potential envi-  
12 ronmental hazards, such as fire and water  
13 damage or technological failures;

14 (B) develop, implement, and maintain ap-  
15 propriate measures to properly dispose of sen-  
16 sitive financial account information and sen-  
17 sitive personal information; and

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

20 (6) ADMINISTRATIVE REQUIREMENTS.—

21 (A) BOARD OVERSIGHT.—If a covered enti-  
22 ty has a board of directors, the covered entity's  
23 board of directors or an appropriate committee  
24 of the board shall—

1 (i) approve the covered entity's writ-  
2 ten information security program; and

3 (ii) oversee the development, imple-  
4 mentation, and maintenance of the covered  
5 entity's information security program, in-  
6 cluding assigning specific responsibility for  
7 its implementation and reviewing reports  
8 from management.

9 (B) REPORT TO THE BOARD.—If a covered  
10 entity has a board of directors, the covered enti-  
11 ty shall report to its board or an appropriate  
12 committee of the board at least annually, in-  
13 cluding describing—

14 (i) the overall status of the informa-  
15 tion security program and the covered enti-  
16 ty's compliance with this Act; and

17 (ii) material matters related to its  
18 program, addressing issues such as risk as-  
19 sessment, risk management and control de-  
20 cisions, service provider arrangements, re-  
21 sults of testing, security breaches or viola-  
22 tions and management's responses, and  
23 recommendations for changes in the infor-  
24 mation security program.

1 (b) INVESTIGATION REQUIRED.—If a covered entity  
2 believes that a breach of data security has or may have  
3 occurred in relation to sensitive financial account informa-  
4 tion or sensitive personal information that is maintained,  
5 communicated, or otherwise handled by, or on behalf of,  
6 the covered entity, the covered entity shall conduct an in-  
7 vestigation to—

8 (1) assess the nature and scope of the incident;

9 (2) identify any sensitive financial account in-  
10 formation or sensitive personal information that may  
11 have been involved in the incident;

12 (3) determine if the sensitive financial account  
13 information or sensitive personal information has  
14 been acquired without authorization; and

15 (4) take reasonable measures to restore the se-  
16 curity and confidentiality of the systems com-  
17 promised in the breach.

18 (c) NOTICE REQUIRED.—

19 (1) IN GENERAL.—If a covered entity deter-  
20 mines under subsection (b) that the unauthorized  
21 acquisition of sensitive financial account information  
22 or sensitive personal information involved in a  
23 breach of data security is reasonably likely to cause  
24 substantial harm to the consumers to whom the in-

1 formation relates, the covered entity, or a third  
2 party acting on behalf of the covered entity, shall—

3 (A) notify, without unreasonable delay—

4 (i) an appropriate Federal law en-  
5 forcement agency;

6 (ii) the appropriate agency or author-  
7 ity identified in section 5;

8 (iii) any relevant payment card net-  
9 work, if the breach involves a breach of  
10 payment card numbers;

11 (iv) each consumer reporting agency  
12 that compiles and maintains files on con-  
13 sumers on a nationwide basis, if the breach  
14 involves sensitive personal information or  
15 sensitive financial account information re-  
16 lating to 5,000 or more consumers; and

17 (v) all consumers to whom the sen-  
18 sitive financial account information or sen-  
19 sitive personal information relates;

20 (B) provide notice to consumers by—

21 (i) written notification sent to the  
22 postal address of the consumer in the  
23 records of the covered entity;

1 (ii) telephonic notification to the num-  
2 ber of the consumer in the records of the  
3 covered entity;

4 (iii) e-mail notification to the con-  
5 sumer (or via other electronic means) in  
6 the records of the covered entity; or

7 (iv) substitute notification in print  
8 and to broadcast media where the indi-  
9 vidual whose personal information was ac-  
10 quired resides, if providing written or e-  
11 mail notification is not feasible due to—

12 (I) lack of sufficient contact in-  
13 formation for the consumers that  
14 must be notified;

15 (II) excessive cost to the covered  
16 entity; or

17 (III) exigent circumstances; and

18 (C) provide notice that includes—

19 (i) a description of the type of sen-  
20 sitive financial account information or sen-  
21 sitive personal information involved in the  
22 breach of data security;

23 (ii) a general description of the ac-  
24 tions taken by the covered entity to restore  
25 the security and confidentiality of the sen-



1 sensitive financial account information or sen-  
2 sitive personal information involved in the  
3 breach of data security; and

4 (iii) a summary of rights of victims of  
5 identity theft prepared under section  
6 609(d) of the Fair Credit Reporting Act  
7 (15 U.S.C. 1681g(d)), if the breach of  
8 data security involves sensitive personal in-  
9 formation.

10 (2) DELAY PERMITTED WHEN REQUESTED BY  
11 LAW ENFORCEMENT.—A covered entity may delay  
12 any notification described under paragraph (1) if  
13 such delay is requested by a law enforcement agen-  
14 cy.

15 (d) CLARIFICATION.—A financial institution shall  
16 have no obligation under this Act for a breach of security  
17 at another covered entity involving sensitive financial ac-  
18 count information relating to an account owned by the fi-  
19 nancial institution.

20 (e) SPECIAL NOTIFICATION REQUIREMENTS.—

21 (1) THIRD-PARTY SERVICE PROVIDERS.—In the  
22 event of a breach of security of a system maintained  
23 by a third-party service provider that has been con-  
24 tracted to maintain, store, or process data in elec-  
25 tronic form containing sensitive financial account in-

1 formation or sensitive personal information on behalf  
2 of a covered entity who owns or possesses such data,  
3 such third-party service provider shall—

4 (A) notify the covered entity; and

5 (B) notify consumers if it is agreed in  
6 writing that the third-party service provider will  
7 provide such notification on behalf of the cov-  
8 ered entity.

9 (2) CARRIER OBLIGATIONS.—

10 (A) IN GENERAL.—If a carrier becomes  
11 aware of a breach of security involving data in  
12 electronic form containing sensitive financial ac-  
13 count information or sensitive personal informa-  
14 tion that is owned or licensed by a covered enti-  
15 ty that connects to or uses a system or network  
16 provided by the carrier for the purpose of trans-  
17 mitting, routing, or providing intermediate or  
18 transient storage of such data, such carrier  
19 shall notify the covered entity who initiated  
20 such connection, transmission, routing, or stor-  
21 age of the data containing sensitive financial  
22 account information or sensitive personal infor-  
23 mation, if such covered entity can be reasonably  
24 identified. If a service provider is acting solely  
25 as a third-party service provider for purposes of

1           this subsection, the service provider has no  
2           other notification obligations under this section.

3                   (B) COVERED ENTITIES WHO RECEIVE NO-  
4           TICE FROM CARRIERS.—Upon receiving notifi-  
5           cation from a service provider under paragraph  
6           (1), a covered entity shall provide notification  
7           as required under this section.

8                   (3) COMMUNICATIONS WITH ACCOUNT HOLD-  
9           ERS.—If a covered entity that is not a financial in-  
10          stitution experiences a breach of security involving  
11          sensitive financial account information, a financial  
12          institution that issues an account to which the sen-  
13          sitive financial account information relates may com-  
14          municate with the account holder regarding the  
15          breach, including—

16                   (A) an explanation that the financial insti-  
17                  tution was not breached, and that the breach  
18                  occurred at a third-party that had access to the  
19                  consumer’s sensitive financial account informa-  
20                  tion; or

21                   (B) identify the covered entity that experi-  
22                  enced the breach after the covered entity has  
23                  provided notice consistent with this Act.

24                   (f) COMPLIANCE.—

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

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

4                   (i) subsection (a), and any regulations  
5       prescribed under subsection (a), if the fi-  
6       nancial institution maintains policies and  
7       procedures to protect the confidentiality  
8       and security of sensitive financial account  
9       information and sensitive personal infor-  
10      mation that are consistent with the policies  
11      and procedures of the financial institution  
12      that are designed to comply with the re-  
13      quirements of section 501(b) of the  
14      Gramm-Leach-Bliley Act (15 U.S.C.  
15      6801(b)) and any regulations or guidance  
16      prescribed under that section that are ap-  
17      plicable to the financial institution; and

18                   (ii) subsections (b) and (c), and any  
19      regulations prescribed under subsections  
20      (b) and (c), if the financial institution—

21                           (I)(aa) maintains policies and  
22      procedures to investigate and provide  
23      notice to consumers of breaches of  
24      data security that are consistent with  
25      the policies and procedures of the fi-

1 nancial institution that are designed  
2 to comply with the investigation and  
3 notice requirements established by  
4 regulations or guidance under section  
5 501(b) of the Gramm-Leach-Bliley  
6 Act (15 U.S.C. 6801(b)) that are ap-  
7 plicable to the financial institution;

8 (bb) is an affiliate of a bank  
9 holding company that maintains poli-  
10 cies and procedures to investigate and  
11 provide notice to consumers of  
12 breaches of data security that are con-  
13 sistent with the policies and proce-  
14 dures of a bank that is an affiliate of  
15 the financial institution, and the poli-  
16 cies and procedures of the bank are  
17 designed to comply with the investiga-  
18 tion and notice requirements estab-  
19 lished by any regulations or guidance  
20 under section 501(b) of the Gramm-  
21 Leach-Bliley Act (15 U.S.C. 6801(b))  
22 that are applicable to the bank; or

23 (cc)(AA) is an affiliate of a sav-  
24 ings and loan holding company that  
25 maintains policies and procedures to

1 investigate and provide notice to con-  
2 sumers of data breaches of data secu-  
3 rity that are consistent with the poli-  
4 cies and procedures of a savings asso-  
5 ciation that is an affiliate of the fi-  
6 nancial institution; and

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

15 (II) provides for notice to the en-  
16 tities described under clauses (ii), (iii),  
17 and (iv) of subsection (c)(1)(A), if no-  
18 tice is provided to consumers pursu-  
19 ant to the policies and procedures of  
20 the financial institution described in  
21 subclause (I); and

22 (B) subsections (a), (b), and (c)—

23 (i) if the entity is a covered entity for  
24 purposes of the regulations promulgated  
25 under section 264(c) of the Health Insur-

1           ance Portability and Accountability Act of  
2           1996 (42 U.S.C. 1320d–2 note), to the ex-  
3           tent that the entity is in compliance with  
4           such regulations; or

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

8           (2) DEFINITIONS.—In this subsection—

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

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

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

20   **SEC. 5. ADMINISTRATIVE ENFORCEMENT.**

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

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

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

12 (B) a member bank of the Federal Reserve  
13 System (other than a national bank), a branch  
14 or agency of a foreign bank (other than a Fed-  
15 eral branch, Federal agency, or insured State  
16 branch of a foreign bank), a commercial lending  
17 company owned or controlled by a foreign bank,  
18 an organization operating under section 25 or  
19 25A of the Federal Reserve Act (12 U.S.C.  
20 601, 611), or a bank holding company and its  
21 nonbank subsidiary or affiliate (other than a  
22 broker, dealer, person providing insurance, in-  
23 vestment company, or investment adviser), by  
24 the Board of Governors of the Federal Reserve  
25 System; and



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

10           (2) the Federal Credit Union Act (12 U.S.C.  
11           1751 et seq.), by the National Credit Union Admin-  
12           istration Board with respect to any federally insured  
13           credit union;

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

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

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

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

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

17           (8) State insurance law, in the case of any per-  
18 son engaged in providing insurance, by the applica-  
19 ble State insurance authority of the State in which  
20 the person is domiciled; and

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

1 (A) notwithstanding section 5(a)(2) of the  
2 Federal Trade Commission Act (15 U.S.C.  
3 45(a)(2)), common carriers subject to the Com-  
4 munications Act of 1934 (47 U.S.C. 151 et  
5 seq.);

6 (B) notwithstanding the Federal Aviation  
7 Act of 1958 (49 U.S.C. App. 1301 et seq.), in-  
8 clude the authority to enforce compliance by air  
9 carriers and foreign air carriers; and

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

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

17 (1) DATA SECURITY AND BREACH NOTIFICA-  
18 TION.—Sections 201, 202, 222, 338, and 631 of the  
19 Communications Act of 1934 (47 U.S.C. 201, 202,  
20 222, 338, and 551), and any regulations promul-  
21 gated in accordance with those sections, shall not  
22 apply with respect to the information security prac-  
23 tices, including practices relating to the notification  
24 of unauthorized access to data in electronic form, of

1 any covered entity otherwise subject to those sec-  
2 tions.

3 (2) **RULE OF CONSTRUCTION.**—Nothing in this  
4 subsection limits authority of the Federal Commu-  
5 nication Commission with respect to sections 201,  
6 202, 222, 338, and 631 of the Communications Act  
7 of 1934 (47 U.S.C. 201, 202, 222, 338, and 551).

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

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

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

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

17 (A) unauthorized access; and

18 (B) unauthorized acquisition;

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

1           (4) mitigate any potential or actual loss or  
2           harm resulting from the unauthorized acquisition of,  
3           or access to, information relating to consumers.

4 **SEC. 7. DELAYED EFFECTIVE DATE FOR CERTAIN PROVI-**  
5 **SIONS.**

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

○