

115TH CONGRESS  
1ST SESSION

# S. 2179

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

NOVEMBER 30, 2017

Mr. NELSON (for himself, Mr. BLUMENTHAL, and Ms. BALDWIN) 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”.

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 or process such data for such  
8 covered entity, to establish and implement policies  
9 and procedures regarding information security prac-  
10 tices for the treatment and protection of personal in-  
11 formation 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, includ-  
12 ing regular monitoring for a breach of security  
13 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), that may include implementing any  
18 changes to information security practices and  
19 the architecture, installation, or implementation  
20 of network 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 **SEC. 3. NOTIFICATION OF BREACH OF SECURITY.**

4 (a) NATIONWIDE NOTIFICATION.—A covered entity  
5 that owns or possesses data in electronic form containing  
6 personal information, following the discovery of a breach  
7 of security of the system maintained by the covered entity  
8 that contains such data, shall notify—

9 (1) each individual who is a citizen or resident  
10 of the United States and whose personal information  
11 was or is reasonably believed to have been acquired  
12 or accessed from the covered entity as a result of the  
13 breach of security; and

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

16 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

17 (1) THIRD-PARTY ENTITIES.—In the event of a  
18 breach of security of a system maintained by a  
19 third-party entity that has been contracted to main-  
20 tain or process data in electronic form containing  
21 personal information on behalf of any other covered  
22 entity who owns or possesses such data, the third-  
23 party entity shall notify the covered entity of the  
24 breach of security. Upon receiving notification from

1 the third-party entity, such covered entity shall pro-  
2 vide the notification required under subsection (a).

3 (2) COORDINATION OF NOTIFICATION WITH  
4 CREDIT REPORTING AGENCIES.—If a covered entity  
5 is required to provide notification to more than  
6 5,000 individuals under subsection (a)(1), the cov-  
7 ered entity also shall notify each major credit report-  
8 ing agency of the timing and distribution of the no-  
9 tices, except when the only personal information that  
10 is the subject of the breach of security is the individ-  
11 ual’s first name or initial and last name, or address,  
12 or phone number, in combination with a credit or  
13 debit card number, and any required security code.  
14 Such notice shall be given to each credit reporting  
15 agency without unreasonable delay and, if it will not  
16 delay notice to the affected individuals, prior to the  
17 distribution of notices to the affected individuals.

18 (c) TIMELINESS OF NOTIFICATION.—Notification  
19 under subsection (a) shall be made—

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

22 (2) as promptly as possible if the covered entity  
23 providing notice can show that providing notice with-  
24 in the timeframe under paragraph (1) is not feasible  
25 due to circumstances necessary—

1 (A) to accurately identify affected con-  
2 sumers;

3 (B) to prevent further breach or unauthor-  
4 ized disclosures; or

5 (C) to reasonably restore the integrity of  
6 the data system.

7 (d) METHOD AND CONTENT OF NOTIFICATION.—

8 (1) DIRECT NOTIFICATION.—

9 (A) METHOD OF DIRECT NOTIFICATION.—

10 A covered entity shall be in compliance with the  
11 notification requirement under subsection (a)(1)

12 if—

13 (i) the covered entity provides con-  
14 spicuous and clearly identified notifica-  
15 tion—

16 (I) in writing; or

17 (II) by e-mail or other electronic  
18 means if—

19 (aa) the covered entity's pri-  
20 mary method of communication  
21 with the individual is by e-mail or  
22 such other electronic means; or

23 (bb) the individual has con-  
24 sented to receive notification by  
25 e-mail or such other electronic

1 means and such notification is  
2 provided in a manner that is con-  
3 sistent with the provisions per-  
4 mitting electronic transmission of  
5 notices under section 101 of the  
6 Electronic Signatures in Global  
7 and National Commerce Act (15  
8 U.S.C. 7001); and

9 (ii) the method of notification selected  
10 under clause (i) can reasonably be expected  
11 to reach the intended individual.

12 (B) CONTENT OF DIRECT NOTIFICA-  
13 TION.—Each method of direct notification  
14 under subparagraph (A) shall include—

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

17 (ii) a description of each type of per-  
18 sonal information that was or is reasonably  
19 believed to have been acquired or accessed  
20 as a result of the breach of security;

21 (iii) a telephone number that an indi-  
22 vidual can use at no cost to the individual  
23 to contact the covered entity to inquire  
24 about the breach of security or the infor-

1           mation the covered entity maintained or  
2           possessed about that individual;

3           (iv) notice that the individual may be  
4           entitled to consumer credit reports under  
5           subsection (e)(1);

6           (v) instructions how an individual can  
7           request consumer credit reports under sub-  
8           section (e)(1);

9           (vi) a telephone number, that an indi-  
10          vidual can use at no cost to the individual,  
11          and an address to contact each major cred-  
12          it reporting agency; and

13          (vii) a telephone number, that an indi-  
14          vidual can use at no cost to the individual,  
15          and an Internet Web site address to obtain  
16          information regarding identity theft from  
17          the Commission.

18          (2) SUBSTITUTE NOTIFICATION.—

19           (A) CIRCUMSTANCES GIVING RISE TO SUB-  
20          STITUTE NOTIFICATION.—A covered entity re-  
21          quired to provide notification under subsection  
22          (a)(1) may provide substitute notification in-  
23          stead of direct notification under paragraph  
24          (1)—

1 (i) if direct notification is not feasible  
2 due to a lack of sufficient contact informa-  
3 tion for the individual required to be noti-  
4 fied; or

5 (ii) if the covered entity owns or pos-  
6 sesses data in electronic form containing  
7 personal information of fewer than 10,000  
8 individuals and direct notification is not  
9 feasible due to excessive cost to the covered  
10 entity required to provide such notification  
11 relative to the resources of such covered  
12 entity, as determined in accordance with  
13 the regulations issued by the Commission  
14 under paragraph (3)(A).

15 (B) METHOD OF SUBSTITUTE NOTIFICA-  
16 TION.—Substitute notification under this para-  
17 graph shall include—

18 (i) conspicuous and clearly identified  
19 notification by e-mail to the extent the cov-  
20 ered entity has an e-mail address for an in-  
21 dividual who is entitled to notification  
22 under subsection (a)(1);

23 (ii) conspicuous and clearly identified  
24 notification on the Internet Web site of the

1 covered entity if the covered entity main-  
2 tains an Internet Web site; and

3 (iii) notification to print and to broad-  
4 cast media, including major media in met-  
5 ropolitan and rural areas where the indi-  
6 viduals whose personal information was ac-  
7 quired reside.

8 (C) CONTENT OF SUBSTITUTE NOTIFICA-  
9 TION.—Each method of substitute notification  
10 under this paragraph shall include—

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

13 (ii) a description of each type of per-  
14 sonal information that was or is reasonably  
15 believed to have been acquired or accessed  
16 as a result of the breach of security;

17 (iii) notice that an individual may be  
18 entitled to consumer credit reports under  
19 subsection (e)(1);

20 (iv) instructions how an individual can  
21 request consumer credit reports under sub-  
22 section (e)(1);

23 (v) a telephone number that an indi-  
24 vidual can use at no cost to the individual  
25 to contact the covered entity to inquire

1 about the breach of security or the infor-  
2 mation the covered entity maintained or  
3 possessed about that individual;

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 (3) REGULATIONS AND GUIDANCE.—

14 (A) REGULATIONS.—Not later than 1 year  
15 after the date of enactment of this Act, the  
16 Commission, by regulation under section 553 of  
17 title 5, United States Code, shall establish cri-  
18 teria for determining circumstances under  
19 which substitute notification may be provided  
20 under paragraph (2), including criteria for de-  
21 termining if direct notification under paragraph  
22 (1) is not feasible due to excessive costs to the  
23 covered entity required to provide such notifica-  
24 tion relative to the resources of such covered  
25 entity. The regulations may also identify other

1           circumstances where substitute notification  
2           would be appropriate, including circumstances  
3           under which the cost of providing direct notifi-  
4           cation exceeds the benefits to consumers.

5           (B) GUIDANCE.—In addition, the Commis-  
6           sion, in consultation with the Small Business  
7           Administration, shall provide and publish gen-  
8           eral guidance with respect to compliance with  
9           this subsection. The guidance shall include—

10                   (i) a description of written or e-mail  
11                   notification that complies with paragraph  
12                   (1); and

13                   (ii) guidance on the content of sub-  
14                   stitute notification under paragraph (2),  
15                   including the extent of notification to print  
16                   and broadcast media that complies with  
17                   paragraph (2)(B)(iii).

18           (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

19                   (1) IN GENERAL.—Not later than 60 days after  
20                   the date of request by an individual who received no-  
21                   tification under subsection (a)(1) and quarterly  
22                   thereafter for 2 years, a covered entity required to  
23                   provide notification under subsection (a)(1) shall  
24                   provide, or arrange for the provision of, to the indi-

1       vidual at no cost, consumer credit reports from at  
2       least 1 major credit reporting agency.

3           (2) LIMITATION.—This subsection shall not  
4       apply if the only personal information that is the  
5       subject of the breach of security is the individual’s  
6       first name or initial and last name, or address, or  
7       phone number, in combination with a credit or debit  
8       card number, and any required security code.

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

11           (A) determination of the circumstances  
12           under which a covered entity required to pro-  
13           vide notification under subsection (a)(1) must  
14           provide or arrange for the provision of free con-  
15           sumer credit reports; and

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

1 (f) DELAY OF NOTIFICATION AUTHORIZED FOR NA-  
2 TIONAL SECURITY AND LAW ENFORCEMENT PUR-  
3 POSES.—

4 (1) IN GENERAL.—If the United States Secret  
5 Service or the Federal Bureau of Investigation de-  
6 termines that notification under this section would  
7 impede a criminal investigation or a national secu-  
8 rity activity, notification shall be delayed upon writ-  
9 ten notice from the United States Secret Service or  
10 the Federal Bureau of Investigation to the covered  
11 entity that experienced the breach of security. Writ-  
12 ten notice from the United States Secret Service or  
13 the Federal Bureau of Investigation shall specify the  
14 period of delay requested for national security or law  
15 enforcement purposes.

16 (2) SUBSEQUENT DELAY OF NOTIFICATION.—

17 (A) IN GENERAL.—A covered entity shall  
18 provide notification under this section not later  
19 than 30 days after the day that the delay was  
20 invoked unless a Federal law enforcement or in-  
21 telligence agency provides subsequent written  
22 notice to the covered entity that further delay  
23 is necessary.

24 (B) WRITTEN JUSTIFICATION REQUIRE-  
25 MENTS.—

1 (i) UNITED STATES SECRET SERV-  
2 ICE.—If the United States Secret Service  
3 instructs a covered entity to delay notifica-  
4 tion under this section beyond the 30-day  
5 period under subparagraph (A) (referred  
6 to in this clause as “subsequent delay”),  
7 the United States Secret Service shall sub-  
8 mit written justification for the subsequent  
9 delay to the Secretary of Homeland Secu-  
10 rity before the subsequent delay begins.

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

21 (3) LAW ENFORCEMENT IMMUNITY.—No cause  
22 of action shall lie in any court against any Federal  
23 agency for acts relating to the delay of notification  
24 for national security or law enforcement purposes  
25 under this Act.

1 (g) GENERAL EXEMPTION.—

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

7 (2) PRESUMPTION.—

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

12 (i) the data is rendered unusable,  
13 unreadable, or indecipherable through a se-  
14 curity technology or methodology; and

15 (ii) the security technology or method-  
16 ology under clause (i) is generally accepted  
17 by experts in the information security field.

18 (B) REBUTTAL.—The presumption under  
19 subparagraph (A) may be rebutted by facts  
20 demonstrating that the security technology or  
21 methodology in a specific case has been or is  
22 reasonably likely to be compromised.

23 (3) TECHNOLOGIES OR METHODOLOGIES.—Not  
24 later than 1 year after the date of enactment of this  
25 Act, and biennially thereafter, the Commission, after

1 consultation with the National Institute of Stand-  
2 ards and Technology, shall issue rules (pursuant to  
3 section 553 of title 5, United States Code) or guid-  
4 ance to identify each security technology and meth-  
5 odology under paragraph (2). In identifying each  
6 such security technology and methodology, the Com-  
7 mission and the National Institute of Standards and  
8 Technology shall—

9 (A) consult with relevant industries, con-  
10 sumer organizations, data security and identity  
11 theft prevention experts, and established stand-  
12 ards setting bodies; and

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

17 (4) COMMISSION GUIDANCE.—Not later than 1  
18 year after the date of enactment of this Act, the  
19 Commission, after consultation with the National In-  
20 stitute of Standards and Technology, shall issue  
21 guidance regarding the application of the exemption  
22 under paragraph (1).

23 (h) EXEMPTIONS FOR NATIONAL SECURITY AND  
24 LAW ENFORCEMENT PURPOSES.—

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

3           (A) a determination is made—

4               (i) by the United States Secret Serv-  
5       ice or the Federal Bureau of Investigation  
6       that notification of the breach of security  
7       could be reasonably expected to reveal sen-  
8       sitive sources and methods or similarly im-  
9       pede the ability of the Government to con-  
10      duct law enforcement or intelligence inves-  
11      tigations; or

12              (ii) by the Federal Bureau of Inves-  
13      tigation that notification of the breach of  
14      security could be reasonably expected to  
15      cause damage to the national security; and

16           (B) the United States Secret Service or the  
17      Federal Bureau of Investigation, as the case  
18      may be, provides written notice of its deter-  
19      mination under subparagraph (A) to the cov-  
20      ered entity.

21           (2) UNITED STATES SECRET SERVICE.—If the  
22      United States Secret Service invokes an exemption  
23      under paragraph (1), the United States Secret Serv-  
24      ice shall submit written justification for invoking the

1 exemption to the Secretary of Homeland Security  
2 before the exemption is invoked.

3 (3) FEDERAL BUREAU OF INVESTIGATION.—If  
4 the Federal Bureau of Investigation invokes an ex-  
5 emption under paragraph (1), the Federal Bureau of  
6 Investigation shall submit written justification for  
7 invoking the exemption to the Attorney General be-  
8 fore the exemption is invoked.

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

13 (5) REPORTS.—Not later than 18 months after  
14 the date of enactment of this Act, and upon request  
15 by Congress thereafter, the United States Secret  
16 Service and Federal Bureau of Investigation shall  
17 submit to Congress a report on the number and na-  
18 ture of breaches of security subject to the exemp-  
19 tions for national security and law enforcement pur-  
20 poses under this subsection.

21 (i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

22 (1) IN GENERAL.—A covered entity shall be ex-  
23 empt from the requirements under this section if the  
24 covered entity utilizes or participates in a security  
25 program that—

1 (A) effectively blocks the use of the per-  
2 sonal information to initiate an unauthorized fi-  
3 nancial transaction before it is charged to the  
4 account of the individual; and

5 (B) provides notice to each affected indi-  
6 vidual after a breach of security that resulted in  
7 attempted fraud or an attempted unauthorized  
8 transaction.

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

11 (A) the breach of security includes per-  
12 sonal information, other than a credit card  
13 number or credit card security code, of any  
14 type; or

15 (B) the breach of security includes both  
16 the individual's credit card number and the in-  
17 dividual's first and last name.

18 (j) FINANCIAL INSTITUTIONS REGULATED BY FED-  
19 ERAL FUNCTIONAL REGULATORS.—

20 (1) IN GENERAL.—A covered financial institu-  
21 tion shall be deemed in compliance with this section  
22 if—

23 (A) the Federal functional regulator with  
24 jurisdiction over the covered financial institu-  
25 tion has issued a standard by regulation or

1 guideline under title V of the Gramm-Leach-  
2 Bliley Act (15 U.S.C. 6801 et seq.) that—

3 (i) requires financial institutions with-  
4 in its jurisdiction to provide notification to  
5 individuals following a breach of security;  
6 and

7 (ii) provides protections substantially  
8 similar to, or greater than, those required  
9 under this Act; and

10 (B) the covered financial institution is in  
11 compliance with the standard under subpara-  
12 graph (A).

13 (2) DEFINITIONS.—In this subsection—

14 (A) the term “covered financial institu-  
15 tion” means a financial institution that is sub-  
16 ject to—

17 (i) the data security requirements of  
18 the Gramm-Leach-Bliley Act (15 U.S.C.  
19 6801 et seq.);

20 (ii) any implementing standard issued  
21 by regulation or guideline issued under  
22 that Act; and

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

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

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

8 (k) EXEMPTION; HEALTH PRIVACY.—

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

20 (2) ENTITY SUBJECT TO HITECH ACT.—To the  
21 extent that a covered entity under this Act acts as  
22 a vendor of personal health records, a third party  
23 service provider, or other entity subject to section  
24 13407 of the Health Information Technology for Ec-  
25 onomical and Clinical Health Act (42 U.S.C.

1 17937), has the obligation to provide notification to  
2 individuals following a breach of security under that  
3 Act or its implementing regulations, and is in com-  
4 pliance with that obligation, the covered entity shall  
5 be deemed in compliance with this section.

6 (3) LIMITATION OF STATUTORY CONSTRUC-  
7 TION.—Nothing in this Act may be construed in any  
8 way to give effect to the sunset provision under sec-  
9 tion 13407(g)(2) of the Health Information Tech-  
10 nology for Economic and Clinical Health Act (42  
11 U.S.C. 17937(g)(2)) or to otherwise limit or affect  
12 the applicability, under section 13407 of that Act, of  
13 the requirement to provide notification to individuals  
14 following a breach of security for vendors of personal  
15 health records and each entity described in clause  
16 (ii), (iii), or (iv) of section 13424(b)(1)(A) of that  
17 Act (42 U.S.C. 17953(b)(1)(A)).

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

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

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

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

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

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

20 (1) the number of individuals whose personal  
21 information was, or is reasonably believed to have  
22 been, acquired or assessed as a result of the breach  
23 of security exceeds 10,000;

24 (2) the breach of security involves a database,  
25 networked or integrated databases, or other data

1 system containing the personal information of more  
2 than 1,000,000 individuals;

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

5 (4) the breach of security involves primarily  
6 personal information of individuals known to the  
7 covered entity to be employees or contractors of the  
8 Federal Government involved in national security or  
9 law enforcement.

10 (c) CONTENT OF NOTICES.—

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

13 (A) the date, estimated date, or estimated  
14 date range of the breach of security;

15 (B) a description of the nature of the  
16 breach of security;

17 (C) a description of each type of personal  
18 information that was or is reasonably believed  
19 to have been acquired or accessed as a result of  
20 the breach of security; and

21 (D) a statement of each paragraph under  
22 subsection (b) that applies to the breach of se-  
23 curity.

24 (2) CONSTRUCTION.—Nothing in this section  
25 shall be construed to require a covered entity to re-

1       veal specific or identifying information about an in-  
2       dividual as part of the notice under paragraph (1).

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

6               (1) the United States Secret Service;

7               (2) the Federal Bureau of Investigation;

8               (3) the Federal Trade Commission;

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

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

13              (6) as appropriate, other Federal agencies for  
14       law enforcement, national security, or data security  
15       purposes.

16       (e) TIMING OF NOTICES.—Notice under this section  
17       shall be delivered as follows:

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

20                      (A) not less than 3 business days before  
21       notification to an individual under section 3;  
22       and

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

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

6 **SEC. 5. APPLICATION AND ENFORCEMENT.**

7           (a) GENERAL APPLICATION.—The requirements of  
8           sections 2 and 3 shall apply to—

9           (1) those persons, partnerships, or corporations  
10          over which the Commission has authority under sec-  
11          tion 5(a)(2) of the Federal Trade Commission Act  
12          (15 U.S.C. 45(a)(2)); and

13          (2) notwithstanding sections 4 and 5(a)(2) of  
14          the Federal Trade Commission Act (15 U.S.C. 44  
15          and 45(a)(2)), any nonprofit organization, including  
16          any organization described in section 501(c) of the  
17          Internal Revenue Code of 1986 that is exempt from  
18          taxation under section 501(a) of the Internal Rev-  
19          enue Code of 1986.

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

21          (1) IN GENERAL.—Notwithstanding sections 4  
22          and 5(a)(2) of the Federal Trade Commission Act  
23          (15 U.S.C. 44 and 45(a)(2)), the requirements of  
24          section 3 shall apply to any other covered entity not  
25          included under subsection (a) that enters into an

1 agreement with the Commission under which that  
2 covered entity would be subject to section 3 with re-  
3 spect to any acts or omissions that occur while the  
4 agreement is in effect and that may constitute a vio-  
5 lation of section 3, if—

6 (A) not less than 30 days prior to entering  
7 into the agreement with the covered entity, the  
8 Commission publishes notice in the Federal  
9 Register of the Commission’s intent to enter  
10 into the agreement; and

11 (B) not later than 14 business days after  
12 entering into the agreement with the covered  
13 entity, the Commission publishes in the Federal  
14 Register—

15 (i) notice of the agreement;

16 (ii) the identity of each person covered  
17 by the agreement; and

18 (iii) the effective date of the agree-  
19 ment.

20 (2) CONSTRUCTION.—

21 (A) OTHER FEDERAL LAW.—An agreement  
22 under paragraph (1) shall not effect a covered  
23 entity’s obligation to provide notice of a breach  
24 of security or similar event under any other  
25 Federal law.

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

6 (c) ENFORCEMENT BY THE FEDERAL TRADE COM-  
7 MISSION.—

8 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
9 TICES.—A violation of section 2 or 3 of this Act  
10 shall be treated as an unfair and deceptive act or  
11 practice in violation of a regulation under section  
12 18(a)(1)(B) of the Federal Trade Commission Act  
13 (15 U.S.C. 57a(a)(1)(B)) regarding unfair or decep-  
14 tive acts or practices.

15 (2) VIOLATION OF TITLE V OF THE GRAMM-  
16 LEACH-BLILEY ACT.—A violation of a regulation  
17 prescribed by the Commission under title V of the  
18 Gramm-Leach-Bliley Act for the financial institu-  
19 tions subject to the Commission's jurisdiction (15  
20 U.S.C. 6801 et seq.) shall be treated as an unfair  
21 and deceptive act or practice in violation of a regula-  
22 tion under section 18(a)(1)(B) of the Federal Trade  
23 Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding  
24 unfair or deceptive acts or practices.

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

12          (4) LIMITATION.—In promulgating rules under  
13          this Act, the Commission shall not require the de-  
14          ployment or use of any specific products or tech-  
15          nologies, including any specific computer software or  
16          hardware.

17          (d) ENFORCEMENT BY STATE ATTORNEYS GEN-  
18          ERAL.—

19               (1) CIVIL ACTION.—In any case in which the  
20               attorney general of a State, or an official or agency  
21               of a State, has reason to believe that an interest of  
22               the residents of that State has been or is threatened  
23               or adversely affected by any covered entity who vio-  
24               lates section 2 or section 3 of this Act, the attorney  
25               general, official, or agency of the State, as parens

1 patriae, may bring a civil action on behalf of the  
2 residents of the State in a district court of the  
3 United States of appropriate jurisdiction—

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

6 (B) to compel compliance with such sec-  
7 tion; or

8 (C) to obtain civil penalties in the amount  
9 determined under paragraph (2).

10 (2) CIVIL PENALTIES.—

11 (A) CALCULATION.—

12 (i) TREATMENT OF VIOLATIONS OF  
13 SECTION 2.—For purposes of paragraph  
14 (1)(C) with regard to a violation of section  
15 2, the amount determined under this para-  
16 graph is the amount calculated by multi-  
17 plying the number of days that a covered  
18 entity is not in compliance with such sec-  
19 tion by an amount not greater than  
20 \$11,000.

21 (ii) TREATMENT OF VIOLATIONS OF  
22 SECTION 3.—For purposes of paragraph  
23 (1)(C) with regard to a violation of section  
24 3, the amount determined under this para-  
25 graph is the amount calculated by multi-

1           plying the number of violations of such  
2           section by an amount not greater than  
3           \$11,000. Each failure to send notification  
4           as required under section 3 to a resident of  
5           the State shall be treated as a separate  
6           violation.

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

18          (C) MAXIMUM TOTAL LIABILITY.—Not-  
19          withstanding the number of actions which may  
20          be brought against a covered entity under this  
21          subsection, the maximum civil penalty for which  
22          any covered entity may be liable under this sub-  
23          section shall not exceed—

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

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

4 (3) INTERVENTION BY THE FTC.—

5 (A) NOTICE AND INTERVENTION.—The  
6 State shall provide prior written notice of any  
7 action under paragraph (1) to the Commission  
8 and provide the Commission with a copy of its  
9 complaint, except in any case in which such  
10 prior notice is not feasible, in which case the  
11 State shall serve such notice immediately upon  
12 commencing such action. The Commission shall  
13 have the right—

14 (i) to intervene in the action;

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

17 (iii) to file petitions for appeal.

18 (B) LIMITATION ON STATE ACTION WHILE  
19 FEDERAL ACTION IS PENDING.—If the Commis-  
20 sion has instituted a civil action for violation of  
21 this Act, no State attorney general, or official  
22 or agency of a State, may bring an action under  
23 this subsection during the pendency of that ac-  
24 tion against any defendant named in the com-

1           plaint of the Commission for any violation of  
2           this Act alleged in the complaint.

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

8                   (A) to conduct investigations;

9                   (B) to administer oaths or affirmations; or

10                  (C) to compel the attendance of witnesses  
11           or the production of documentary and other evi-  
12           dence.

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

15           (1) IN GENERAL.—The Attorney General may  
16           bring a civil action in the appropriate United States  
17           district court against any covered entity that en-  
18           gages in conduct constituting a violation of section  
19           4.

20           (2) PENALTIES.—

21                   (A) IN GENERAL.—Upon proof of such  
22           conduct by a preponderance of the evidence, a  
23           covered entity shall be subject to a civil penalty  
24           of not more than \$1,000 per individual whose  
25           personal information was or is reasonably be-

1           lied to have been accessed or acquired as a  
2           result of the breach of security that is the basis  
3           of the violation, up to a maximum of \$100,000  
4           per day while such violation persists.

5           (B) LIMITATIONS.—The total amount of  
6           the civil penalty assessed under this subsection  
7           against a covered entity for acts or omissions  
8           relating to a single breach of security shall not  
9           exceed \$1,000,000, unless the conduct consti-  
10          tuting a violation of section 4 was willful or in-  
11          tentional, in which case an additional civil pen-  
12          alty of up to \$1,000,000 may be imposed.

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

23          (3) INJUNCTIVE ACTIONS.—If it appears that a  
24          covered entity has engaged, or is engaged, in any act  
25          or practice that constitutes a violation of section 4,

1 the Attorney General may petition an appropriate  
2 United States district court for an order enjoining  
3 such practice or enforcing compliance with section 4.

4 (4) ISSUANCE OF ORDER.—A court may issue  
5 such an order under paragraph (3) if it finds that  
6 the conduct in question constitutes a violation of  
7 section 4.

8 (f) CONCEALMENT OF BREACHES OF SECURITY.—

9 (1) IN GENERAL.—Chapter 47 of title 18,  
10 United States Code, is amended by adding at the  
11 end the following:

12 **“§ 1041. Concealment of breaches of security involv-**  
13 **ing personal information**

14 “(a) IN GENERAL.—Any person who, having knowl-  
15 edge of a breach of security and of the fact that notifica-  
16 tion of the breach of security is required under the Data  
17 Security and Breach Notification Act, intentionally and  
18 willfully conceals the fact of the breach of security, shall,  
19 in the event that the breach of security results in economic  
20 harm to any individual in the amount of \$1,000 or more,  
21 be fined under this title, imprisoned for not more than  
22 5 years, or both.

23 “(b) PERSON DEFINED.—For purposes of subsection  
24 (a), the term ‘person’ has the same meaning as in section  
25 1030(e)(12) of this title.

1 “(c) ENFORCEMENT AUTHORITY.—

2 “(1) IN GENERAL.—The United States Secret  
3 Service and the Federal Bureau of Investigation  
4 shall have the authority to investigate offenses under  
5 this section.

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

9 (2) CONFORMING AND TECHNICAL AMEND-  
10 MENTS.—The table of sections for chapter 47 of title  
11 18, United States Code, is amended by adding at  
12 the end the following:

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

13 **SEC. 6. DEFINITIONS.**

14 In this Act:

15 (1) BREACH OF SECURITY.—

16 (A) IN GENERAL.—The term “breach of  
17 security” means compromise of the security,  
18 confidentiality, or integrity of, or loss of, data  
19 in electronic form that results in, or there is a  
20 reasonable basis to conclude has resulted in,  
21 unauthorized access to or acquisition of per-  
22 sonal information from a covered entity.

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

1 (i) a good faith acquisition of personal  
2 information by a covered entity, or an em-  
3 ployee or agent of a covered entity, if the  
4 personal information is not subject to fur-  
5 ther use or unauthorized disclosure;

6 (ii) any lawfully authorized investiga-  
7 tive, protective, or intelligence activity of a  
8 law enforcement or an intelligence agency  
9 of the United States, a State, or a political  
10 subdivision of a State; or

11 (iii) the release of a public record not  
12 otherwise subject to confidentiality or non-  
13 disclosure requirements.

14 (2) COMMISSION.—The term “Commission”  
15 means the Federal Trade Commission.

16 (3) COVERED ENTITY.—The term “covered en-  
17 tity” means a sole proprietorship, partnership, cor-  
18 poration, trust, estate, cooperative, association, or  
19 other commercial entity, and any charitable, edu-  
20 cational, or nonprofit organization, that acquires,  
21 maintains, or utilizes personal information.

22 (4) DATA IN ELECTRONIC FORM.—The term  
23 “data in electronic form” means any data stored  
24 electronically or digitally on any computer system or

1 other database, including recordable tapes and other  
2 mass storage devices.

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

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

17 (7) IDENTITY THEFT.—The term “identity  
18 theft” means the unauthorized use of another per-  
19 son’s personal information for the purpose of engag-  
20 ing in commercial transactions under the identity of  
21 such other person, including any contact that vio-  
22 lates section 1028A of title 18, United States Code.

23 (8) MAJOR CREDIT REPORTING AGENCY.—The  
24 term “major credit reporting agency” means a con-  
25 sumer reporting agency that compiles and maintains

1 files on consumers on a nationwide basis within the  
2 meaning of section 603(p) of the Fair Credit Re-  
3 porting Act (15 U.S.C. 1681a(p)).

4 (9) PERSONAL INFORMATION.—

5 (A) DEFINITION.—The term “personal in-  
6 formation” means any information or compila-  
7 tion of information that includes—

8 (i) a non-truncated social security  
9 number;

10 (ii) a financial account number or  
11 credit or debit card number in combination  
12 with any security code, access code, or  
13 password that is required for an individual  
14 to obtain credit, withdraw funds, or engage  
15 in a financial transaction; or

16 (iii) an individual’s first and last  
17 name or first initial and last name in com-  
18 bination with—

19 (I) a driver’s license number, a  
20 passport number, or an alien registra-  
21 tion number, or other similar number  
22 issued on a government document  
23 used to verify identity;

24 (II) unique biometric data such  
25 as a finger print, voice print, retina or

1 iris image, or any other unique phys-  
2 ical representation;

3 (III) a unique account identifier,  
4 electronic identification number, user  
5 name, or routing code in combination  
6 with any associated security code, ac-  
7 cess code, or password that is re-  
8 quired for an individual to obtain  
9 money, goods, services, or any other  
10 thing of value; or

11 (IV) two of the following:

12 (aa) Home address or tele-  
13 phone number.

14 (bb) Mother's maiden name,  
15 if identified as such.

16 (cc) Month, day, and year of  
17 birth.

18 (B) MODIFIED DEFINITION BY RULE-  
19 MAKING.—If the Commission determines that  
20 the definition under subparagraph (A) is not  
21 reasonably sufficient to protect individuals from  
22 identity theft, fraud, or other unlawful conduct,  
23 the Commission by rule promulgated under sec-  
24 tion 553 of title 5, United States Code, may  
25 modify the definition of “personal information”

1           under subparagraph (A) to the extent the modi-  
2           fication will not unreasonably impede interstate  
3           commerce.

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

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

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

12                   (A) requires information security practices  
13 and treatment of data containing personal in-  
14 formation, as defined in section 6, similar to  
15 any of those required under section 2; or

16                   (B) requires notification to individuals of a  
17 breach of security of personal information as  
18 defined in section 6.

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

1 (b) ADDITIONAL PREEMPTION.—

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

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

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

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

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

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

22 **SEC. 8. EFFECTIVE DATE.**

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

○