

109<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# S. 3713

To protect privacy rights associated with electronic and commercial transactions.

---

IN THE SENATE OF THE UNITED STATES

JULY 21, 2006

Mrs. CLINTON introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

## A BILL

To protect privacy rights associated with electronic and commercial transactions.

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 “Privacy Rights and  
5 Oversight for Electronic and Commercial Transactions  
6 Act of 2006” or the “PROTECT Act”.

7 **SEC. 2. PRIVATE RIGHT OF ACTION.**

8 (a) COMPROMISED DATA.—

9 (1) IN GENERAL.—It shall be unlawful for any  
10 for profit entity that stores, processes, or otherwise

1 handles the personal data of an individual to com-  
2 promise the personal, nonpublic information of that  
3 individual through theft, loss, data breach or other  
4 malfeasance.

5 (2) LIABILITY.—An entity that violates this  
6 subsection shall—

7 (A) be liable to the injured individual for  
8 \$1,000; and

9 (B) have a net liability arising from any  
10 individual data breach, theft, or loss event of  
11 not to exceed 1 percent of annual revenues for  
12 the entity.

13 (b) IDENTITY THEFT.—

14 (1) IN GENERAL.—It shall be unlawful for any  
15 for profit entity to issue credit or an account for  
16 services to an unauthorized individual or make an  
17 inaccurate change to a credit report as a result of  
18 identity theft.

19 (2) LIABILITY.—An entity that violates this  
20 subsection shall—

21 (A) be liable for \$5,000 to the injured indi-  
22 vidual for each instance of unauthorized use;  
23 and

24 (B) have a net liability for identity thefts  
25 resulting from a specific data breach event of

1           not to exceed 5 percent of annual revenues for  
2           the entity.

3           (c) **SMALL BUSINESS EXCEPTION.**—A small business  
4 as defined by the standards of the Small Business Admin-  
5 istration shall be exempt from this section although noth-  
6 ing in this section shall prohibit private rights of action  
7 against any entity for data loss or identity theft.

8           (d) **COLLECTIVE ACTION.**—A collective action may be  
9 brought under this section pursuant to the procedures pro-  
10 vided in section 16(b) of the Fair Labor Standards Act  
11 of 1938.

12 **SEC. 3. OPT-IN FOR CERTAIN TYPES OF INFORMATION.**

13           Section 502 of the Gramm-Leach-Bliley Act (15  
14 U.S.C. 6802) is amended by adding at the end the fol-  
15 lowing:

16           “(f) **OPT IN REQUIREMENT FOR CERTAIN INFORMA-**  
17 **TION.**—

18           “(1) **LIMITATION.**—Notwithstanding subsection  
19 (b), a financial institution may not disclose usage  
20 data relating to a consumer to a nonaffiliated third  
21 part, unless—

22           “(A) such financial institution clearly and  
23 conspicuously requests authority from the con-  
24 sumer, in writing or in electronic form or other  
25 form permitted by the regulations prescribed

1 under section 504 to disclose such information  
2 to such third party; and

3 “(B) the consumer affirmatively authorizes  
4 such disclosure, in writing.

5 “(2) DEFINITION.—As used in this subsection,  
6 the term ‘usage data’, means any information relat-  
7 ing to purchase history records or any listing of  
8 items and services purchased by the consumer to  
9 whom the information relates.”.

10 **SEC. 4. CHIEF PRIVACY OFFICER WITHIN THE OFFICE OF**  
11 **MANAGEMENT AND BUDGET.**

12 (a) DEFINITIONS.—In this section—

13 (1) the term “agency” has the meaning given  
14 under section 551(1) of title 5, United States Code;  
15 and

16 (2) the term “system of records” has the mean-  
17 ing given under section 552a(5) of title 5, United  
18 States Code.

19 (b) DESIGNATION OF CHIEF PRIVACY OFFICER.—

20 The President shall designate a senior officer within the  
21 Office of Management and Budget as the Chief Privacy  
22 Officer, who shall have primary responsibility for privacy  
23 policy throughout all agencies.

24 (c) RESPONSIBILITIES.—The Chief Privacy Officer  
25 shall—

1           (1) ensure that the technologies procured and  
2 use of technologies by agencies sustain, and do not  
3 erode, privacy protections relating to the use, collec-  
4 tion, and disclosure of personally identifiable infor-  
5 mation;

6           (2) ensure that agency officers have the author-  
7 ity to enforce rules and regulations relating to the  
8 collection, processing, and storage of personally iden-  
9 tifiable information within, between, and among  
10 agencies;

11           (3) ensure that personally identifiable informa-  
12 tion contained in each system of records is handled  
13 in full compliance with fair information practices re-  
14 quired under section 552a of title 5, United States  
15 Code, (commonly referred to as the “Privacy Act”);

16           (4) evaluate legislative and regulatory proposals  
17 involving collection, use, and disclosure of personally  
18 identifiable information by agencies;

19           (5) exercise responsibility under the direction of  
20 the Director of the Office of Management and Budg-  
21 et with respect to privacy impact assessment rules,  
22 regulations, and oversight under section 208 of the  
23 E-Government Act of 2002 (44 U.S.C. 3501 note);  
24 and

1           (6) submit an annual report to the Congress  
2           containing an analysis of each agency of Federal ac-  
3           tivities that affect privacy, including complaints of  
4           privacy violations, implementation of section 552a of  
5           title 5, United States Code, (commonly referred to  
6           as the “Privacy Act”), internal controls, and other  
7           matters.

8           (d) AGENCY REPORTS TO THE CHIEF PRIVACY OFFI-  
9           CER .—The head of each agency and the Chief Privacy  
10          Officer of each agency established under section 522 of  
11          the Consolidated Appropriations Act, 2005 (relating to  
12          Chief Privacy Officers) (5 U.S.C. 552a note; Public Law  
13          108–447; 118 Stat. 3268) shall—

14                 (1) provide to the Chief Privacy Officer estab-  
15                 lished under this section such information as the  
16                 Chief Privacy Officer considers necessary for the  
17                 completion of the annual reports under subsection  
18                 (c)(6); and

19                 (2) submit annual reports to the Chief Privacy  
20                 Officer established under this section that include—

21                         (A) an assessment of agency policies and  
22                         protocols relating to data security; and

23                         (B) a description of the actions that are  
24                         being taken to ensure protection against—

- 1 (i) threats and hazards to data secu-  
2 rity; and  
3 (ii) unauthorized access or use of  
4 data.

5 (e) NOTIFICATIONS ON BREACHES OF PERSONALLY  
6 IDENTIFIABLE INFORMATION .—

7 (1) NOTIFICATION TO INDIVIDUAL.—

8 (A) IN GENERAL.—If a system of records  
9 maintained by an agency is breached and data  
10 with personally identifiable information is  
11 accessed or disclosed without authorization as a  
12 result of that breach, the agency shall provide  
13 timely notification to each individual affected by  
14 that breach.

15 (B) EXCEPTION.—An agency may delay  
16 notification under subparagraph (A) on the  
17 basis of national security.

18 (2) NOTIFICATION TO MAJOR CREDIT REPORT-  
19 ING SERVICES.—

20 (A) IN GENERAL.—If an individual re-  
21 ceives notification of a breach under paragraph  
22 (1), the individual may request the agency to  
23 provide notification of the breach to all major  
24 credit reporting services.

1 (B) NOTIFICATION.—Upon the receipt of a  
2 request under subparagraph (A), the agency  
3 shall provide notification of the breach to all  
4 major credit reporting services.

5 (3) NO COST TO INDIVIDUAL.—Notification  
6 under paragraphs (1) or (2) shall be at no cost to  
7 any individual.

8 **SEC. 5. RULEMAKING RELATING TO DISCLOSURES.**

9 Section 504 of the Gramm-Leach-Bliley Act (15  
10 U.S.C. 6804) is amended by adding at the end the fol-  
11 lowing:

12 “(c) DISCLOSURE REGULATIONS.—The Federal  
13 Trade Commission and each of the Federal functional reg-  
14 ulators shall, promptly upon the date of enactment of this  
15 subsection, issue final rules applicable to financial institu-  
16 tions subject to their authority to require standard, clear,  
17 easy to understand disclosures of what specific informa-  
18 tion could be shared under this title, the types of third  
19 parties with which such information could be shared, and  
20 when consumers are given opt out opportunities.”.

21 **SEC. 6. ANNUAL DISCLOSURES TO CONSUMERS.**

22 Section 503 of the Gramm-Leach-Bliley Act (15  
23 U.S.C. 6803) is amended by adding at the end the fol-  
24 lowing:



1       “(c) ANNUAL DISCLOSURES.—In addition to the dis-  
2 closures required under subsection (a), upon written re-  
3 quest of a consumer, each financial institution shall pro-  
4 vide free of charge to the consumer up to once each year,  
5 a copy of all information maintained by the financial insti-  
6 tution relating to the consumer, including any consoli-  
7 dated profile.”.

8 **SEC. 7. AUTOMATIC FREE ANNUAL CREDIT REPORTS.**

9       Section 612(a) of the Fair Credit Reporting Act (15  
10 U.S.C. 1681j(a)) is amended by striking “period upon re-  
11 quest of the consumer and” and inserting “period,”.

12 **SEC. 8. NOTICE OF SECURITY BREACHES.**

13       (a) NOTICE TO PERSONS AFFECTED.—Each Federal  
14 agency, and each business entity, whether a nonprofit or  
15 for profit concern, shall promptly notify each person who  
16 may be a victim of identity theft due to a security breach  
17 involving the agency or entity, including the theft or po-  
18 tential theft of or other inappropriate access to identifying  
19 information relating to that person that is collected or  
20 maintained by the agency or business entity.

21       (b) NOTICE TO CONSUMER REPORTING AGENCIES.—  
22 Each Federal agency and business entity described in sub-  
23 section (a) shall promptly notify each consumer reporting  
24 agency described in section 603(p) of the Fair Credit Re-  
25 porting Act (15 U.S.C. 1681a(p)) of a security breach de-

1 scribed in subsection (a), including the names of all per-  
2 sons affected or potentially affected thereby.

3 (c) REGULATIONS.—The Federal Trade Commission  
4 shall issue regulations to carry out the provisions of this  
5 section.

6 **SEC. 9. SECURITY FREEZE ON CREDIT REPORTS.**

7 Section 605B of the Fair Credit Reporting Act (15  
8 U.S.C. 1681C–2) is amended to read as follows:

9 **“SEC. 605B. SECURITY FREEZE ON RELEASE OF INFORMA-**  
10 **TION.**

11 “(a) IN GENERAL.—

12 “(1) CONSUMER PLACEMENT OF A SECURITY  
13 FREEZE ON INDIVIDUAL CREDIT FILES.—A con-  
14 sumer may place a security freeze on his or her file  
15 by making a request to a consumer reporting agency  
16 in writing, by telephone, or through a secure elec-  
17 tronic connection made available by the consumer  
18 reporting agency.

19 “(2) CONSUMER DISCLOSURE.—If a consumer  
20 requests a security freeze under this section, the  
21 consumer reporting agency shall disclose to the con-  
22 sumer the process of placing and removing the secu-  
23 rity freeze and explain to the consumer the potential  
24 consequences of the security freeze. A consumer re-  
25 porting agency may not imply or inform a consumer

1 that the placement or presence of a security freeze  
2 on the file of the consumer may negatively affect the  
3 consumer's credit score.

4 “(b) EFFECT OF SECURITY FREEZE.—

5 “(1) RELEASE OF INFORMATION BLOCKED.—If  
6 a security freeze is in place on the file of a con-  
7 sumer, a consumer reporting agency may not release  
8 information relating to that file for consumer credit  
9 purposes to a third party without prior express au-  
10 thorization from the consumer.

11 “(2) INFORMATION PROVIDED TO THIRD PAR-  
12 TIES.—Paragraph (1) does not prevent a consumer  
13 reporting agency from advising a third party that a  
14 security freeze is in effect with respect to the file of  
15 a consumer. If a third party requests access to the  
16 file of a consumer on which a security freeze is in  
17 place in connection with an application for credit,  
18 the third party may treat the application as incom-  
19 plete.

20 “(3) CONSUMER CREDIT SCORE NOT AF-  
21 FECTED.—The placement of a security freeze on a  
22 consumer file may not be taken into account for any  
23 purpose in determining the credit score of the con-  
24 sumer to whom the account relates.

25 “(c) REMOVAL; TEMPORARY SUSPENSION.—

1           “(1) IN GENERAL.—Except as provided in para-  
2           graph (4), a security freeze under this section shall  
3           remain in place until the consumer requests that the  
4           security freeze be removed. A consumer may remove  
5           a security freeze on his or her credit file by making  
6           a request to a consumer reporting agency in writing,  
7           by telephone, or through a secure electronic connec-  
8           tion made available by the consumer reporting agen-  
9           cy.

10           “(2) CONDITIONS.—A consumer reporting  
11           agency may remove a security freeze placed on the  
12           file of a consumer only—

13                   “(A) upon request of the consumer, pursu-  
14                   ant to paragraph (1); or

15                   “(B) if the agency determines that the  
16                   credit file of the consumer was frozen due to a  
17                   material misrepresentation of fact by the con-  
18                   sumer.

19           “(3) NOTIFICATION TO CONSUMER.—If a con-  
20           sumer reporting agency intends to remove a security  
21           freeze on the file of a consumer pursuant to para-  
22           graph (2)(B), the consumer reporting agency shall  
23           notify the consumer in writing prior to removing the  
24           security freeze.

1           “(4) TEMPORARY SUSPENSION.—A consumer  
2           may have a security freeze on his or her credit file  
3           temporarily suspended by making a request to a  
4           consumer reporting agency in writing or by tele-  
5           phone and specifying beginning and ending dates for  
6           the period during which the security freeze is not to  
7           apply to that file.

8           “(d) RESPONSE TIMES; NOTIFICATION OF OTHER  
9 ENTITIES.—

10           “(1) IN GENERAL.—A consumer reporting  
11           agency shall—

12                   “(A) place a security freeze on the file of  
13                   a consumer under subsection (a) not later than  
14                   5 business days after receiving a request from  
15                   the consumer under subsection (a)(1); and

16                   “(B) remove or temporarily suspend a se-  
17                   curity freeze not later than 3 business days  
18                   after receiving a request for removal or tem-  
19                   porary suspension from the consumer under  
20                   subsection (c).

21           “(2) NOTIFICATION TO OTHER AGENCIES.—If  
22           the consumer so requests in writing or by telephone,  
23           a consumer reporting agency shall notify all other  
24           consumer reporting agencies described in section  
25           603(p)(1) not later than 3 days after placing, re-

1 moving, or temporarily suspending a security freeze  
2 on the file of the consumer under subsection (a),  
3 (c)(2)(A), or (c)(4), respectively.

4 “(3) IMPLEMENTATION BY OTHER COVERED  
5 ENTITIES.—A consumer reporting agency that is no-  
6 tified of a request under paragraph (2) to place, re-  
7 move, or temporarily suspend a security freeze on  
8 the file of a consumer shall—

9 “(A) request proper identification from the  
10 consumer, in accordance with subsection (f),  
11 not later than 3 business days after receiving  
12 the notification; and

13 “(B) place, remove, or temporarily suspend  
14 the security freeze on that credit report not  
15 later than 3 business days after receiving prop-  
16 er identification.

17 “(e) CONFIRMATION.—Except as provided in sub-  
18 section (c)(3), whenever a consumer reporting agency  
19 places, removes, or temporarily suspends a security freeze  
20 on the file of a consumer at the request of that consumer  
21 under subsection (a) or (c), respectively, it shall send a  
22 written confirmation thereof to the consumer not later  
23 than 10 business days after placing, removing, or tempo-  
24 rarily suspending the security freeze on the file. This sub-  
25 section does not apply to the placement, removal, or tem-

1 porary suspension of a security freeze by a consumer re-  
2 porting agency because of a notification received under  
3 subsection (d)(2).

4 “(f) IDENTIFICATION REQUIRED.—A consumer re-  
5 porting agency may not place, remove, or temporarily sus-  
6 pend a security freeze on the file of a consumer or other-  
7 wise provide a credit report or score in accordance with  
8 this section at the request of the consumer, unless the con-  
9 sumer provides proper identification (within the meaning  
10 of section 610(a)(1) and the regulations thereunder).

11 “(g) EXCEPTIONS.—This section does not apply to  
12 the use of a consumer credit report by any of the fol-  
13 lowing:

14 “(1) A person or entity, or a subsidiary, affil-  
15 iate, or agent of that person or entity, or an as-  
16 signee of a financial obligation owing by the con-  
17 sumer to that person or entity, or a prospective as-  
18 signee of a financial obligation owing by the con-  
19 sumer to that person or entity in conjunction with  
20 the proposed purchase of the financial obligation,  
21 with which the consumer has or had prior to assign-  
22 ment an account or contract, including a demand de-  
23 posit account, or to whom the consumer issued a ne-  
24 gotiable instrument, for the purposes of reviewing  
25 the account or collecting the financial obligation

1 owing for the account, contract, or negotiable instru-  
2 ment.

3 “(2) Any Federal, State, or local agency, law  
4 enforcement agency, trial court, or private collection  
5 agency acting pursuant to a court order, warrant,  
6 subpoena, or other compulsory process.

7 “(3) A child support agency or its agents or as-  
8 signs acting pursuant to subtitle D of title IV of the  
9 Social Security Act (42 U.S.C. et seq.) or similar  
10 State law.

11 “(4) The Department of Health and Human  
12 Services, a similar State agency, or the agents or as-  
13 signs of the Federal or State agency acting to inves-  
14 tigate Medicare or Medicaid fraud.

15 “(5) The Internal Revenue Service or a State  
16 or municipal taxing authority, or a State department  
17 of motor vehicles, or any of the agents or assigns of  
18 these Federal, State, or municipal agencies acting to  
19 investigate or collect delinquent taxes, or unpaid  
20 court orders, or to fulfill any of their other statutory  
21 responsibilities.

22 “(6) The use of consumer credit information for  
23 the purposes of prescreening as provided in this  
24 title.



1           “(7) Any person or entity administering a cred-  
2           it file monitoring subscription to which the consumer  
3           has subscribed.

4           “(8) Any person or entity for the purpose of  
5           providing a consumer with a copy of his or her cred-  
6           it report or credit score, upon the request of the con-  
7           sumer and upon provision of appropriate identifica-  
8           tion in accordance with subsection (f).

9           “(h) FEES.—

10           “(1) IN GENERAL.—Except as provided in para-  
11           graph (2), a consumer reporting agency may charge  
12           a reasonable fee, as determined by the Commission  
13           by rule, promulgated in accordance with section 553  
14           of title 5, United States Code, for placing, removing,  
15           or temporarily suspending a security freeze on the  
16           file of a consumer under this section.

17           “(2) EXCEPTION FOR IDENTIFICATION THEFT  
18           VICTIMS.—A consumer reporting agency may not  
19           charge a fee for placing, removing, or temporarily  
20           suspending a security freeze on the file of a con-  
21           sumer, if—

22                   “(A) the consumer is a victim of identity  
23           theft;

24                   “(B) the consumer requests the security  
25           freeze in writing;

1           “(C) the consumer has filed a police report  
2 with respect to the theft, or an identity theft re-  
3 port (as defined in section 603(q)(4)), not later  
4 than 90 days after the date on which the theft  
5 occurred or was discovered by the consumer;

6           “(D) the consumer provides a copy of the  
7 police report to the consumer reporting agency;  
8 and

9           “(E) the consumer—

10           “(i) has been notified by any entity  
11 that personally identifiable information  
12 handled by that entity has been com-  
13 promised or breached; and

14           “(ii) notifies the consumer reporting  
15 agency of such compromise or breach.

16           “(i) LIMITATION ON INFORMATION CHANGES IN  
17 FROZEN FILES.—

18           “(1) IN GENERAL.—If a security freeze is in  
19 place on the file of consumer, a consumer reporting  
20 agency may not change any of the following official  
21 information in that file without sending a written  
22 confirmation of the change to the consumer, not  
23 later than 30 days after the change is made:

24           “(A) Name.

25           “(B) Date of birth.

1           “(C) Social Security number.

2           “(D) Address.

3           “(2) CONFIRMATION.—Paragraph (1) does not  
4 require written confirmation for technical modifica-  
5 tions of a consumer’s official information, including  
6 name and street abbreviations, complete spellings, or  
7 transposition of numbers or letters. In the case of an  
8 address change, the written confirmation shall be  
9 sent to both the new address and to the former ad-  
10 dress.

11          “(j) CERTAIN ENTITY EXEMPTIONS.—

12           “(1) AGGREGATORS AND OTHER AGENCIES.—  
13 The provisions of subsections (a) through (i) do not  
14 apply to a consumer reporting agency that acts only  
15 as a reseller of credit information by assembling and  
16 merging information contained in the data base of  
17 another consumer reporting agency or multiple con-  
18 sumer reporting agencies, and does not maintain a  
19 permanent data base of credit information from  
20 which new consumer credit reports are produced.

21           “(2) OTHER EXEMPTED ENTITIES.—The fol-  
22 lowing entities are not required to place a security  
23 freeze on the file of a consumer under this section:

24           “(A) A check services or fraud prevention  
25 services company which issues reports on inci-

1           dents of fraud or authorizations for the purpose  
2           of approving or processing negotiable instru-  
3           ments, electronic funds transfers, or similar  
4           methods of payments.

5           “(B) A deposit account information service  
6           company which issues reports regarding ac-  
7           count closures due to fraud, substantial over-  
8           drafts, ATM abuse, or similar negative informa-  
9           tion regarding a consumer, to inquiring banks  
10          or other financial institutions for use only in re-  
11          viewing a consumer request for a deposit ac-  
12          count at the inquiring bank or financial institu-  
13          tion.

14          “(k) STATE PREEMPTION.—This section shall pre-  
15          empt any provision of State or local law, regulation, or  
16          rule that requires consumer reporting agencies to comply  
17          with the request of a consumer to place, remove, or tempo-  
18          rarily suspend a prohibition on the release by a consumer  
19          reporting agency of information from its files on that con-  
20          sumer, but only if it is determined by the Commission that  
21          this section will provide materially stronger consumer pro-  
22          tections than those afforded to consumers under otherwise  
23          applicable State or local law.”.

1 **SEC. 10. SAFEGUARDING AMERICANS FROM EXPORTING**  
2 **IDENTIFICATION DATA.**

3 (a) DEFINITIONS.—As used in this section:

4 (1) BUSINESS ENTERPRISE.—The term “busi-  
5 ness enterprise” means—

6 (A) any organization, association, or ven-  
7 ture established to make a profit;

8 (B) any health care business;

9 (C) any private, nonprofit organization; or

10 (D) any contractor, subcontractor, or po-  
11 tential subcontractor of an entity described in  
12 subparagraph (A), (B), or (C).

13 (2) HEALTH CARE BUSINESS.—The term  
14 “health care business” means any business enter-  
15 prise or private, nonprofit organization that collects  
16 or retains personally identifiable information about  
17 consumers in relation to medical care, including—

18 (A) hospitals;

19 (B) health maintenance organizations;

20 (C) medical partnerships;

21 (D) emergency medical transportation  
22 companies;

23 (E) medical transcription companies;

24 (F) banks that collect or process medical  
25 billing information; and

1           (G) subcontractors, or potential sub-  
2           contractors, of the entities described in sub-  
3           paragraphs (A) through (F).

4           (3) PERSONALLY IDENTIFIABLE INFORMA-  
5           TION.—The term “personally identifiable informa-  
6           tion” includes information such as—

7                   (A) name;

8                   (B) postal address;

9                   (C) financial information;

10                  (D) medical records;

11                  (E) date of birth;

12                  (F) phone number;

13                  (G) e-mail address;

14                  (H) social security number;

15                  (I) mother’s maiden name;

16                  (J) password;

17                  (K) State identification information; and

18                  (L) driver’s license number.

19           (b) TRANSMISSION OF INFORMATION.—

20                   (1) PROHIBITION.—A business enterprise may  
21           not disclose personally identifiable information re-  
22           garding a resident of the United States to any for-  
23           eign branch, affiliate, subcontractor, or unaffiliated  
24           third party located in a foreign country unless—

1 (A) the business enterprise provides the  
2 notice of privacy protections described in sec-  
3 tions 502 and 503 of the Gramm-Leach-Bliley  
4 Act (15 U.S.C. 6802 and 6803) or required by  
5 the regulations promulgated pursuant to section  
6 264(c) of the Health Insurance Portability and  
7 Accountability Act of 1996 (42 U.S.C. 1320d-  
8 2 note), as appropriate;

9 (B) the business enterprise complies with  
10 the safeguards described in section 501(b) of  
11 the Gramm-Leach-Bliley Act (15 U.S.C.  
12 6801(b)), as appropriate;

13 (C) the consumer is given the opportunity,  
14 before the time that such information is initially  
15 disclosed, to object to the disclosure of such in-  
16 formation to such foreign branch, affiliate, sub-  
17 contractor, or unaffiliated third party; and

18 (D) the consumer is given an explanation  
19 of how the consumer can exercise the nondisclo-  
20 sure option described in subparagraph (C).

21 (2) HEALTH CARE BUSINESSES.—A health care  
22 business may not terminate an existing relationship  
23 with a consumer of health care services to avoid the  
24 consumer from objecting to the disclosure under  
25 paragraph (1)(C).

1 (3) EFFECT ON BUSINESS RELATIONSHIP.—

2 (A) NONDISCRIMINATION.—A business en-  
3 terprise may not discriminate against or deny  
4 an otherwise qualified consumer a financial  
5 product or a health care service because the  
6 consumer has objected to the disclosure under  
7 paragraph (1)(C).

8 (B) PRODUCTS AND SERVICES.—A busi-  
9 ness enterprise shall not be required to offer or  
10 provide a product or service through affiliated  
11 entities or jointly with nonaffiliated business en-  
12 terprises.

13 (C) INCENTIVES AND DISCOUNTS.—Noth-  
14 ing in this subsection is intended to prohibit a  
15 business enterprise from offering incentives or  
16 discounts to elicit a specific response to the no-  
17 tice required under paragraph (1).

18 (4) LIABILITY.—

19 (A) IN GENERAL.—A business enterprise  
20 that knowingly and directly transfers personally  
21 identifiable information to a foreign branch, af-  
22 filiate, subcontractor, or unaffiliated third party  
23 shall be liable to any person suffering damages  
24 resulting from the improper storage, duplica-



1           tion, sharing, or other misuse of such informa-  
2           tion by the transferee.

3           (B) CIVIL ACTION.—An injured party  
4           under subparagraph (A) may sue in law or in  
5           equity in any court of competent jurisdiction to  
6           recover the damages sustained as a result of a  
7           violation of this subsection.

8           (5) RULEMAKING.—The Chairman of the Fed-  
9           eral Trade Commission shall promulgate regulations  
10          through which the Chairman may enforce the provi-  
11          sions of this subsection and impose a civil penalty  
12          for a violation of this section.

13          (c) PRIVACY FOR CONSUMERS OF HEALTH SERV-  
14          ICES.—The Secretary of Health and Human Services shall  
15          revise the regulations promulgated pursuant to section  
16          264(c) of the Health Insurance Portability and Account-  
17          ability Act of 1996 (42 U.S.C. 1320d–2 note) to require  
18          a covered entity (as defined by such regulations) that  
19          outsources protected health information (as defined by  
20          such regulations) outside the United States to include in  
21          such entity’s notice of privacy protections—

22               (1) notification that the covered entity  
23               outsources protected health information to business  
24               associates (as defined by such regulations) for proc-  
25               essing outside the United States;

1           (2) a description of the privacy laws of the  
2 country to which the protected health information  
3 will be sent;

4           (3) any additional risks and consequences to  
5 the privacy and security of protected health informa-  
6 tion that arise as a result of the processing of such  
7 information in a foreign country;

8           (4) additional measures the covered entity is  
9 taking to protect the protected health information  
10 outsourced for processing outside the United States;

11           (5) notification that the protected health infor-  
12 mation will not be outsourced outside the United  
13 States if the consumer objects; and

14           (6) a certification that—

15           (A) the covered entity has taken reason-  
16 able steps to identify the locations where pro-  
17 tected health information is outsourced by such  
18 business associates;

19           (B) attests to the privacy and security of  
20 the protected health information outsourced for  
21 processing outside the United States; and

22           (C) states the reasons for the determina-  
23 tion by the covered entity that the privacy and  
24 security of such information is maintained.

1 (d) PRIVACY FOR CONSUMERS OF FINANCIAL SERV-  
2 ICES.—Section 503(b) of the Gramm-Leach-Bliley Act (15  
3 U.S.C. 6803(b)) is amended—

4 (1) in paragraph (3), by striking “and” after  
5 the semicolon;

6 (2) in paragraph (4), by striking the period at  
7 the end and inserting “; and”; and

8 (3) by adding at the end the following:

9 “(5) if the financial institution outsources non-  
10 public personal information outside the United  
11 States—

12 “(A) information informing the consumer  
13 in simple language—

14 “(i) that the financial institution  
15 outsources nonpublic personal information  
16 to entities for processing outside the  
17 United States;

18 “(ii) of the privacy laws of the coun-  
19 try to which nonpublic personal informa-  
20 tion will be sent;

21 “(iii) of any additional risks and con-  
22 sequences to the privacy and security of an  
23 individual’s nonpublic personal information  
24 that arise as a result of the processing of  
25 such information in a foreign country; and

1           “(iv) of the additional measures the  
2           financial institution is taking to protect the  
3           nonpublic personal information outsourced  
4           for processing outside the United States;  
5           and

6           “(B) a certification that—

7           “(i) the financial institution has taken  
8           reasonable steps to identify the locations  
9           where nonpublic personal information is  
10          outsourced by such entities;

11          “(ii) attests to the privacy and secu-  
12          rity of the nonpublic personal information  
13          outsourced for processing outside the  
14          United States; and

15          “(iii) states the reasons for the deter-  
16          mination by the institution that the privacy  
17          and security of such information is main-  
18          tained.”.

19          (e) **EFFECTIVE DATE.**—This section shall take effect  
20          on the expiration of the date which is 90 days after the  
21          date of enactment of this Act.

22          **SEC. 11. TELEPHONE AND COMMUNICATIONS RECORDS .**

23          (a) **IN GENERAL.**—Not later than 120 days after the  
24          date of enactment of this Act, the Federal Trade Commis-  
25          sion, the Federal Communications Commission and the

1 Attorney General shall establish a Center for Tele-  
2 communications Records Privacy (referred to in this sec-  
3 tion as the “Center”) which shall consist of the appro-  
4 priate designees of each agency which shall be established  
5 by a memorandum of understanding among the agencies.

6 (b) RESPONSIBILITIES.—The Center shall—

7 (1) be charged with evaluating the current  
8 rules, regulations and law regarding the unauthor-  
9 ized disclosure, access, and sharing of telephone and  
10 telephony technology call records and identify gaps  
11 in coverage and enforcement regarding the unau-  
12 thorized disclosure, sharing, or sale of telephone and  
13 communications records; and

14 (2) on an annual basis—

15 (A) provide an assessment of the frequency  
16 and scope of the unauthorized and criminal dis-  
17 closure of telecommunications records and pro-  
18 vide an evaluation of the effectiveness of en-  
19 acted laws and regulations;

20 (B) identify new telecommunications tech-  
21 nologies not covered by current law or regula-  
22 tion; and

23 (C) make recommendations to Congress re-  
24 garding other legislative or regulatory steps  
25 that can be taken to address emerging issues.

1 **SEC. 12. FEDERAL TRADE COMMISSION RULES FOR DATA**  
2 **PROCESSORS AND RULES FOR FEDERAL**  
3 **AGENCIES.**

4 (a) IN GENERAL.—The Federal Trade Commission  
5 shall issue new rules for Federal agencies responsible for  
6 working with data processors to ensure the security and  
7 confidentiality of nonpublic personal information to—

8 (1) protect against any anticipated threats or  
9 hazards to the security or integrity of such informa-  
10 tion;

11 (2) protect against unauthorized access to or  
12 use of such information which could result in sub-  
13 stantial harm or inconvenience to a customer or the  
14 relevant financial institution; and

15 (3) protect against the illegal or unauthorized  
16 collection of personally identifiable information by  
17 data processors.

18 (b) DEFINITION.—In this section, the term “data  
19 processor” means any entity the business of which in  
20 whole or in part is the handling processing, compilation,  
21 exchange, transmittal, or other management or processing  
22 of the nonpublic personal information of consumers by  
23 agreement on behalf of another institution.

24 (c) REPORT.—Each Federal agency covered by this  
25 section shall submit annual reports to the Chief Privacy  
26 Officer established under section 4, which shall include an

1 assessment of agency policies and protocols dealing with  
2 data security and what steps are being taken to ensure  
3 against threats and hazards to that security and pro-  
4 tecting against unauthorized access or use of data.

5 **SEC. 13. MEDICAL RECORDS.**

6 (a) APPLICATION OF PENALTIES TO CERTAIN EM-  
7 PLOYEES.—Section 1177 of the Social Security Act (42  
8 U.S.C. 1320d–6) is amended by adding at the end the fol-  
9 lowing:

10 “(c) CLARIFICATION OF APPLICATION.—The provi-  
11 sions of subsection (a) shall apply to individuals who  
12 knowingly use, obtain, or disclose individually identifiable  
13 health information or a unique health identifier regardless  
14 of the manner in which such individuals obtain such infor-  
15 mation or the relation of the individual to the entity that  
16 maintains the information involved. The preceding sen-  
17 tence shall apply to individuals who illegally hack into  
18 computer systems to obtain data.”.

19 (b) EXPANDING THE SCOPE OF THE HIPAA PRI-  
20 VACY RULE.—

21 (1) IN GENERAL.—The Secretary of Health and  
22 Human Services shall modify the regulations pro-  
23 mulgated under section 264(c) of the Health Insur-  
24 ance Portability and Accountability Act (42 U.S.C.  
25 1320dd–2 note) to broaden the scope of who is con-

1       sidered to be a covered entity to include those enti-  
2       ties and individuals that disclose health information  
3       to other entities in the course of their commercial  
4       activities and not in relation to the provision of  
5       healthcare services.

6           (2) TIMING.—The Secretary of Health and  
7       Human Services shall—

8           (A) not later than 12 months after the  
9       date of enactment of this Act, promulgate a  
10      proposed rule for the modifications described in  
11      paragraph (1); and

12          (B) not later than 24 months after the  
13      date of enactment of this Act, promulgate a  
14      final rule for the modifications described in  
15      paragraph (1).

16          (3) REINSTATEMENT OF CERTAIN CONSENT  
17      PROVISIONS.—Notwithstanding any other provision  
18      of law, the provisions of section 164–506(b) of title  
19      45, Code of Federal Regulations, as in effect on  
20      April 14, 2001 and modified in 2002, relating to the  
21      consent to use and disclose certain information for  
22      treatment, payment, or health care operations, shall  
23      be deemed to be reinstated and implemented accord-  
24      ingly.



1           (c) REPORTING REQUIREMENTS.—The Secretary of  
2 Health and Human Services shall develop a procedure for  
3 the reporting to the Secretary, by individuals or entities  
4 receiving assistance from the Department of Health and  
5 Human Services, of any unlawful disclosures of identifi-  
6 able health information in violation of section 1176 or  
7 1177 of the Social Security Act (42 U.S.C. 12320d–5;  
8 1320d–6) or the regulations promulgated under section  
9 264(c) of the Health Insurance Portability and Account-  
10 ability Act (42 U.S.C. 1320dd–2 note) by such individuals  
11 or entities. In developing such procedure, the Secretary  
12 shall—

13           (1) take into consideration the notification pro-  
14 cedures used by other public or private sector enti-  
15 ties, including the TRICARE program; and

16           (2) provide for the appropriate notification, by  
17 individuals or entities receiving assistance from the  
18 Department of Health and Human Services, to indi-  
19 viduals whose identifiable health information has  
20 been disclosed in violation of such section 1176 or  
21 1177 or such regulations by such individuals or enti-  
22 ties.

23           (d) INVESTIGATION OF COMPLAINTS.—With respect  
24 to a report of an unlawful disclosure of health information  
25 under subsection (c), the Secretary of Health and Human

1 Services shall investigate such disclosure using the com-  
2 plaint process contained in subpart C of part 160 of title  
3 45, Code of Federal Regulations (as in effect on the date  
4 of enactment of this Act), except that for purposes of the  
5 review process contained in section 160.308 of such sub-  
6 part, the Secretary shall establish a schedule of routine  
7 compliance reviews of covered entities (as such term is  
8 used for purposes of such section).

○