

113TH CONGRESS
1ST SESSION

S. 1193

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 20, 2013

Mr. TOOMEY (for himself, Mr. KING, Mr. THUNE, Mr. HELLER, Mr. BLUNT, Mr. RUBIO, Mr. COATS, and Mr. ROBERTS) 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 2013”.

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 security following discovery by the covered entity of
12 the breach of security to each individual who is a cit-
13 izen or resident of the United States whose personal
14 information was or that the covered entity reason-
15 ably believes to have been accessed and acquired by
16 an unauthorized person and that the covered entity
17 reasonably believes has caused or will cause identity
18 theft or other actual financial harm.

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

26 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

1 (1) THIRD-PARTY AGENTS.—

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

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

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

19 (2) SERVICE PROVIDERS.—

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

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

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

12 (c) TIMELINESS OF NOTIFICATION.—

13 (1) IN GENERAL.—Unless subject to a delay au-
14 thorized under paragraph (3), a notification required
15 under subsection (a) with respect to a breach of se-
16 curity shall be made as expeditiously as practicable
17 and without unreasonable delay.

18 (2) REASONABLE DELAY.—For purposes of
19 paragraph (1), a delay for the purpose of allowing
20 the covered entity time to determine the scope of the
21 breach of security, to identify individuals affected by
22 the breach of security, and to restore the reasonable
23 integrity of the data system that was breached, shall
24 be considered reasonable.

1 (3) DELAY OF NOTIFICATION AUTHORIZED FOR
2 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
3 POSES.—

4 (A) LAW ENFORCEMENT.—If a Federal
5 law enforcement agency determines that the no-
6 tification required under subsection (a) would
7 interfere with a civil or criminal investigation,
8 such notification shall be delayed upon the writ-
9 ten request of the law enforcement agency for
10 any period which the law enforcement agency
11 determines is reasonably necessary. A law en-
12 forcement agency may, by a subsequent written
13 request, revoke such delay or extend the period
14 set forth in the original request made under
15 this subparagraph by a subsequent request if
16 further delay is necessary.

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

1 sonably necessary. A Federal national security
2 agency or homeland security agency may revoke
3 such delay or extend the period set forth in the
4 original request made under this subparagraph
5 by a subsequent written request if further delay
6 is necessary.

7 (d) METHOD AND CONTENT OF NOTIFICATION.—

8 (1) DIRECT NOTIFICATION.—

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

15 (i) Written notification, sent to the
16 postal address of the individual in the
17 records of the covered entity.

18 (ii) Telephone.

19 (iii) Email or other electronic means.

20 (B) CONTENT OF NOTIFICATION.—Regard-
21 less of the method by which notification is pro-
22 vided to an individual under subparagraph (A)
23 with respect to a breach of security, such notifi-
24 cation, to the extent practicable, shall include—

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

3 (ii) a description of the personal infor-
 4 mation that was accessed and acquired, or
 5 reasonably believed to have been accessed
 6 and acquired, by an unauthorized person
 7 as a part of the breach of security; and

8 (iii) information that the individual
 9 can use to contact the covered entity to in-
 10 quire about—

11 (I) the breach of security; or

12 (II) the personal information the
 13 covered entity maintained about that
 14 individual.

15 (2) SUBSTITUTE NOTIFICATION.—

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

23 (i) excessive cost to the covered entity
 24 required to provide such notification rel-

1 ative to the resources of such covered enti-
2 ty; or

3 (ii) lack of sufficient contact informa-
4 tion for the individual required to be noti-
5 fied.

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

9 (i) A conspicuous notice on the Inter-
10 net website of the covered entity (if such
11 covered entity maintains such a website).

12 (ii) Notification in print and to broad-
13 cast media, including major media in met-
14 ropolitan and rural areas where the indi-
15 viduals whose personal information was ac-
16 quired reside.

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

23 **SEC. 4. APPLICATION AND ENFORCEMENT.**

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

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

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

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

18 (c) ENFORCEMENT BY FEDERAL TRADE COMMIS-
19 SION.—

20 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
21 TICES.—A violation of section 2 or 3 shall be treated
22 as an unfair or deceptive act or practice in violation
23 of a regulation under section 18(a)(1)(B) of the
24 Federal Trade Commission Act (15 U.S.C.

1 57a(a)(1)(B)) regarding unfair or deceptive acts or
2 practices.

3 (2) POWERS OF COMMISSION.—

4 (A) IN GENERAL.—Except as provided in
5 subsection (a), the Commission shall enforce
6 this Act in the same manner, by the same
7 means, and with the same jurisdiction, powers,
8 and duties as though all applicable terms and
9 provisions of the Federal Trade Commission
10 Act (15 U.S.C. 41 et seq.) were incorporated
11 into and made a part of this Act.

12 (B) PRIVILEGES AND IMMUNITIES.—Any
13 person who violates section 2 or 3 shall be sub-
14 ject to the penalties and entitled to the privi-
15 leges and immunities provided in such Act.

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

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

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

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

6 **SEC. 5. DEFINITIONS.**

7 In this Act:

8 (1) BREACH OF SECURITY.—The term “breach
9 of security” means unauthorized access and acquisi-
10 tion of data in electronic form containing personal
11 information.

12 (2) COMMISSION.—The term “Commission”
13 means the Federal Trade Commission.

14 (3) COVERED ENTITY.—

15 (A) IN GENERAL.—The term “covered en-
16 tity” means a sole proprietorship, partnership,
17 corporation, trust, estate, cooperative, associa-
18 tion, or other commercial entity that acquires,
19 maintains, stores, or utilizes personal informa-
20 tion.

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

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

1 (ii) An entity covered by the regula-
2 tions issued under section 264(c) of the
3 Health Insurance Portability and Account-
4 ability Act of 1996 (Public Law 104–191)
5 to the extent that such entity is subject to
6 the requirements of such regulations with
7 respect to protected health information.

8 (4) DATA IN ELECTRONIC FORM.—The term
9 “data in electronic form” means any data stored
10 electronically or digitally on any computer system or
11 other database and includes recordable tapes and
12 other mass storage devices.

13 (5) PERSONAL INFORMATION.—

14 (A) IN GENERAL.—The term “personal in-
15 formation” means an individual’s first name or
16 first initial and last name in combination with
17 any 1 or more of the following data elements
18 for that individual:

19 (i) Social Security number.

20 (ii) Driver’s license number, passport
21 number, military identification number, or
22 other similar number issued on a govern-
23 ment document used to verify identity.

24 (iii) Financial account number or
25 credit or debit card number, in combina-

1 tion with any required security code, access
2 code, or password that is necessary to per-
3 mit access to an individual’s financial ac-
4 count.

5 (B) EXCLUSIONS.—

6 (i) PUBLIC RECORD INFORMATION.—

7 Personal information does not include in-
8 formation obtained about an individual
9 which has been lawfully made publicly
10 available by a Federal, State, or local gov-
11 ernment entity or widely distributed by
12 media.

13 (ii) ENCRYPTED, REDACTED, OR SE-

14 CURED DATA.—Personal information does
15 not include information that is encrypted,
16 redacted, or secured by any other method
17 or technology that removes elements that
18 personally identify an individual or that
19 otherwise renders the information unus-
20 able.

21 (6) SERVICE PROVIDER.—The term “service
22 provider” means an entity that provides electronic
23 data transmission, routing, intermediate, and tran-
24 sient storage, or connections to its system or net-
25 work, where such entity providing such services does

1 not select or modify the content of the electronic
2 data, is not the sender or the intended recipient of
3 the data, and does not differentiate personal infor-
4 mation from other information that such entity
5 transmits, routes, stores, or for which such entity
6 provides connections. Any such entity shall be treat-
7 ed as a service provider under this Act only to the
8 extent that it is engaged in the provision of such
9 transmission, routing, intermediate and transient
10 storage, or connections.

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

12 This Act preempts any law, rule, regulation, require-
13 ment, standard, or other provision having the force and
14 effect of law of any State, or political subdivision of a
15 State, relating to the protection or security of data in elec-
16 tronic form containing personal information or the notifi-
17 cation of a breach of security.

18 **SEC. 7. EFFECTIVE DATE.**

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

○