

112TH CONGRESS
2^D SESSION

S. 3333

To require certain entities that 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 SENATE OF THE UNITED STATES

JUNE 21, 2012

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

A BILL

To require certain entities that 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.**

4 This Act may be cited as the “Data Security and
5 Breach Notification Act of 2012”.

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

2 Each covered entity shall take reasonable measures
3 to protect and secure data in electronic form containing
4 personal information.

5 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
6 **BREACH.**

7 (a) NOTIFICATION.—

8 (1) IN GENERAL.—A covered entity that owns
9 or licenses data in electronic form containing per-
10 sonal information shall give notice of any breach of
11 the security of the system following discovery by the
12 covered entity of the breach of the security of the
13 system to each individual who is a citizen or resident
14 of the United States whose personal information was
15 or that the covered entity reasonably believes to have
16 been accessed and acquired by an unauthorized per-
17 son and that the covered entity reasonably believes
18 has caused or will cause, identity theft or other fi-
19 nancial harm.

20 (2) LAW ENFORCEMENT.—A covered entity
21 shall notify the Secret Service or the Federal Bureau
22 of Investigation of the fact that a breach of security
23 has occurred if the number of individuals whose per-
24 sonal information the covered entity reasonably be-
25 lieves to have been accessed and acquired by an un-
26 authorized person exceeds 10,000.

1 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

2 (1) THIRD-PARTY AGENTS.—

3 (A) IN GENERAL.—In the event of a
4 breach of security of a system maintained by a
5 third-party entity that has been contracted to
6 maintain, store, or process data in electronic
7 form containing personal information on behalf
8 of a covered entity who owns or possesses such
9 data, such third-party entity shall notify such
10 covered entity of the breach of security.

11 (B) COVERED ENTITIES WHO RECEIVE NO-
12 TICE FROM THIRD PARTIES.—Upon receiving
13 notification from a third party under subpara-
14 graph (A), a covered entity shall provide notifi-
15 cation as required under subsection (a).

16 (C) EXCEPTION FOR SERVICE PRO-
17 VIDERS.—A service provider shall not be consid-
18 ered a third-party agent for purposes of this
19 paragraph.

20 (2) SERVICE PROVIDERS.—

21 (A) IN GENERAL.—If a service provider be-
22 comes aware of a breach of security involving
23 data in electronic form containing personal in-
24 formation that is owned or possessed by a cov-
25 ered entity that connects to or uses a system or

1 network provided by the service provider for the
2 purpose of transmitting, routing, or providing
3 intermediate or transient storage of such data,
4 such service provider shall notify the covered
5 entity who initiated such connection, trans-
6 mission, routing, or storage if such covered en-
7 tity can be reasonably identified.

8 (B) COVERED ENTITIES WHO RECEIVE NO-
9 TICE FROM SERVICE PROVIDERS.—Upon receiv-
10 ing notification from a service provider under
11 subparagraph (A), a covered entity shall provide
12 notification as required under subsection (a).

13 (c) TIMELINESS OF NOTIFICATION.—

14 (1) IN GENERAL.—Unless subject to a delay au-
15 thorized under paragraph (2), a notification required
16 under subsection (a) with respect to a security
17 breach shall be made as expeditiously as practicable
18 and without unreasonable delay, consistent with any
19 measures necessary to determine the scope of the se-
20 curity breach and restore the reasonable integrity of
21 the data system that was breached.

22 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
23 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
24 POSES.—

1 (A) LAW ENFORCEMENT.—If a Federal
2 law enforcement agency determines that the no-
3 tification required under subsection (a) would
4 impede a civil or criminal investigation, such
5 notification shall be delayed upon the written
6 request of the law enforcement agency for any
7 period which the law enforcement agency deter-
8 mines is reasonably necessary. A law enforce-
9 ment agency may, by a subsequent written re-
10 quest, revoke such delay or extend the period
11 set forth in the original request made under
12 this subparagraph by a subsequent request if
13 further delay is necessary.

14 (B) NATIONAL SECURITY.—If a Federal
15 national security agency or homeland security
16 agency determines that the notification required
17 under this section would threaten national or
18 homeland security, such notification may be de-
19 layed upon the written request of the national
20 security agency or homeland security agency for
21 any period which the national security agency
22 or homeland security agency determines is rea-
23 sonably necessary. A Federal national security
24 agency or homeland security agency may revoke
25 such delay or extend the period set forth in the

1 original request made under this subparagraph
2 by a subsequent written request if further delay
3 is necessary.

4 (d) METHOD AND CONTENT OF NOTIFICATION.—

5 (1) DIRECT NOTIFICATION.—

6 (A) METHOD OF NOTIFICATION.—A cov-
7 ered entity required to provide notification to
8 an individual under subsection (a) shall be in
9 compliance with such requirement if the covered
10 entity provides such notice by one of the fol-
11 lowing methods:

12 (i) Written notification, sent to the
13 postal address of the individual in the
14 records of the covered entity.

15 (ii) Telephone.

16 (iii) Email or other electronic means.

17 (B) CONTENT OF NOTIFICATION.—Regard-
18 less of the method by which notification is pro-
19 vided to an individual under subparagraph (A)
20 with respect to a security breach, such notifica-
21 tion, to the extent practicable, shall include—

22 (i) the date, estimated date, or esti-
23 mated date range of the breach of security;

24 (ii) a description of the personal infor-
25 mation that was accessed and acquired, or

1 reasonably believed to have been accessed
 2 and acquired, by an unauthorized person
 3 as a part of the security breach; and

4 (iii) information that the individual
 5 can use to contact the covered entity to in-
 6 quire about—

7 (I) the breach of security; or

8 (II) the information the covered
 9 entity maintained about that indi-
 10 vidual.

11 (2) SUBSTITUTE NOTIFICATION.—

12 (A) CIRCUMSTANCES GIVING RISE TO SUB-
 13 STITUTE NOTIFICATION.—A covered entity re-
 14 quired to provide notification to an individual
 15 under subsection (a) may provide substitute no-
 16 tification in lieu of the direct notification re-
 17 quired by paragraph (1) if such direct notifica-
 18 tion is not feasible due to—

19 (i) excessive cost to the covered entity
 20 required to provide such notification rel-
 21 ative to the resources of such covered enti-
 22 ty; or

23 (ii) lack of sufficient contact informa-
 24 tion for the individual required to be noti-
 25 fied.

1 (B) FORM OF SUBSTITUTE NOTIFICA-
2 TION.—Such substitute notification shall in-
3 clude at least one of the following:

4 (i) A conspicuous notice on the Inter-
5 net Web site of the covered entity (if such
6 covered entity maintains such a Web site).

7 (ii) Notification in print and to broad-
8 cast media, including major media in met-
9 ropolitan and rural areas where the indi-
10 viduals whose personal information was ac-
11 quired reside.

12 (e) TREATMENT OF PERSONS GOVERNED BY OTHER
13 FEDERAL LAW.—Except as provided in section 4(b), a
14 covered entity who is in compliance with any other Federal
15 law that requires such covered entity to provide notifica-
16 tion to individuals following a breach of security shall be
17 deemed to be in compliance with this section.

18 **SEC. 4. APPLICATION AND ENFORCEMENT.**

19 (a) GENERAL APPLICATION.—The requirements of
20 sections 2 and 3 apply to—

21 (1) those persons, partnerships, or corporations
22 over which the Commission has authority pursuant
23 to section 5(a)(2) of the Federal Trade Commission
24 Act (15 U.S.C. 45(a)(2)); and

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

5 (b) APPLICATION TO CABLE OPERATORS, SATELLITE
6 OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—
7 Sections 222, 338, and 631 of the Communications Act
8 of 1934 (47 U.S.C. 222, 338, and 551), and any regula-
9 tions promulgated thereunder, shall not apply with respect
10 to the information security practices, including practices
11 relating to the notification of unauthorized access to data
12 in electronic form, of any covered entity otherwise subject
13 to those sections.

14 (c) ENFORCEMENT BY FEDERAL TRADE COMMIS-
15 SION.—

16 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
17 TICES.—A violation of section 2 or 3 shall be treated
18 as an unfair or deceptive act or practice in violation
19 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.—

24 (A) IN GENERAL.—Except as provided in
25 subsection (a), the Commission shall enforce

1 this Act in the same manner, by the same
2 means, and with the same jurisdiction, powers,
3 and duties as though all applicable terms and
4 provisions of the Federal Trade Commission
5 Act (15 U.S.C. 41 et seq.) were incorporated
6 into and made a part of this Act.

7 (B) PRIVILEGES AND IMMUNITIES.—Any
8 person who violates section 3 or 4 shall be sub-
9 ject to the penalties and entitled to the privi-
10 leges and immunities provided in such Act.

11 (3) MAXIMUM TOTAL LIABILITY.—Notwith-
12 standing the number of actions which may be
13 brought against a covered entity under this sub-
14 section, the maximum civil penalty for which any
15 covered entity may be liable under this subsection
16 for all actions shall not exceed—

17 (A) \$500,000 for all violations of section 2
18 resulting from the same related act or omission;
19 and

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

22 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
23 this Act shall be construed to establish a private cause
24 of action against a person for a violation of this Act.

1 **SEC. 5. DEFINITIONS.**

2 In this Act:

3 (1) **BREACH OF SECURITY.**—The term “breach
4 of security” means unauthorized access and acquisi-
5 tion of data in electronic form containing personal
6 information.

7 (2) **COMMISSION.**—The term “Commission”
8 means the Federal Trade Commission.

9 (3) **COVERED ENTITY.**—

10 (A) **IN GENERAL.**—The term “covered en-
11 tity” means a sole proprietorship, partnership,
12 corporation, trust, estate, cooperative, associa-
13 tion, or other commercial entity that acquires,
14 maintains, stores, or utilizes personal informa-
15 tion.

16 (B) **EXEMPTIONS.**—The term “covered en-
17 tity” does not include the following:

18 (i) Financial institutions subject to
19 title V of the Gramm-Leach-Bliley Act (15
20 U.S.C. 6801 et seq.).

21 (ii) An entity covered by the regula-
22 tions issued under section 264(c) of the
23 Health Insurance Portability and Account-
24 ability Act of 1996 (Public Law 104–191)
25 to the extent that such entity is subject to

1 the requirements of such regulations with
2 respect to protected health information.

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

8 (5) PERSONAL INFORMATION.—

9 (A) IN GENERAL.—The term “personal in-
10 formation” means an individual’s first name or
11 first initial and last name in combination with
12 any one or more of the following data elements
13 for that individual:

14 (i) Social Security number.

15 (ii) Driver’s license number, passport
16 number, military identification number, or
17 other similar number issued on a govern-
18 ment document used to verify identity.

19 (iii) Financial account number, or
20 credit or debit card number, and any re-
21 quired security code, access code, or pass-
22 word that is necessary to permit access to
23 an individual’s financial account.

24 (B) EXCLUSIONS.—

1 (i) PUBLIC RECORD INFORMATION.—

2 Personal information does not include in-
3 formation obtained about an individual
4 which has been lawfully made publicly
5 available by a Federal, State, or local gov-
6 ernment entity or widely distributed by
7 media.

8 (ii) ENCRYPTED, REDACTED, OR SE-

9 CURED DATA.—Personal information does
10 not include information that is encrypted,
11 redacted, or secured by any other method
12 or technology that renders the data ele-
13 ments unusable.

14 (6) SERVICE PROVIDER.—The term “service
15 provider” means an entity that provides electronic
16 data transmission, routing, intermediate, and tran-
17 sient storage, or connections to its system or net-
18 work, where such entity providing such services does
19 not select or modify the content of the electronic
20 data, is not the sender or the intended recipient of
21 the data, and does not differentiate personal infor-
22 mation from other information that such entity
23 transmits, routes, stores, or for which such entity
24 provides connections. Any such entity shall be treat-
25 ed as a service provider under this Act only to the

1 extent that it is engaged in the provision of such
2 transmission, routing, intermediate and transient
3 storage, or connections.

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

5 This Act preempts any law, rule, regulation, require-
6 ment, standard, or other provision having the force and
7 effect of law of any State, or political subdivision of a
8 State, relating to the protection or security of data in elec-
9 tronic form containing personal information or the notifi-
10 cation of a breach of security.

11 **SEC. 7. EFFECTIVE DATE.**

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

○