

113TH CONGRESS
2D SESSION

S. 1976

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.

IN THE SENATE OF THE UNITED STATES

JANUARY 30, 2014

Mr. ROCKEFELLER (for himself, Mrs. FEINSTEIN, Mr. PRYOR, and Mr. NELSON) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.

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 2014”.

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

7 (a) GENERAL SECURITY POLICIES AND PROCE-
8 DURES.—

1 (1) REGULATIONS.—Not later than 1 year after
2 the date of enactment of this Act, the Commission
3 shall promulgate regulations under section 553 of
4 title 5, United States Code, to require each covered
5 entity that owns or possesses data containing per-
6 sonal information, or contracts to have any third-
7 party entity maintain such data for such covered en-
8 tity, to establish and implement policies and proce-
9 dures regarding information security practices for
10 the treatment and protection of personal information
11 taking into consideration—

12 (A) the size of, and the nature, scope, and
13 complexity of the activities engaged in by such
14 covered entity;

15 (B) the current state of the art in adminis-
16 trative, technical, and physical safeguards for
17 protecting such information;

18 (C) the cost of implementing the safe-
19 guards under subparagraph (B); and

20 (D) the impact on small businesses and
21 nonprofits.

22 (2) REQUIREMENTS.—The regulations shall re-
23 quire the policies and procedures to include the fol-
24 lowing:

1 (A) A security policy with respect to the
2 collection, use, sale, other dissemination, and
3 maintenance of personal information.

4 (B) The identification of an officer or
5 other individual as the point of contact with re-
6 sponsibility for the management of information
7 security.

8 (C) A process for identifying and assessing
9 any reasonably foreseeable vulnerabilities in
10 each system maintained by the covered entity
11 that contains such personal information, which
12 shall include regular monitoring for a breach of
13 security of each such system.

14 (D) A process for taking preventive and
15 corrective action to mitigate any vulnerabilities
16 identified in the process required by subpara-
17 graph (C), which may include implementing any
18 changes to security practices and the architec-
19 ture, installation, or implementation of network
20 or operating software.

21 (E) A process for disposing of data in elec-
22 tronic form containing personal information by
23 destroying, permanently erasing, or otherwise
24 modifying the personal information contained in

1 such data to make such personal information
2 permanently unreadable or indecipherable.

3 (F) A standard method or methods for the
4 destruction of paper documents and other non-
5 electronic data containing personal information.

6 (b) LIMITATIONS.—

7 (1) COVERED ENTITIES SUBJECT TO THE
8 GRAMM-LEACH-BLILEY ACT.—A financial institution
9 that is subject to title V of the Gramm-Leach-Bliley
10 Act (15 U.S.C. 6801 et seq.) and is in compliance
11 with information security requirements under that
12 Act shall be deemed in compliance with this section.

13 (2) APPLICABILITY OF OTHER INFORMATION
14 SECURITY REQUIREMENTS.—A person who is subject
15 to, and in compliance with, the information security
16 requirements of section 13401 of the Health Infor-
17 mation Technology for Economic and Clinical
18 Health Act (42 U.S.C. 17931) or of section 1173(d)
19 of title XI, part C of the Social Security Act (42
20 U.S.C. 1320d–2(d)) shall be deemed in compliance
21 with this section with respect to any data governed
22 by section 13401 of the Health Information Tech-
23 nology for Economic and Clinical Health Act (42
24 U.S.C. 17931) or by the Health Insurance Port-

1 ability and Accountability Act of 1996 Security Rule
2 (45 C.F.R. 160.103 and Part 164).

3 (3) CERTAIN SERVICE PROVIDERS.—Nothing in
4 this section shall apply to a service provider for any
5 electronic communication by a third party to the ex-
6 tent that the service provider is engaged in the
7 transmission, routing, or temporary, intermediate, or
8 transient storage of that communication.

9 **SEC. 3. NOTIFICATION OF BREACH OF SECURITY.**

10 (a) NATIONWIDE NOTIFICATION.—A covered entity
11 that owns or possesses data in electronic form containing
12 personal information, following the discovery of a breach
13 of security of the system maintained by the covered entity
14 that contains such data, shall notify—

15 (1) each individual who is a citizen or resident
16 of the United States and whose personal information
17 was or is reasonably believed to have been acquired
18 or accessed from the covered entity as a result of the
19 breach of security; and

20 (2) the Commission, unless the covered entity
21 has notified the designated entity under section 4.

22 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

23 (1) THIRD-PARTY ENTITIES.—In the event of a
24 breach of security of a system maintained by a
25 third-party entity that has been contracted to main-

1 tain or process data in electronic form containing
2 personal information on behalf of any other covered
3 entity who owns or possesses such data, the third-
4 party entity shall notify the covered entity of the
5 breach of security. Upon receiving notification from
6 the third party entity, such covered entity shall pro-
7 vide the notification required under subsection (a).

8 (2) SERVICE PROVIDERS.—If a service provider
9 becomes aware of a breach of security of data in
10 electronic form containing personal information that
11 is owned or possessed by another covered entity that
12 connects to or uses a system or network provided by
13 the service provider for the purpose of transmitting,
14 routing, or providing intermediate or transient stor-
15 age of such data, the service provider shall notify of
16 the breach of security only the covered entity who
17 initiated such connection, transmission, routing, or
18 storage if such covered entity can be reasonably
19 identified. Upon receiving the notification from the
20 service provider, the covered entity shall provide the
21 notification required under subsection (a).

22 (3) COORDINATION OF NOTIFICATION WITH
23 CREDIT REPORTING AGENCIES.—If a covered entity
24 is required to provide notification to more than
25 5,000 individuals under subsection (a)(1), the cov-

1 ered entity also shall notify each major credit report-
2 ing agency of the timing and distribution of the no-
3 tices, except when the only personal information that
4 is the subject of the breach of security is the individ-
5 ual's first name or initial and last name, or address,
6 or phone number, in combination with a credit or
7 debit card number, and any required security code.
8 Such notice shall be given to each credit reporting
9 agency without unreasonable delay and, if it will not
10 delay notice to the affected individuals, prior to the
11 distribution of notices to the affected individuals.

12 (c) **TIMELINESS OF NOTIFICATION.**—Notification
13 under subsection (a) shall be made—

14 (1) not later than 30 days after the date of dis-
15 covery of a breach of security; or

16 (2) as promptly as possible if the covered entity
17 providing notice can show that providing notice with-
18 in the timeframe under paragraph (1) is not feasible
19 due to circumstances necessary—

20 (A) to accurately identify affected con-
21 sumers;

22 (B) to prevent further breach or unauthor-
23 ized disclosures; or

24 (C) to reasonably restore the integrity of
25 the data system.

1 (d) METHOD AND CONTENT OF NOTIFICATION.—

2 (1) DIRECT NOTIFICATION.—

3 (A) METHOD OF DIRECT NOTIFICATION.—

4 A covered entity shall be in compliance with the
5 notification requirement under subsection (a)(1)
6 if—

7 (i) the covered entity provides con-
8 spicuous and clearly identified notifica-
9 tion—

10 (I) in writing; or

11 (II) by e-mail or other electronic
12 means if—

13 (aa) the covered entity's pri-
14 mary method of communication
15 with the individual is by e-mail or
16 such other electronic means; or

17 (bb) the individual has con-
18 sented to receive notification by
19 e-mail or such other electronic
20 means and such notification is
21 provided in a manner that is con-
22 sistent with the provisions per-
23 mitting electronic transmission of
24 notices under section 101 of the
25 Electronic Signatures in Global

1 and National Commerce Act (15
2 U.S.C. 7001); and

3 (ii) the method of notification selected
4 under clause (i) can reasonably be expected
5 to reach the intended individual.

6 (B) CONTENT OF DIRECT NOTIFICA-
7 TION.—Each method of direct notification
8 under subparagraph (A) shall include—

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

11 (ii) a description of the personal infor-
12 mation that was or is reasonably believed
13 to have been acquired or accessed as a re-
14 sult of the breach of security;

15 (iii) a telephone number that an indi-
16 vidual can use at no cost to the individual
17 to contact the covered entity to inquire
18 about the breach of security or the infor-
19 mation the covered entity maintained
20 about that individual;

21 (iv) notice that the individual may be
22 entitled to consumer credit reports under
23 subsection (e)(1);

1 (v) instructions how an individual can
2 request consumer credit reports under sub-
3 section (e)(1);

4 (vi) a telephone number, that an indi-
5 vidual can use at no cost to the individual,
6 and an address to contact each major cred-
7 it reporting agency; and

8 (vii) a telephone number, that an indi-
9 vidual can use at no cost to the individual,
10 and an Internet Web site address to obtain
11 information regarding identity theft from
12 the Commission.

13 (2) SUBSTITUTE NOTIFICATION.—

14 (A) CIRCUMSTANCES GIVING RISE TO SUB-
15 STITUTE NOTIFICATION.—A covered entity re-
16 quired to provide notification to individuals
17 under subsection (a)(1) may provide substitute
18 notification instead of direct notification under
19 paragraph (1)—

20 (i) if direct notification is not feasible
21 due to lack of sufficient contact informa-
22 tion for the individual required to be noti-
23 fied; or

24 (ii) if the covered entity owns or pos-
25 sesses data in electronic form containing

1 personal information of fewer than 10,000
2 individuals and direct notification is not
3 feasible due to excessive cost to the covered
4 entity required to provide such notification
5 relative to the resources of such covered
6 entity, as determined in accordance with
7 the regulations issued by the Commission
8 under paragraph (3)(A).

9 (B) METHOD OF SUBSTITUTE NOTIFICA-
10 TION.—Substitute notification under this para-
11 graph shall include—

12 (i) conspicuous and clearly identified
13 notification by e-mail to the extent the cov-
14 ered entity has an e-mail address for an in-
15 dividual who is entitled to notification
16 under subsection (a)(1);

17 (ii) conspicuous and clearly identified
18 notification on the Internet Web site of the
19 covered entity if the covered entity main-
20 tains an Internet Web site; and

21 (iii) notification to print and to broad-
22 cast media, including major media in met-
23 ropolitan and rural areas where the indi-
24 viduals whose personal information was ac-
25 quired reside.

1 (C) CONTENT OF SUBSTITUTE NOTIFICA-
2 TION.—Each method of substitute notification
3 under this paragraph shall include—

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

6 (ii) a description of the types of per-
7 sonal information that were or are reason-
8 ably believed to have been acquired or
9 accessed as a result of the breach of secu-
10 rity;

11 (iii) notice that an individual may be
12 entitled to consumer credit reports under
13 subsection (e)(1);

14 (iv) instructions how an individual can
15 request consumer credit reports under sub-
16 section (e)(1);

17 (v) a telephone number that an indi-
18 vidual can use at no cost to the individual
19 to learn whether the individual's personal
20 information is included in the breach of se-
21 curity;

22 (vi) a telephone number, that an indi-
23 vidual can use at no cost to the individual,
24 and an address to contact each major cred-
25 it reporting agency; and

1 (vii) a telephone number, that an indi-
2 vidual can use at no cost to the individual,
3 and an Internet Web site address to obtain
4 information regarding identity theft from
5 the Commission.

6 (3) REGULATIONS AND GUIDANCE.—

7 (A) REGULATIONS.—Not later than 1 year
8 after the date of enactment of this Act, the
9 Commission, by regulation under section 553 of
10 title 5, United States Code, shall establish cri-
11 teria for determining circumstances under
12 which substitute notification may be provided
13 under section 3(d)(2) of this Act, including cri-
14 teria for determining if direct notification under
15 section 3(d)(1) of this Act is not feasible due to
16 excessive costs to the covered entity required to
17 provide such notification relative to the re-
18 sources of such covered entity. The regulations
19 may also identify other circumstances where
20 substitute notification would be appropriate, in-
21 cluding circumstances under which the cost of
22 providing direct notification exceeds the benefits
23 to consumers.

24 (B) GUIDANCE.—In addition, the Commis-
25 sion, in consultation with the Small Business

1 Administration, shall provide and publish gen-
2 eral guidance with respect to compliance with
3 this subsection. The guidance shall include—

4 (i) a description of written or e-mail
5 notification that complies with paragraph
6 (1); and

7 (ii) guidance on the content of sub-
8 stitute notification under paragraph (2),
9 including the extent of notification to print
10 and broadcast media that complies with
11 paragraph (2)(B)(iii).

12 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

13 (1) IN GENERAL.—Not later than 60 days after
14 the date of request by an individual who received no-
15 tification under subsection (a)(1) and quarterly
16 thereafter for 2 years, a covered entity required to
17 provide notification under subsection (a)(1) shall
18 provide, or arrange for the provision of, to the indi-
19 vidual at no cost, consumer credit reports from at
20 least 1 major credit reporting agency.

21 (2) LIMITATION.—This subsection shall not
22 apply if the only personal information that is the
23 subject of the breach of security is the individual's
24 first name or initial and last name, or address, or

1 phone number, in combination with a credit or debit
2 card number, and any required security code.

3 (3) RULEMAKING.—The Commission’s rule-
4 making under subsection (d)(3) shall include—

5 (A) determination of the circumstances
6 under which a covered entity required to pro-
7 vide notification under subsection (a)(1) must
8 provide or arrange for the provision of free con-
9 sumer credit reports; and

10 (B) establishment of a simple process
11 under which a covered entity that is a small
12 business or small non-profit organization may
13 request a full or a partial waiver or a modified
14 or an alternative means of complying with this
15 subsection if providing free consumer credit re-
16 ports is not feasible due to excessive costs rel-
17 ative to the resources of such covered entity
18 and relative to the level of harm, to affected in-
19 dividuals, caused by the breach of security.

20 (f) DELAY OF NOTIFICATION AUTHORIZED FOR NA-
21 TIONAL SECURITY AND LAW ENFORCEMENT PUR-
22 POSES.—

23 (1) IN GENERAL.—If the United States Secret
24 Service or the Federal Bureau of Investigation de-
25 termines that notification under this section would

1 impede a criminal investigation or a national secu-
2 rity activity, notification shall be delayed upon writ-
3 ten notice from the United States Secret Service or
4 the Federal Bureau of Investigation to the covered
5 entity that experienced the breach of security. Writ-
6 ten notice from the United States Secret Service or
7 the Federal Bureau of Investigation shall specify the
8 period of delay requested for national security or law
9 enforcement purposes.

10 (2) SUBSEQUENT DELAY OF NOTIFICATION.—

11 (A) IN GENERAL.—A covered entity shall
12 provide notification under this section not later
13 than 30 days after the day that the delay was
14 invoked unless a Federal law enforcement or in-
15 telligence agency provides subsequent written
16 notice to the covered entity that further delay
17 is necessary.

18 (B) WRITTEN JUSTIFICATION REQUIRE-
19 MENTS.—

20 (i) UNITED STATES SECRET SERV-
21 ICE.—If the United States Secret Service
22 instructs a covered entity to delay notifica-
23 tion under this section beyond the 30-day
24 period under subparagraph (A) (referred
25 to in this clause as “subsequent delay”),

1 the United States Secret Service shall sub-
2 mit written justification for the subsequent
3 delay to the Secretary of Homeland Secu-
4 rity before the subsequent delay begins.

5 (ii) FEDERAL BUREAU OF INVESTIGA-
6 TION.—If the Federal Bureau of Investiga-
7 tion instructs a covered entity to delay no-
8 tification under this section beyond the 30-
9 day period under subparagraph (A) (re-
10 ferred to in this clause as “subsequent
11 delay”), the Federal Bureau of Investiga-
12 tion shall submit written justification for
13 the subsequent delay to the Attorney Gen-
14 eral before the subsequent delay begins.

15 (3) LAW ENFORCEMENT IMMUNITY.—No cause
16 of action shall lie in any court against any Federal
17 agency for acts relating to the delay of notification
18 for national security or law enforcement purposes
19 under this Act.

20 (g) GENERAL EXEMPTION.—

21 (1) IN GENERAL.—A covered entity shall be ex-
22 empt from the requirements under this section if,
23 following a breach of security, the covered entity
24 reasonably concludes that there is no reasonable risk
25 of identity theft, fraud, or other unlawful conduct.

1 (2) PRESUMPTION.—

2 (A) IN GENERAL.—There shall be a pre-
3 sumption that no reasonable risk of identity
4 theft, fraud, or other unlawful conduct exists
5 following a breach of security if—

6 (i) the data is rendered unusable,
7 unreadable, or indecipherable through a se-
8 curity technology or methodology; and

9 (ii) the security technology or method-
10 ology under clause (i) is generally accepted
11 by experts in the information security field.

12 (B) REBUTTAL.—The presumption under
13 subparagraph (A) may be rebutted by facts
14 demonstrating that the security technology or
15 methodology in a specific case has been or is
16 reasonably likely to be compromised.

17 (3) TECHNOLOGIES OR METHODOLOGIES.—Not
18 later than 1 year after the date of enactment of this
19 Act, and biennially thereafter, the Commission, after
20 consultation with the National Institute of Stand-
21 ards and Technology, shall issue rules (pursuant to
22 section 553 of title 5, United States Code) or guid-
23 ance to identify each security technology and meth-
24 odology under paragraph (2). In identifying each
25 such security technology and methodology, the Com-

1 mission and the National Institute of Standards and
2 Technology shall—

3 (A) consult with relevant industries, con-
4 sumer organizations, data security and identity
5 theft prevention experts, and established stand-
6 ards setting bodies; and

7 (B) consider whether and in what cir-
8 cumstances a security technology or method-
9 ology currently in use, such as encryption, com-
10 plies with the standards under paragraph (2).

11 (4) FTC GUIDANCE.—Not later than 1 year
12 after the date of enactment of this Act, the Commis-
13 sion, after consultation with the National Institute
14 of Standards and Technology, shall issue guidance
15 regarding the application of the exemption under
16 paragraph (1).

17 (h) EXEMPTIONS FOR NATIONAL SECURITY AND
18 LAW ENFORCEMENT PURPOSES.—

19 (1) IN GENERAL.—A covered entity shall be ex-
20 empt from the requirements under this section if—

21 (A) a determination is made—

22 (i) by the United States Secret Serv-
23 ice or the Federal Bureau of Investigation
24 that notification of the breach of security
25 could be reasonably expected to reveal sen-

1 sitive sources and methods or similarly im-
2 pede the ability of the Government to con-
3 duct law enforcement or intelligence inves-
4 tigations; or

5 (ii) by the Federal Bureau of Inves-
6 tigation that notification of the breach of
7 security could be reasonably expected to
8 cause damage to the national security; and

9 (B) the United States Secret Service or the
10 Federal Bureau of Investigation, as the case
11 may be, provides written notice of its deter-
12 mination under subparagraph (A) to the cov-
13 ered entity.

14 (2) UNITED STATES SECRET SERVICE.—If the
15 United States Secret Service invokes an exemption
16 under paragraph (1), the United States Secret Serv-
17 ice shall submit written justification for invoking the
18 exemption to the Secretary of Homeland Security
19 before the exemption is invoked.

20 (3) FEDERAL BUREAU OF INVESTIGATION.—If
21 the Federal Bureau of Investigation invokes an ex-
22 emption under paragraph (1), the Federal Bureau of
23 Investigation shall submit written justification for
24 invoking the exemption to the Attorney General be-
25 fore the exemption is invoked.

1 (4) IMMUNITY.—No cause of action shall lie in
2 any court against any Federal agency for acts relat-
3 ing to the exemption from notification for national
4 security or law enforcement purposes under this Act.

5 (5) REPORTS.—Not later than 18 months after
6 the date of enactment of this Act, and upon request
7 by Congress thereafter, the United States Secret
8 Service and Federal Bureau of Investigation shall
9 submit to Congress a report on the number and na-
10 ture of breaches of security subject to the exemp-
11 tions for national security and law enforcement pur-
12 poses under this subsection.

13 (i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

14 (1) IN GENERAL.—A covered entity shall be ex-
15 empt from the requirements under this section if the
16 covered entity utilizes or participates in a security
17 program that—

18 (A) effectively blocks the use of the per-
19 sonal information to initiate an unauthorized fi-
20 nancial transaction before it is charged to the
21 account of the individual; and

22 (B) provides notice to each affected indi-
23 vidual after a breach of security that resulted in
24 attempted fraud or an attempted unauthorized
25 transaction.

1 (2) LIMITATIONS.—An exemption under para-
2 graph (1) shall not apply if—

3 (A) the breach of security includes per-
4 sonal information, other than a credit card
5 number or credit card security code, of any
6 type; or

7 (B) the breach of security includes both
8 the individual's credit card number and the in-
9 dividual's first and last name.

10 (j) FINANCIAL INSTITUTIONS REGULATED BY FED-
11 ERAL FUNCTIONAL REGULATORS.—

12 (1) IN GENERAL.—A covered financial institu-
13 tion shall be deemed in compliance with this section
14 if—

15 (A) the Federal functional regulator with
16 jurisdiction over the covered financial institu-
17 tion has issued a standard by regulation or
18 guideline under title V of the Gramm-Leach-
19 Bliley Act (15 U.S.C. 6801 et seq.) that—

20 (i) requires financial institutions with-
21 in its jurisdiction to provide notification to
22 individuals following a breach of security;
23 and

1 (ii) provides protections substantially
2 similar to, or greater than, those required
3 under this Act; and

4 (B) the covered financial institution is in
5 compliance with the standard under subpara-
6 graph (A).

7 (2) DEFINITIONS.—In this subsection—

8 (A) the term “covered financial institu-
9 tion” means a financial institution that is sub-
10 ject to—

11 (i) the data security requirements of
12 the Gramm-Leach-Bliley Act (15 U.S.C.
13 6801 et seq.);

14 (ii) any implementing standard issued
15 by regulation or guideline issued under
16 that Act; and

17 (iii) the jurisdiction of a Federal func-
18 tional regulator under that Act;

19 (B) the term “Federal functional regu-
20 lator” has the meaning given the term in sec-
21 tion 509 of the Gramm-Leach-Bliley Act (15
22 U.S.C. 6809); and

23 (C) the term “financial institution” has
24 the meaning given the term in section 509 of
25 the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

1 (k) EXEMPTION; HEALTH PRIVACY.—

2 (1) COVERED ENTITY OR BUSINESS ASSOCIATE
3 UNDER HITECH ACT.—To the extent that a covered
4 entity under this Act acts as a covered entity or a
5 business associate under section 13402 of the
6 Health Information Technology for Economic and
7 Clinical Health Act (42 U.S.C. 17932), has the obli-
8 gation to provide notification to individuals following
9 a breach of security under that Act or its imple-
10 menting regulations, and is in compliance with that
11 obligation, the covered entity shall be deemed in
12 compliance with this section.

13 (2) ENTITY SUBJECT TO HITECH ACT.—To the
14 extent that a covered entity under this Act acts as
15 a vendor of personal health records, a third party
16 service provider, or other entity subject to section
17 13407 of the Health Information Technology for Ec-
18 onomical and Clinical Health Act (42 U.S.C.
19 17937), has the obligation to provide notification to
20 individuals following a breach of security under that
21 Act or its implementing regulations, and is in com-
22 pliance with that obligation, the covered entity shall
23 be deemed in compliance with this section.

24 (3) LIMITATION OF STATUTORY CONSTRUC-
25 TION.—Nothing in this Act may be construed in any

1 way to give effect to the sunset provision under sec-
2 tion 13407(g)(2) of the Health Information Tech-
3 nology for Economic and Clinical Health Act (42
4 U.S.C. 17937(g)(2)) or to otherwise limit or affect
5 the applicability, under section 13407 of that Act, of
6 the requirement to provide notification to individuals
7 following a breach of security for vendors of personal
8 health records and each entity described in clause
9 (ii), (iii), or (iv) of section 13424(b)(1)(A) of that
10 Act (42 U.S.C. 17953(b)(1)(A)).

11 (l) WEB SITE NOTICE OF FEDERAL TRADE COMMIS-
12 SION.—If the Commission, upon receiving notification of
13 any breach of security that is reported to the Commission,
14 finds that notification of the breach of security via the
15 Commission’s Internet Web site would be in the public in-
16 terest or for the protection of consumers, the Commission
17 shall place such a notice in a clear and conspicuous loca-
18 tion on its Internet Web site.

19 (m) FTC STUDY ON NOTIFICATION IN LANGUAGES
20 IN ADDITION TO ENGLISH.—Not later than 1 year after
21 the date of enactment of this Act, the Commission shall
22 conduct a study on the practicality and cost effectiveness
23 of requiring the direct notification required by subsection
24 (d)(1) to be provided in a language in addition to English
25 to individuals known to speak only such other language.

1 (n) GENERAL RULEMAKING AUTHORITY.—The Com-
2 mission may promulgate regulations necessary under sec-
3 tion 553 of title 5, United States Code, to effectively en-
4 force the requirements of this section.

5 **SEC. 4. NOTICE TO LAW ENFORCEMENT.**

6 (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-
7 CEIVE NOTICE.—Not later than 60 days after the date
8 of enactment of this Act, the Secretary of the Department
9 of Homeland Security shall designate a Federal Govern-
10 ment entity to receive notice under this section.

11 (b) NOTICE.—A covered entity shall notify the des-
12 ignated entity of a breach of security if—

13 (1) the number of individuals whose personal
14 information was, or is reasonably believed to have
15 been, acquired or assessed as a result of the breach
16 of security exceeds 10,000;

17 (2) the breach of security involves a database,
18 networked or integrated databases, or other data
19 system containing the personal information of more
20 than 1,000,000 individuals;

21 (3) the breach of security involves databases
22 owned by the Federal Government; or

23 (4) the breach of security involves primarily
24 personal information of individuals known to the
25 covered entity to be employees or contractors of the

1 Federal Government involved in national security or
2 law enforcement.

3 (c) CONTENT OF NOTICES.—

4 (1) IN GENERAL.—Each notice under sub-
5 section (b) shall contain—

6 (A) the date, estimated date, or estimated
7 date range of the breach of security;

8 (B) a description of the nature of the
9 breach of security;

10 (C) a description of each type of personal
11 information that was or is reasonably believed
12 to have been acquired or accessed as a result of
13 the breach of security; and

14 (D) a statement of each paragraph under
15 subsection (b) that applies to the breach of se-
16 curity.

17 (2) CONSTRUCTION.—Nothing in this section
18 shall be construed to require a covered entity to re-
19 veal specific or identifying information about an in-
20 dividual as part of the notice under paragraph (1).

21 (d) RESPONSIBILITIES OF THE DESIGNATED ENTI-
22 TY.—The designated entity shall promptly provide each
23 notice it receives under subsection (b) to—

24 (1) the United States Secret Service;

25 (2) the Federal Bureau of Investigation;

1 (3) the Federal Trade Commission;

2 (4) the United States Postal Inspection Service,
3 if the breach of security involves mail fraud;

4 (5) the attorney general of each State affected
5 by the breach of security; and

6 (6) as appropriate, other Federal agencies for
7 law enforcement, national security, or data security
8 purposes.

9 (e) **TIMING OF NOTICES.**—Notice under this section
10 shall be delivered as follows:

11 (1) Notice under subsection (b) shall be deliv-
12 ered as promptly as possible, but—

13 (A) not less than 3 business days before
14 notification to an individual under section 3;
15 and

16 (B) not later than 10 days after the date
17 of discovery of the events requiring notice.

18 (2) Notice under subsection (d) shall be deliv-
19 ered as promptly as possible, but not later than 1
20 business day after the date that the designated enti-
21 ty receives notice of a breach of security from a cov-
22 ered entity.

23 **SEC. 5. APPLICATION AND ENFORCEMENT.**

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

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

5 (2) notwithstanding sections 4 and 5(a)(2) of
6 the Federal Trade Commission Act (15 U.S.C. 44
7 and 45(a)(2)), any non-profit organization, including
8 any organization described in section 501(c) of the
9 Internal Revenue Code of 1986 that is exempt from
10 taxation under section 501(a) of the Internal Rev-
11 enue Code of 1986.

12 (b) OPT-IN FOR CERTAIN OTHER ENTITIES.—

13 (1) IN GENERAL.—Notwithstanding sections 4
14 and 5(a)(2) of the Federal Trade Commission Act
15 (15 U.S.C. 44 and 45(a)(2)), the requirements of
16 section 3 shall apply to any other covered entity not
17 included under subsection (a) that enters into an
18 agreement with the Commission under which that
19 covered entity would be subject to section 3 with re-
20 spect to any acts or omissions that occur while the
21 agreement is in effect and that may constitute a vio-
22 lation of section 3, if—

23 (A) not less than 30 days prior to entering
24 into the agreement with the person or entity,
25 the Commission publishes notice in the Federal

1 Register of the Commission's intent to enter
2 into the agreement; and

3 (B) not later than 14 business days after
4 entering into the agreement with the person or
5 entity, the Commission publishes in the Federal
6 Register—

7 (i) notice of the agreement;

8 (ii) the identity of each person or enti-
9 ty covered by the agreement; and

10 (iii) the effective date of the agree-
11 ment.

12 (2) CONSTRUCTION.—

13 (A) OTHER FEDERAL LAW.—An agreement
14 under paragraph (1) shall not effect a covered
15 entity's obligation to provide notice of a breach
16 of security or similar event under any other
17 Federal law.

18 (B) NO PREEMPTION PRIOR TO VALID
19 AGREEMENT.—Subsections (a)(2) and (b) of
20 section 7 shall not apply to a breach of security
21 that occurs before a valid agreement under
22 paragraph (1) is in effect.

23 (c) ENFORCEMENT BY THE FEDERAL TRADE COM-
24 MISSION.—

1 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
2 TICES.—A violation of section 2 or 3 of this Act
3 shall be treated as an unfair and deceptive act or
4 practice in violation of a regulation under section
5 18(a)(1)(B) of the Federal Trade Commission Act
6 (15 U.S.C. 57a(a)(1)(B)) regarding unfair or decep-
7 tive acts or practices.

8 (2) POWERS OF COMMISSION.—The Commis-
9 sion shall enforce this Act in the same manner, by
10 the same means, with the same jurisdiction, except
11 as provided in subsections (a)(2) and (b) of this sec-
12 tion, and with the same powers and duties as though
13 all applicable terms and provisions of the Federal
14 Trade Commission Act (15 U.S.C. 41 et seq.) were
15 incorporated into and made a part of this Act. Any
16 covered entity who violates such regulations shall be
17 subject to the penalties and entitled to the privileges
18 and immunities provided in that Act.

19 (3) LIMITATION.—In promulgating rules under
20 this Act, the Commission shall not require the de-
21 ployment or use of any specific products or tech-
22 nologies, including any specific computer software or
23 hardware.

24 (d) ENFORCEMENT BY STATE ATTORNEYS GEN-
25 ERAL.—

1 (1) CIVIL ACTION.—In any case in which the
2 attorney general of a State, or an official or agency
3 of a State, has reason to believe that an interest of
4 the residents of that State has been or is threatened
5 or adversely affected by any covered entity who vio-
6 lates section 2 or section 3 of this Act, the attorney
7 general, official, or agency of the State, as *parens*
8 *patriae*, may bring a civil action on behalf of the
9 residents of the State in a district court of the
10 United States of appropriate jurisdiction—

11 (A) to enjoin further violation of such sec-
12 tion by the defendant;

13 (B) to compel compliance with such sec-
14 tion; or

15 (C) to obtain civil penalties in the amount
16 determined under paragraph (2).

17 (2) CIVIL PENALTIES.—

18 (A) CALCULATION.—

19 (i) TREATMENT OF VIOLATIONS OF
20 SECTION 2.—For purposes of paragraph
21 (1)(C) with regard to a violation of section
22 2, the amount determined under this para-
23 graph is the amount calculated by multi-
24 plying the number of days that a covered
25 entity is not in compliance with such sec-

1 tion by an amount not greater than
2 \$11,000.

3 (ii) TREATMENT OF VIOLATIONS OF
4 SECTION 3.—For purposes of paragraph
5 (1)(C) with regard to a violation of section
6 3, the amount determined under this para-
7 graph is the amount calculated by multi-
8 plying the number of violations of such
9 section by an amount not greater than
10 \$11,000. Each failure to send notification
11 as required under section 3 to a resident of
12 the State shall be treated as a separate
13 violation.

14 (B) ADJUSTMENT FOR INFLATION.—Be-
15 ginning on the date that the Consumer Price
16 Index is first published by the Bureau of Labor
17 Statistics that is after 1 year after the date of
18 enactment of this Act, and each year thereafter,
19 the amounts specified in clauses (i) and (ii) of
20 subparagraph (A) and in clauses (i) and (ii) of
21 subparagraph (C) shall be increased by the per-
22 centage increase in the Consumer Price Index
23 published on that date from the Consumer
24 Price Index published the previous year.

1 (C) MAXIMUM TOTAL LIABILITY.—Not-
2 withstanding the number of actions which may
3 be brought against a covered entity under this
4 subsection, the maximum civil penalty for which
5 any covered entity may be liable under this sub-
6 section shall not exceed—

7 (i) \$5,000,000 for each violation of
8 section 2; and

9 (ii) \$5,000,000 for all violations of
10 section 3 resulting from a single breach of
11 security.

12 (3) INTERVENTION BY THE FTC.—

13 (A) NOTICE AND INTERVENTION.—The
14 State shall provide prior written notice of any
15 action under paragraph (1) to the Commission
16 and provide the Commission with a copy of its
17 complaint, except in any case in which such
18 prior notice is not feasible, in which case the
19 State shall serve such notice immediately upon
20 commencing such action. The Commission shall
21 have the right—

22 (i) to intervene in the action;

23 (ii) upon so intervening, to be heard
24 on all matters arising therein; and

25 (iii) to file petitions for appeal.

1 (B) LIMITATION ON STATE ACTION WHILE
2 FEDERAL ACTION IS PENDING.—If the Commis-
3 sion has instituted a civil action for violation of
4 this Act, no State attorney general, or official
5 or agency of a State, may bring an action under
6 this subsection during the pendency of that ac-
7 tion against any defendant named in the com-
8 plaint of the Commission for any violation of
9 this Act alleged in the complaint.

10 (4) CONSTRUCTION.—For purposes of bringing
11 any civil action under paragraph (1), nothing in this
12 Act shall be construed to prevent an attorney gen-
13 eral of a State from exercising the powers conferred
14 on the attorney general by the laws of that State—

15 (A) to conduct investigations;

16 (B) to administer oaths or affirmations; or

17 (C) to compel the attendance of witnesses

18 or the production of documentary and other evi-

19 dence.

20 (e) NOTICE TO LAW ENFORCEMENT; CIVIL EN-
21 FORCEMENT BY ATTORNEY GENERAL.—

22 (1) IN GENERAL.—The Attorney General may
23 bring a civil action in the appropriate United States
24 district court against any covered entity that en-

1 gages in conduct constituting a violation of section
2 4.

3 (2) PENALTIES.—

4 (A) IN GENERAL.—Upon proof of such
5 conduct by a preponderance of the evidence, a
6 covered entity shall be subject to a civil penalty
7 of not more than \$1,000 per individual whose
8 personal information was or is reasonably be-
9 lieved to have been accessed or acquired as a
10 result of the breach of security that is the basis
11 of the violation, up to a maximum of \$100,000
12 per day while such violation persists.

13 (B) LIMITATIONS.—The total amount of
14 the civil penalty assessed under this subsection
15 against a covered entity for acts or omissions
16 relating to a single breach of security shall not
17 exceed \$1,000,000, unless the conduct consti-
18 tuting a violation of section 4 was willful or in-
19 tentional, in which case an additional civil pen-
20 alty of up to \$1,000,000 may be imposed.

21 (C) ADJUSTMENT FOR INFLATION.—Be-
22 ginning on the date that the Consumer Price
23 Index is first published by the Bureau of Labor
24 Statistics that is after 1 year after the date of
25 enactment of this Act, and each year thereafter,

1 tionally and willfully conceals the fact of the breach of se-
 2 curity, shall, in the event that the breach of security re-
 3 sults in economic harm to any individual in the amount
 4 of \$1,000 or more, be fined under this title, imprisoned
 5 for not more than 5 years, or both.

6 “(b) PERSON DEFINED.—For purposes of subsection
 7 (a), the term ‘person’ has the same meaning as in section
 8 1030(e)(12) of this title.

9 “(c) ENFORCEMENT AUTHORITY.—

10 “(1) IN GENERAL.—The United States Secret
 11 Service and the Federal Bureau of Investigation
 12 shall have the authority to investigate offenses under
 13 this section.

14 “(2) CONSTRUCTION.—The authority granted
 15 in paragraph (1) shall not be exclusive of any exist-
 16 ing authority held by any other Federal agency.”.

17 (2) CONFORMING AND TECHNICAL AMEND-
 18 MENTS.—The table of sections for chapter 47 of title
 19 18, United States Code, is amended by adding at
 20 the end the following:

“1041. Concealment of breaches of security involving personal information.”.

21 **SEC. 6. DEFINITIONS.**

22 In this Act:

23 (1) BREACH OF SECURITY.—

24 (A) IN GENERAL.—The term “breach of
 25 security” means compromise of the security,

1 confidentiality, or integrity of, or loss of, data
2 in electronic form that results in, or there is a
3 reasonable basis to conclude has resulted in,
4 unauthorized access to or acquisition of per-
5 sonal information from a covered entity.

6 (B) EXCLUSIONS.—The term “breach of
7 security” does not include—

8 (i) a good faith acquisition of personal
9 information by a covered entity, or an em-
10 ployee or agent of a covered entity, if the
11 personal information is not subject to fur-
12 ther use or unauthorized disclosure;

13 (ii) any lawfully authorized investiga-
14 tive, protective, or intelligence activity of a
15 law enforcement or an intelligence agency
16 of the United States, a State, or a political
17 subdivision of a State; or

18 (iii) the release of a public record not
19 otherwise subject to confidentiality or non-
20 disclosure requirements.

21 (2) COMMISSION.—The term “Commission”
22 means the Federal Trade Commission.

23 (3) COVERED ENTITY.—The term “covered en-
24 tity” means a sole proprietorship, partnership, cor-
25 poration, trust, estate, cooperative, association, or

1 other commercial entity, and any charitable, edu-
2 cational, or nonprofit organization, that acquires,
3 maintains, or utilizes personal information.

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

9 (5) DESIGNATED ENTITY.—The term “des-
10 ignated entity” means the Federal Government enti-
11 ty designated by the Secretary of Homeland Security
12 under section 4.

13 (6) ENCRYPTION.—The term “encryption”
14 means the protection of data in electronic form in
15 storage or in transit using an encryption technology
16 that has been adopted by an established standards
17 setting body which renders such data indecipherable
18 in the absence of associated cryptographic keys nec-
19 essary to enable decryption of such data. Such
20 encryption must include appropriate management
21 and safeguards of such keys to protect the integrity
22 of the encryption.

23 (7) IDENTITY THEFT.—The term “identity
24 theft” means the unauthorized use of another per-
25 son’s personal information for the purpose of engag-

1 ing in commercial transactions under the identity of
2 such other person, including any contact that vio-
3 lates section 1028A of title 18, United States Code.

4 (8) MAJOR CREDIT REPORTING AGENCY.—The
5 term “major credit reporting agency” means a con-
6 sumer reporting agency that compiles and maintains
7 files on consumers on a nationwide basis within the
8 meaning of section 603(p) of the Fair Credit Re-
9 porting Act (15 U.S.C. 1681a(p)).

10 (9) PERSONAL INFORMATION.—

11 (A) DEFINITION.—The term “personal in-
12 formation” means any information or compila-
13 tion of information that includes—

14 (i) a non-truncated social security
15 number;

16 (ii) a financial account number or
17 credit or debit card number in combination
18 with any security code, access code, or
19 password that is required for an individual
20 to obtain credit, withdraw funds, or engage
21 in a financial transaction; or

22 (iii) an individual’s first and last
23 name or first initial and last name in com-
24 bination with—

1 (I) a driver's license number, a
2 passport number, or an alien registra-
3 tion number, or other similar number
4 issued on a government document
5 used to verify identity;

6 (II) unique biometric data such
7 as a finger print, voice print, retina or
8 iris image, or any other unique phys-
9 ical representation;

10 (III) a unique account identifier,
11 electronic identification number, user
12 name, or routing code in combination
13 with any associated security code, ac-
14 cess code, or password that is re-
15 quired for an individual to obtain
16 money, goods, services, or any other
17 thing of value; or

18 (IV) 2 of the following:

19 (aa) Home address or tele-
20 phone number.

21 (bb) Mother's maiden name,
22 if identified as such.

23 (cc) Month, day, and year of
24 birth.

1 (B) MODIFIED DEFINITION BY RULE-
2 MAKING.—If the Commission determines that
3 the definition under subparagraph (A) is not
4 reasonably sufficient to protect individuals from
5 identity theft, fraud, or other unlawful conduct,
6 the Commission by rule promulgated under sec-
7 tion 553 of title 5, United States Code, may
8 modify the definition of “personal information”
9 under subparagraph (A) to the extent the modi-
10 fication will not unreasonably impede interstate
11 commerce.

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

1 transmission, routing, intermediate and transient
2 storage, or connections.

3 **SEC. 7. EFFECT ON OTHER LAWS.**

4 (a) PREEMPTION OF STATE INFORMATION SECURITY
5 LAWS.—

6 (1) COVERED ENTITIES UNDER SECTION
7 5(a).—With respect to a covered entity subject to
8 the Act under section 5(a), this Act supersedes any
9 provision of a statute, regulation, or rule of a State
10 or political subdivision of a State that expressly—

11 (A) requires information security practices
12 and treatment of data containing personal in-
13 formation similar to any of those required
14 under section 2; or

15 (B) requires notification to individuals of a
16 breach of security as defined in section 6.

17 (2) COVERED ENTITIES UNDER SECTION
18 5(b).—With respect to a covered entity subject to
19 the Act under section 5(b), this Act supersedes any
20 provision of a statute, regulation, or rule of a State
21 or political subdivision of a State that expressly re-
22 quires notification to individuals of a breach of secu-
23 rity as defined in section 6.

24 (b) ADDITIONAL PREEMPTION.—

1 (1) IN GENERAL.—No person other than a per-
 2 son specified in section 5(d) may bring a civil action
 3 under the laws of any State if such action is pre-
 4 mised in whole or in part upon the defendant vio-
 5 lating any provision of this Act.

6 (2) PROTECTION OF CONSUMER PROTECTION
 7 LAWS.—Except as provided in subsection (a) of this
 8 section, this subsection shall not be construed to
 9 limit the enforcement of any State consumer protec-
 10 tion law by an attorney general of a State.

11 (c) PROTECTION OF CERTAIN STATE LAWS.—This
 12 Act shall not be construed to preempt the applicability
 13 of—

14 (1) State trespass, contract, or tort law; or

15 (2) any other State laws to the extent that
 16 those laws relate to acts of fraud.

17 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
 18 in this Act may be construed in any way to limit or affect
 19 the Commission's authority under any other provision of
 20 law.

21 **SEC. 8. EFFECTIVE DATE.**

22 This Act and the amendments made by this Act shall
 23 take effect 1 year after the date of enactment of this Act.

○