

113TH CONGRESS
2D SESSION

S. 1927

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

IN THE SENATE OF THE UNITED STATES

JANUARY 15, 2014

Mr. CARPER (for himself and Mr. BLUNT) introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

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 2014”.

6 **SEC. 2. DEFINITIONS.**

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

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

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

7 (3) BREACH OF DATA SECURITY.—

8 (A) IN GENERAL.—The term “breach of
9 data security” means the unauthorized acquisition
10 of sensitive account information or sen-
11 sitive personal information.

12 (B) EXCEPTION FOR DATA THAT IS NOT IN
13 USABLE FORM.—

14 (i) IN GENERAL.—The term “breach
15 of data security” does not include the un-
16 authorized acquisition of sensitive account
17 information or sensitive personal informa-
18 tion that is maintained or communicated in
19 a manner that is not usable—

20 (I) to commit identity theft; or

21 (II) to make fraudulent trans-
22 actions on financial accounts.

23 (ii) RULE OF CONSTRUCTION.—For
24 purposes of this subparagraph, information
25 that is maintained or communicated in a

1 manner that is not usable includes any in-
2 formation that is maintained or commu-
3 nicated in an encrypted, redacted, altered,
4 edited, or coded form.

5 (4) COMMISSION.—The term “Commission”
6 means the Federal Trade Commission.

7 (5) CONSUMER.—The term “consumer” means
8 an individual.

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

16 (7) COVERED ENTITY.—

17 (A) IN GENERAL.—The term “covered en-
18 tity” means any—

19 (i) entity, the business of which is en-
20 gaging in financial activities, as described
21 in section 4(k) of the Bank Holding Com-
22 pany Act of 1956 (12 U.S.C. 1843(k));

23 (ii) financial institution, including any
24 institution described in section 313.3(k) of

1 title 16, Code of Federal Regulations, as in
2 effect on the date of enactment of this Act;

3 (iii) entity that maintains or otherwise
4 possesses information that is subject to
5 section 628 of the Fair Credit Reporting
6 Act (15 U.S.C. 1681w); or

7 (iv) other individual, partnership, cor-
8 poration, trust, estate, cooperative, associa-
9 tion, or entity that maintains or commu-
10 nicates sensitive account information or
11 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 (8) 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 (9) SENSITIVE ACCOUNT INFORMATION.—The
21 term “sensitive account information” means a finan-
22 cial account number relating to a consumer, includ-
23 ing a credit card number or debit card number, in
24 combination with any security code, access code,

1 password, or other personal identification informa-
 2 tion required to access the financial account.

3 (10) SENSITIVE PERSONAL INFORMATION.—

4 (A) IN GENERAL.—The term “sensitive
 5 personal information” means the first and last
 6 name, address, or telephone number of a con-
 7 sumer, in combination with any of the following
 8 relating to the consumer:

9 (i) Social security account number.

10 (ii) Driver’s license number or equiva-
 11 lent State identification number.

12 (iii) Taxpayer identification number.

13 (B) EXCEPTION.—The term “sensitive per-
 14 sonal information” does not include publicly
 15 available information that is lawfully made
 16 available to the general public from—

17 (i) Federal, State, or local government
 18 records; or

19 (ii) widely distributed media.

20 (11) SUBSTANTIAL HARM OR INCONVEN-
 21 IENCE.—

22 (A) IN GENERAL.—The term “substantial
 23 harm or inconvenience” means—

24 (i) material financial loss to, or civil
 25 or criminal penalties imposed on, a con-

1 consumer, due to the unauthorized use of sen-
2 sitive account information or sensitive per-
3 sonal information relating to the consumer;
4 or

5 (ii) the need for a consumer to expend
6 significant time and effort to correct erro-
7 neous information relating to the con-
8 sumer, including information maintained
9 by a consumer reporting agency, financial
10 institution, or government entity, in order
11 to avoid material financial loss, increased
12 costs, or civil or criminal penalties, due to
13 the unauthorized use of sensitive account
14 information or sensitive personal informa-
15 tion relating to the consumer.

16 (B) EXCEPTION.—The term “substantial
17 harm or inconvenience” does not include—

18 (i) changing a financial account num-
19 ber or closing a financial account; or

20 (ii) harm or inconvenience that does
21 not result from identity theft or account
22 fraud.

23 **SEC. 3. PROTECTION OF INFORMATION AND SECURITY**
24 **BREACH NOTIFICATION.**

25 (a) SECURITY PROCEDURES REQUIRED.—

1 (1) IN GENERAL.—Each covered entity shall
2 implement, maintain, and enforce reasonable policies
3 and procedures to protect the confidentiality and se-
4 curity of, sensitive account information and sensitive
5 personal information that is maintained or is being
6 communicated by or on behalf of a covered entity
7 from the unauthorized use of the information that is
8 reasonably likely to result in substantial harm or in-
9 convenience to the consumer to whom the informa-
10 tion relates.

11 (2) LIMITATION.—Any policy or procedure im-
12 plemented or maintained under paragraph (1) shall
13 be appropriate to—

14 (A) the size and complexity of the covered
15 entity;

16 (B) the nature and scope of the activities
17 of the covered entity; and

18 (C) the sensitivity of the consumer infor-
19 mation to be protected.

20 (b) INVESTIGATION REQUIRED.—

21 (1) IN GENERAL.—If a covered entity deter-
22 mines that a breach of data security has or may
23 have occurred in relation to sensitive account infor-
24 mation or sensitive personal information that is
25 maintained or is being communicated by, or on be-

1 half of, the covered entity, the covered entity shall
2 conduct an investigation to—

3 (A) assess the nature and scope of the
4 breach;

5 (B) identify any sensitive account informa-
6 tion or sensitive personal information that may
7 have been involved in the breach; and

8 (C) determine if the sensitive account in-
9 formation or sensitive personal information is
10 reasonably likely to be misused in a manner
11 causing substantial harm or inconvenience to
12 the consumers to whom the information relates.

13 (2) NEURAL NETWORKS AND INFORMATION SE-
14 CURITY PROGRAMS.—In determining the likelihood
15 of misuse of sensitive account information under
16 paragraph (1)(C), a covered entity shall consider
17 whether any neural network or security program has
18 detected, or is likely to detect or prevent, fraudulent
19 transactions resulting from the breach of security.

20 (c) NOTICE REQUIRED.—If a covered entity deter-
21 mines under subsection (b)(1)(C) that sensitive account
22 information or sensitive personal information involved in
23 a breach of data security is reasonably likely to be misused
24 in a manner causing substantial harm or inconvenience
25 to the consumers to whom the information relates, the cov-

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

3 (1) notify, in the following order—

4 (A) the appropriate agency or authority
5 identified in section 5;

6 (B) an appropriate law enforcement agen-
7 cy;

8 (C) any entity that owns, or is obligated
9 on, a financial account to which the sensitive
10 account information relates, if the breach in-
11 volves a breach of sensitive account informa-
12 tion;

13 (D) each consumer reporting agency that
14 compiles and maintains files on consumers on a
15 nationwide basis, if the breach involves sensitive
16 personal information relating to 5,000 or more
17 consumers; and

18 (E) all consumers to whom the sensitive
19 account information or sensitive personal infor-
20 mation relates; and

21 (2) take reasonable measures to restore the se-
22 curity and confidentiality of the sensitive account in-
23 formation or sensitive personal information involved
24 in the breach.

25 (d) 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 account informa-
9 tion and sensitive personal information
10 that are consistent with the policies and
11 procedures of the financial institution that
12 are designed to comply with the require-
13 ments of section 501(b) of the Gramm-
14 Leach-Bliley Act (15 U.S.C. 6801(b)) and
15 any regulations or guidance prescribed
16 under that section that are applicable to
17 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 financial 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; or

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; and

23 (II) provides for notice to the en-
24 tities described under subparagraphs
25 (B), (C), and (D) of subsection (c)(1),

1 if notice is provided to consumers pur-
2 suant to the policies and procedures
3 of the financial institution described
4 in subclause (I); and

5 (B) subsections (a), (b), and (c), if the en-
6 tity is a covered entity for purposes of the regu-
7 lations promulgated under section 264(c) of the
8 Health Insurance Portability and Accountability
9 Act of 1996 (42 U.S.C. 1320d–2 note), to the
10 extent that the entity is in compliance with
11 such regulations.

12 (2) DEFINITIONS.—For purposes of this sub-
13 section, the terms “bank holding company” and
14 “bank” shall have the same meaning given the terms
15 under section 2 of the Bank Holding Company Act
16 of 1956 (12 U.S.C. 1841).

17 **SEC. 4. IMPLEMENTING REGULATIONS.**

18 (a) IN GENERAL.—Notwithstanding any other provi-
19 sion of law, and except as provided in section 6, the agen-
20 cies and authorities identified in section 5, with respect
21 to the covered entities that are subject to the respective
22 enforcement authority of the agencies and authorities,
23 shall prescribe regulations to implement this Act.

24 (b) COORDINATION.—Each agency and authority re-
25 quired to prescribe regulations under subsection (a) shall

1 consult and coordinate with each other agency and author-
2 ity identified in section 5 so that, to the extent possible,
3 the regulations prescribed by each agency and authority
4 are consistent and comparable.

5 (c) METHOD OF PROVIDING NOTICE TO CON-
6 SUMERS.—The regulations required under subsection (a)
7 shall—

8 (1) prescribe the methods by which a covered
9 entity shall notify a consumer of a breach of data se-
10 curity under section 3; and

11 (2) allow a covered entity to provide the notice
12 by—

13 (A) written, telephonic, or e-mail notifica-
14 tion; or

15 (B) substitute notification, if providing
16 written, telephonic, or e-mail notification is not
17 feasible due to—

18 (i) lack of sufficient contact informa-
19 tion for the consumers that must be noti-
20 fied; or

21 (ii) excessive cost to the covered enti-
22 ty.

23 (d) CONTENT OF CONSUMER NOTICE.—The regula-
24 tions required under subsection (a) shall—

1 (1) prescribe the content that shall be included
2 in a notice of a breach of data security that is re-
3 quired to be provided to consumers under section 3;
4 and

5 (2) require the notice to include—

6 (A) a description of the type of sensitive
7 account information or sensitive personal infor-
8 mation involved in the breach of data security;

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

14 (C) the summary of rights of victims of
15 identity theft prepared by the Commission
16 under section 609(d) of the Fair Credit Report-
17 ing Act (15 U.S.C. 1681g(d)), if the breach of
18 data security involves sensitive personal infor-
19 mation.

20 (e) TIMING OF NOTICE.—The regulations required
21 under subsection (a) shall establish standards for when
22 a covered entity shall provide any notice required under
23 section 3.

24 (f) LAW ENFORCEMENT DELAY.—The regulations
25 required under subsection (a) shall allow a covered entity

1 to delay providing notice of a breach of data security to
2 consumers under section 3 if a law enforcement agency
3 requests such a delay in writing.

4 (g) SERVICE PROVIDERS.—The regulations required
5 under subsection (a) shall—

6 (1) require any party that maintains or commu-
7 nicates sensitive account information or sensitive
8 personal information on behalf of a covered entity to
9 provide notice to that covered entity if the party de-
10 termines that a breach of data security has, or may
11 have, occurred with respect to the sensitive account
12 information or sensitive personal information; and

13 (2) ensure that there is only 1 notification re-
14 sponsibility with respect to a breach of data security.

15 (h) TIMING OF REGULATIONS.—The regulations re-
16 quired under subsection (a) shall—

17 (1) be issued in final form not later than 6
18 months after the date of enactment of this Act; and

19 (2) take effect not later than 6 months after
20 the date on which they are issued in final form.

21 **SEC. 5. ADMINISTRATIVE ENFORCEMENT.**

22 (a) IN GENERAL.—Notwithstanding any other provi-
23 sion of law, section 3, and the regulations required under
24 section 4, shall be enforced exclusively under—

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

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

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

1 the Board of Governors of the Federal Reserve
2 System; and

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

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

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

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

23 (5) the Investment Advisers Act of 1940 (15
24 U.S.C. 80b-1 et seq.), by the Securities and Ex-
25 change Commission with respect to any investment

1 adviser registered with the Securities and Exchange
2 Commission under that Act;

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

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

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

23 (9) the Federal Trade Commission Act (15
24 U.S.C. 41 et seq.), by the Commission for any other
25 covered entity that is not subject to the jurisdiction

1 of any agency or authority described under para-
2 graphs (1) through (8).

3 (b) EXTENSION OF FEDERAL TRADE COMMISSION
4 ENFORCEMENT AUTHORITY.—The authority of the Com-
5 mission to enforce compliance with section 3, and the reg-
6 ulations required under section 4, under subsection (a)(8)
7 shall—

8 (1) notwithstanding the Federal Aviation Act of
9 1958 (49 U.S.C. App. 1301 et seq.), include the au-
10 thority to enforce compliance by air carriers and for-
11 eign air carriers; and

12 (2) notwithstanding the Packers and Stock-
13 yards Act (7 U.S.C. 181 et seq.), include the author-
14 ity to enforce compliance by persons, partnerships,
15 and corporations subject to the provisions of that
16 Act.

17 (c) NO PRIVATE RIGHT OF ACTION.—

18 (1) IN GENERAL.—This Act, and the regula-
19 tions prescribed under this Act, may not be con-
20 strued to provide a private right of action, including
21 a class action with respect to any act or practice
22 regulated under this Act.

23 (2) CIVIL AND CRIMINAL ACTIONS.—No civil or
24 criminal action relating to any act or practice gov-
25 erned under this Act, or the regulations prescribed

1 under this Act, shall be commenced or maintained in
2 any State court or under State law, including a
3 pendent State claim to an action under Federal law.

4 **SEC. 6. PROTECTION OF INFORMATION AT FEDERAL AGEN-**
5 **CIES.**

6 (a) DATA SECURITY STANDARDS.—Each agency
7 shall implement appropriate standards relating to admin-
8 istrative, technical, and physical safeguards—

9 (1) to insure the security and confidentiality of
10 the sensitive account information and sensitive per-
11 sonal information that is maintained or is being
12 communicated by, or on behalf of, that agency;

13 (2) to protect against any anticipated threats or
14 hazards to the security of the sensitive account in-
15 formation and sensitive personal information; and

16 (3) to protect against misuse of the sensitive
17 account information and sensitive personal informa-
18 tion that could result in substantial harm or incon-
19 venience to a consumer.

20 (b) SECURITY BREACH NOTIFICATION STAND-
21 ARDS.—Each agency shall implement appropriate stand-
22 ards providing for notification of consumers when the
23 agency determines that sensitive account information or
24 sensitive personal information that is maintained or is
25 being communicated by, or on behalf of, the agency—

1 (1) has been acquired without authorization;
2 and

3 (2) is reasonably likely to be misused in a man-
4 ner causing substantial harm or inconvenience to the
5 consumers to whom the information relates.

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

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

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

13 (2) safeguard information relating to consumers
14 from potential misuse;

15 (3) investigate or provide notice of the unau-
16 thorized access to information relating to consumers,
17 or the potential misuse of the information, for fraud-
18 ulent, illegal, or other purposes; or

19 (4) mitigate any loss or harm resulting from
20 the unauthorized access or misuse of information re-
21 lating to consumers.

22 **SEC. 8. DELAYED EFFECTIVE DATE FOR CERTAIN PROVI-**
23 **SIONS.**

24 (a) COVERED ENTITIES.—Sections 3 and 7 shall take
25 effect on the later of—

1 (1) 1 year after the date of enactment of this
2 Act; or

3 (2) the effective date of the final regulations re-
4 quired under section 4.

5 (b) AGENCIES.—Section 6 shall take effect 1 year
6 after the date of enactment of this Act.

○