

109TH CONGRESS
1ST SESSION

S. _____

To provide for comprehensive identity theft prevention.

IN THE SENATE OF THE UNITED STATES

Mr. SCHUMER (for himself and Mr. NELSON of Florida) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To provide for comprehensive identity theft prevention.

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; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Comprehensive Identity Theft Prevention Act”.

6 (b) **TABLE OF CONTENTS.**—The table of contents of
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Establishment of Office of Identity Theft.
- Sec. 4. Helping consumers recapture their stolen identities.
- Sec. 5. Reasonable steps to protect sensitive personal information.
- Sec. 6. Limitations on sale or transfer of sensitive personal information.
- Sec. 7. Coordinating international action against identity theft.
- Sec. 8. Notification of information breaches.
- Sec. 9. Social security number protection.

- Sec. 10. Information sharing requirements.
- Sec. 11. Improving cybersecurity.
- Sec. 12. Prohibition of posting account numbers and individuals' names.
- Sec. 13. Online information security working group.
- Sec. 14. Study to examine the use of social security numbers by the government.
- Sec. 15. Annual identity theft report.
- Sec. 16. Preemption of State law.
- Sec. 17. Noninterference with the Fair Credit Reporting Act.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) COVERED PERSON.—Except as otherwise
4 provided, the term “covered person” means a com-
5 mercial entity.

6 (2) SENSITIVE PERSONAL INFORMATION.—The
7 term “sensitive personal information” means the fol-
8 lowing information with regard to an individual:

9 (A) The social security number of such in-
10 dividual.

11 (B) The medical condition and legal drugs,
12 therapies, or medical products or equipment
13 used by such individual.

14 (C) The bank or investment account num-
15 ber of such individual.

16 (D) The credit card or debit card number
17 of such individual.

18 (E) The payment history of such indi-
19 vidual.

1 (F) The State driver's license identification
2 number or State resident identification number
3 of such individual.

4 (G) Any other information regarding an
5 individual determined appropriate by the Fed-
6 eral Trade Commission.

7 **SEC. 3. ESTABLISHMENT OF OFFICE OF IDENTITY THEFT.**

8 (a) **ESTABLISHMENT.**—There is established in the
9 Federal Trade Commission an Office of Identity Theft.

10 (b) **JURISDICTION.**—The Office of Identity Theft
11 shall have civil jurisdiction of any covered person that col-
12 lects, maintains, sells, or transfers sensitive personal infor-
13 mation, or attempts to collect, maintain, sell, or transfer
14 sensitive personal information.

15 (c) **REGULATIONS.**—Consistent with this Act, the
16 Federal Trade Commission shall promulgate regulations
17 to enable the Office of Identity Theft to protect con-
18 sumers' sensitive personal information collected, main-
19 tained, sold, or transferred, or attempted to be collected,
20 maintained, sold, or transferred by covered persons.

21 (d) **CIVIL ENFORCEMENT.**—The Office of Identity
22 Theft may take civil enforcement actions against covered
23 persons that violate the requirements of this Act and the
24 Office of Identity Theft's rules promulgated to carry out
25 this Act.

1 (e) AUTHORIZATION OF APPROPRIATIONS.—There
2 are authorized to be appropriated for the Office of Identity
3 Theft \$60,000,000 for fiscal year 2006 and each of the
4 4 succeeding fiscal years.

5 **SEC. 4. HELPING CONSUMERS RECAPTURE THEIR STOLEN**
6 **IDENTITIES.**

7 The Office of Identity Theft shall carry out the fol-
8 lowing activities:

9 (1) Establish a website, easily and conspicu-
10 ously accessible from ftc.gov, dedicated to assisting
11 consumers with the retrieval of the consumer's sto-
12 len or compromised sensitive personal information.

13 (2) Maintain a toll-free phone number to help
14 answer questions concerning identity theft from con-
15 sumers.

16 (3) Establish online and offline consumer-serv-
17 ice teams to assist consumers seeking the retrieval
18 of the consumer's sensitive personal information.

19 (4) Establish a reasonable standard for deter-
20 mining when an individual becomes a victim of iden-
21 tity theft.

22 (5) Issue certifications to individuals who,
23 under the standard described in paragraph (4), are
24 identity theft victims.

1 (6) Permit an individual to use the Office of
2 Identity Theft certification in all Federal, State, and
3 local jurisdictions, in lieu of a police report or any
4 other document required by State or local law, as a
5 prerequisite to accessing business records of trans-
6 actions done by someone claiming to be the indi-
7 vidual.

8 (7) In addition to the requirements in para-
9 graphs (1) through (6), the Federal Trade Commis-
10 sion shall promulgate regulations that enable the Of-
11 fice of Identity Theft to help consumers restore their
12 stolen or otherwise compromised sensitive personal
13 information quickly and inexpensively.

14 **SEC. 5. REASONABLE STEPS TO PROTECT SENSITIVE PER-**
15 **SONAL INFORMATION.**

16 (a) REGULATIONS.—Not later than 9 months after
17 the date of enactment of this Act, the Federal Trade Com-
18 mission shall promulgate regulations governing the sale,
19 maintenance, collection, or transfer of sensitive personal
20 information by covered persons, including a requirement
21 that covered persons take reasonable steps to prevent un-
22 authorized access to sensitive personal information the
23 covered person sells, maintains, collects, or transfers.

1 (b) PENALTIES.—A covered person that violates sub-
2 section (a) shall be subject to a civil penalty of not more
3 than \$500 per person per violation.

4 (c) ACTIONS.—An action to enforce a violation of
5 subsection (a) may be brought by the Federal Trade Com-
6 mission in any appropriate United States district court or
7 any other court of competent jurisdiction.

8 **SEC. 6. LIMITATIONS ON SALE OR TRANSFER OF SENSITIVE**
9 **PERSONAL INFORMATION.**

10 (a) DATA MERCHANT.—

11 (1) IN GENERAL.—In this section, except as
12 provided in paragraph (2), the term “data mer-
13 chant” means any covered person that engages in
14 collecting, assembling, or selling sensitive personal
15 information in a significant manner or that is a sig-
16 nificant part of the operations of such person,
17 whether such collection, assembly, or sale of person-
18 ally identifiable information is performed by the cov-
19 ered person directly, or by contract or subcontract
20 with another entity .

21 (2) EXCLUSIONS.—The term “data merchant”
22 shall not include either of the following:

23 (A) An organization described in section
24 501(c) or 527 of the Internal Revenue Code of
25 1986.

1 (B) An entity that only collects, assembles,
2 or sells information that is completely de-identi-
3 fied.

4 (3) CREDIT BUREAUS.—

5 (A) IN GENERAL.—

6 (i) REGULATION OF CREDIT HEADER
7 INFORMATION FURNISHED OUTSIDE A
8 FULL CONSUMER REPORT.—A credit bu-
9 reau that furnishes information regarding
10 the social security numbers and any other
11 nonpublic personal information of a con-
12 sumer, or any derivative thereof, to any
13 person other than in a full consumer re-
14 port furnished in accordance with section
15 604 of the Fair Credit Reporting Act (15
16 U.S.C. 1681b), shall be a data merchant
17 for purposes of this section and shall reg-
18 ister with the Office of Identity Theft pur-
19 suant to subsection (b), and such trans-
20 action of furnishing such information out-
21 side of a full consumer report shall be sub-
22 ject to the provisions of this section and
23 regulations promulgated to carry out this
24 section.

1 (ii) FCRA AND FACTA TO APPLY TO
2 FULL CONSUMER REPORTS.—Except as
3 provided in clause (i), to the extent that an
4 activity or transaction of a credit bureau is
5 covered under the Fair Credit Reporting
6 Act (15 U.S.C. 1601 et seq.) or the Fair
7 and Accurate Credit Transactions Act of
8 2003 (Public Law 108–159), including fur-
9 nishing information regarding the social
10 security numbers and any other nonpublic
11 personal information of a consumer, or any
12 derivative thereof, to a person in a full
13 consumer report, such activity or trans-
14 action shall be governed by such Acts and
15 not under this section.

16 (B) NONPUBLIC PERSONAL INFORMA-
17 TION.—In this paragraph, the term “nonpublic
18 personal information” has the meaning given
19 such term in section 509(4) of the Gramm-
20 Leach-Bliley Act.

21 (b) REGISTRATION.—

22 (1) IN GENERAL.—Each data merchant shall
23 register with the Office of Identity Theft.

24 (2) FAILURE TO REGISTER.—A data merchant
25 that does not register with the Office of Identity

1 Theft within 9 months of the date of enactment of
2 this Act shall be subject to a fine of not more than
3 \$75 for each consumer's record the data merchant
4 keeps for each day the data merchant failed to time-
5 ly register with the Office of Identity Theft as a
6 data merchant.

7 (c) RESTRICTIONS.—

8 (1) IN GENERAL.—Not later than 9 months
9 after the date of enactment of this Act, the Federal
10 Trade Commission shall promulgate rules governing
11 the sale or transfer of sensitive personal information
12 by data merchants registered pursuant to this sec-
13 tion.

14 (2) RULES.—The rules described in paragraph
15 (1) shall include the following:

16 (A) AUTHENTICATION PROCESS.—A re-
17 quirement that each data merchant to have a
18 secure and dependable authentication process
19 for each third party whom the data merchant
20 permits to have access to consumer's sensitive
21 personal information kept in the data mer-
22 chant's custody.

23 (B) PASSWORDS.—A requirement that
24 each data merchant adopt a password for each
25 individual employee of a third party customer of

1 consumer's sensitive personal information, in-
2 cluding a requirement that each data merchant
3 only allow an individual employee of a third
4 party customer who has passed a reasonably ef-
5 fective background check to have access to such
6 password.

7 (C) TRACKING.—A requirement that each
8 data merchant have the ability to track who
9 accessed what records containing sensitive per-
10 sonal information and for what purpose the
11 records were accessed.

12 (D) SAFEGUARDS.—A requirement that
13 each data merchant have safeguards in place to
14 prevent access to sensitive personal information
15 by unauthorized parties.

16 (E) REPORT.—Standards for the creation
17 of a simple procedure that would permit a con-
18 sumer to request and receive a report from any
19 data merchant holding the consumer's sensitive
20 personal information. Such procedure shall be a
21 nearly identical procedure to the procedure out-
22 lined for requests for consumer reports provided
23 under sections 612 and 609(e) of the Fair
24 Credit Reporting Act (15 U.S.C. 1681j and
25 1681g(c)) and section 211 of the Fair and Ac-

1 curate Credit Transactions Act of 2003 (Public
2 Law 108–159), and shall include the following:

3 (i) CONTENT OF REPORT.—The re-
4 port shall provide the consumer with a sta-
5 tus of what sensitive personal information
6 the data merchant has with regard to the
7 requesting consumer, what the data mer-
8 chant has done, if anything, with the con-
9 sumer’s sensitive personal information in
10 the data merchant’s custody, the names of
11 the third parties who have gained access,
12 or who have sought to gain access, to the
13 consumer’s sensitive personal information,
14 and the purposes for which the third party
15 gained access, or sought to gain access, to
16 the consumer’s sensitive personal informa-
17 tion.

18 (ii) FREE REPORT.—Each year, the
19 consumer shall be permitted 1 free report,
20 but shall be permitted to request additional
21 reports within a calendar year for a rea-
22 sonable fee to be set by the Office of Iden-
23 tity Theft.

24 (iii) PROCESS.—The process for re-
25 questing a report from the Office of Iden-

1 tity Theft shall closely follow the process
2 for requesting consumer reports under sec-
3 tion 211 of the Fair and Accurate Credit
4 Transactions Act of 2003 (Public Law
5 108–159) and the amendments made by
6 such section.

7 (iv) CORRECTION.—The procedure
8 shall permit consumers to demand and re-
9 ceive prompt correction of errors found in
10 the data merchant’s records.

11 (F) ACCURACY.—A requirement for data
12 merchants for dealing with the data that guar-
13 antees the same standard of accuracy as ex-
14 pected under the Fair Credit Reporting Act (15
15 U.S.C. 1601 et seq.) for entities within the ju-
16 risdiction of such Act.

17 (d) PENALTY.—A data merchant that violates a re-
18 quirement of this section or regulations promulgated by
19 the Federal Trade Commission pursuant to this section
20 shall be subject to a civil penalty of not more than \$1,000
21 per individual record per violation.

22 (e) ACTIONS.—An action to enforce a violation of this
23 section or regulations promulgated by the Federal Trade
24 Commission pursuant to this section may be brought by
25 the Federal Trade Commission or the appropriate State

1 attorney general in any appropriate United States district
2 court or any other court of competent jurisdiction.

3 (f) EXEMPTION.—The Federal Trade Commission, in
4 promulgating regulations under this section, may exempt
5 any data merchant from such regulations, in whole or in
6 part, if the Commission determines that granting such an
7 exemption is in the public interest, and if the data mer-
8 chant’s collecting, assembling, or selling of sensitive per-
9 sonal information is only incidental to the data merchant’s
10 primary business.

11 **SEC. 7. COORDINATING INTERNATIONAL ACTION AGAINST**
12 **IDENTITY THEFT.**

13 There is established within the Office of Identity
14 Theft an international directorate that shall be devoted
15 to coordinating international responses to identity theft
16 and the international development of best practices to pro-
17 tect consumers worldwide from identity theft.

18 **SEC. 8. NOTIFICATION OF INFORMATION BREACHES.**

19 (a) IN GENERAL.—If a covered person has sensitive
20 personal information regarding an individual and such in-
21 dividual’s unencrypted sensitive personal information was,
22 or is reasonably believed to have been, acquired by an un-
23 authorized person in combination with the individual’s
24 first name or first initial and last name or any combina-
25 tion of identifying information that would allow the unau-

1 thORIZED person to reasonably be able to identify the indi-
2 VIDUAL, the covered person shall—

3 (1) give notice to the individual whose
4 unencrypted sensitive personal information was, or is
5 reasonable believed to have been, acquired by an un-
6 authorized person; and

7 (2) notify the Office of Identity Theft, if the
8 covered person holds sensitive personal information
9 for more than 1,000 individuals.

10 (b) METHODS OF NOTICE.—

11 (1) IN GENERAL.—A covered person that is re-
12 quired to provide notification pursuant to subsection
13 (a) shall notify the individual either in writing or by
14 electronic mail.

15 (2) TIMING.—Except as provided in paragraph
16 (3), notifications required under this section shall be
17 made in the most expedient time possible and with-
18 out unreasonable delay consistent with any measures
19 necessary to determine the scope of the breach and
20 restore the reasonable integrity of the data system.

21 (3) DELAY.—A notification may be delayed if
22 either of the following occur:

23 (A) If Federal, State, or local law enforce-
24 ment determines that notification would impede
25 a criminal investigation, notification may be de-

1 laid as long as the law enforcement agency de-
2 termines reasonably necessary.

3 (B) The Office of Identity Theft certifies
4 that the covered person showed cause of exigent
5 circumstance meriting further delay.

6 (c) PENALTIES AND ACTIONS FOR VIOLATIONS.—

7 (1) PENALTY.—Any covered person that vio-
8 lates the notice requirements under this section shall
9 be subject to a civil penalty of not more than \$1,000
10 per violation per individual record accessed.

11 (2) ACTIONS.—An action to enforce a violation
12 of this section may be brought by the Federal Trade
13 Commission or the appropriate State attorney gen-
14 eral in any appropriate United States district court
15 or any other court of competent jurisdiction.

16 (d) CONSUMER REDRESS.—

17 (1) IN GENERAL.—After receiving a notification
18 under this section, an individual may request in
19 writing that the covered person expunge the individ-
20 ual’s sensitive personal information from the covered
21 person’s records.

22 (2) COVERED PERSON.—In this subsection, the
23 term “covered person” does not include credit bu-
24 reaus.

1 **SEC. 9. SOCIAL SECURITY NUMBER PROTECTION.**

2 (a) PROHIBITION OF UNNECESSARY SOLICITATION
3 OF SOCIAL SECURITY NUMBERS.—

4 (1) IN GENERAL.—No person may solicit any
5 social security number unless—

6 (A) such number is necessary for the nor-
7 mal course of business; and

8 (B) there is a specific use of the social se-
9 curity number for which no other identifying
10 number can be used.

11 (2) ENFORCEMENT.—

12 (A) IN GENERAL.—An action to enforce a
13 violation of paragraph (1) may be brought by
14 the Federal Trade Commission or the appro-
15 priate State attorney general in any appropriate
16 United States district court or any other court
17 of competent jurisdiction.

18 (B) CIVIL PENALTY.—A civil money pen-
19 alty of not more than \$1,000 may be imposed
20 for each violation of this subsection.

21 (b) PROHIBITION OF THE DISPLAY OF PERSONAL
22 IDENTIFICATION NUMBERS ON EMPLOYEE IDENTIFICA-
23 TION CARDS OR TAGS.—

24 (1) IN GENERAL.—Section 205(c)(2)(C) of the
25 Social Security Act (42 U.S.C. 405(c)(2)(C)) is

1 amended by adding at the end the following new
2 clause:

3 “(x) No employer (including any executive, legisla-
4 tive, or judicial agency or instrumentality of the Federal
5 Government or of a State or political subdivision thereof),
6 and no person offering benefits in connection with an em-
7 ployee benefit plan maintained by such employer or acting
8 as an agent of such employer, may display the social secu-
9 rity account number (or any derivative of such number)
10 on any card or tag that is commonly provided to employees
11 of such employer (or to their family members) for pur-
12 poses of identification.”.

13 (2) EFFECTIVE DATE.—The amendment made
14 by this subsection shall apply with respect to cards
15 or tags issued on or after the date that is 1 year
16 after the date of enactment of this Act.

17 (c) PROHIBITION OF INMATE ACCESS TO SOCIAL SE-
18 CURITY ACCOUNT NUMBERS.—

19 (1) IN GENERAL.—Section 205(c)(2)(C) of the
20 Social Security Act (42 U.S.C. 405(c)(2)(C)), as
21 amended by subsection (b), is amended by adding at
22 the end the following new clause:

23 “(xi) No executive, legislative, or judicial agency or
24 instrumentality of the Federal Government or of a State
25 or political subdivision thereof (or person acting as an

1 agent of such an agency or instrumentality) may employ,
2 or enter into a contract for the use or employment of, pris-
3 oners in any capacity that would allow such prisoners ac-
4 cess to the social security account numbers of other indi-
5 viduals. For purposes of this clause, the term ‘prisoner’
6 means an individual confined in a jail, prison, or other
7 penal institution or correctional facility.’’.

8 (2) EFFECTIVE DATE.—

9 (A) IN GENERAL.—Except as provided in
10 subparagraph (B), the amendment made by this
11 subsection shall apply with respect to employ-
12 ment of prisoners, or entry into contract for the
13 use or employment of prisoners, on or after the
14 date of enactment of this Act.

15 (B) TREATMENT OF CURRENT ARRANGE-
16 MENTS.—In the case of—

17 (i) prisoners employed as described in
18 clause (xi) of section 205(c)(2)(C) of the
19 Social Security Act (42 U.S.C.
20 405(c)(2)(C)), as added by paragraph (1),
21 on the date of enactment of this Act, and

22 (ii) contracts described in such clause
23 in effect on such date,

1 the amendment made by this section shall take
2 effect 90 days after the date of enactment of
3 this Act.

4 (d) PROHIBITION OF THE SALE, PURCHASE, OR DIS-
5 PLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECU-
6 RITY ACCOUNT NUMBER IN THE PRIVATE SECTOR.—

7 (1) IN GENERAL.—Title II of the Social Secu-
8 rity Act (42 U.S.C. 401 et seq.) is amended by in-
9 serting after section 208 the following new section:
10 “PROHIBITION OF THE SALE, PURCHASE, OR DISPLAY TO
11 THE GENERAL PUBLIC OF THE SOCIAL SECURITY
12 ACCOUNT NUMBER IN THE PRIVATE SECTOR

13 “SEC. 208A. (a) In this section:

14 “(1) PERSON.—

15 “(A) IN GENERAL.—Subject to subpara-
16 graph (B), the term ‘person’ means any indi-
17 vidual, partnership, corporation, trust, estate,
18 cooperative, association, or any other entity.

19 “(B) GOVERNMENTAL ENTITIES.—Such
20 term does not include a governmental entity.
21 Nothing in this subparagraph shall be con-
22 strued to authorize, in connection with a gov-
23 ernmental entity, an act or practice otherwise
24 prohibited under this section or section
25 205(c)(2)(C).

26 “(2) SELLING AND PURCHASING.—

1 “(A) IN GENERAL.—Subject to subpara-
2 graph (B)—

3 “(i) SELL.—The term ‘sell’, in con-
4 nection with a social security account num-
5 ber, means to obtain, directly or indirectly,
6 anything of value in exchange for such
7 number.

8 “(ii) PURCHASE.—The term ‘pur-
9 chase’, in connection with a social security
10 account number, means to provide, directly
11 or indirectly, anything of value in exchange
12 for such number.

13 “(B) EXCEPTIONS.—The terms ‘sell’ and
14 ‘purchase’, in connection with a social security
15 account number, do not include the submission
16 of such number as part of—

17 “(i) the process for applying for any
18 type of Government benefits or programs
19 (such as grants or loans or welfare or
20 other public assistance programs); or

21 “(ii) the administration of, or provi-
22 sion of benefits under, an employee benefit
23 plan.

24 “(3) DISPLAY TO THE GENERAL PUBLIC.—The
25 term ‘display to the general public’ means, in con-

1 nection with a social security account number, to in-
2 tentionally place such number in a viewable manner
3 on an Internet site that is available to the general
4 public or to make such number available in any
5 other manner intended to provide access to such
6 number by the general public.

7 “(4) SOCIAL SECURITY ACCOUNT NUMBER.—
8 The term ‘social security account number’ means a
9 social security account number assigned by the Com-
10 missioner under section 205(c)(2)(B).

11 “(b) PROHIBITION.—Except as provided in sub-
12 section (c), it shall be unlawful for any person to—

13 “(1) sell or purchase a social security account
14 number or display to the general public a social se-
15 curity account number or any derivative thereof; or

16 “(2) obtain or use any individual’s social secu-
17 rity account number for the purpose of locating or
18 identifying such individual with the intent to phys-
19 ically injure or harm such individual or using the
20 identity of such individual for any illegal purpose.

21 “(c) EXCEPTIONS.—

22 “(1) IN GENERAL.—Notwithstanding subsection
23 (b), a social security account number may be sold,
24 purchased, or displayed to the general public by any

1 person to the extent provided in this subsection (and
2 for no other purpose) as follows:

3 “(A) To the extent necessary for law en-
4 forcement, including the enforcement of a child
5 support obligation, as determined under regula-
6 tions of the Attorney General issued under sec-
7 tion 205(c)(2)(I).

8 “(B) To the extent necessary for national
9 security purposes, as determined under regula-
10 tions of the Attorney General issued under sec-
11 tion 205(c)(2)(I).

12 “(C) To the extent necessary for public
13 health purposes.

14 “(D) To the extent necessary in emergency
15 situations to protect the health or safety of 1
16 or more individuals.

17 “(E) To the extent necessary for research
18 conducted for the purpose of advancing public
19 knowledge, on the condition that the researcher
20 provides adequate assurances that—

21 “(i) the social security account num-
22 bers will not be used to harass, target, or
23 publicly reveal information concerning any
24 identifiable individuals;

1 “(ii) information about identifiable in-
2 dividuals obtained from the research will
3 not be used to make decisions that directly
4 affect the rights, benefits, or privileges of
5 specific individuals; and

6 “(iii) the researcher has in place ap-
7 propriate safeguards to protect the privacy
8 and confidentiality of any information
9 about identifiable individuals.

10 “(F) To the extent consistent with an indi-
11 vidual’s voluntary and affirmative written con-
12 sent to the sale, purchase, or display to the gen-
13 eral public of a social security account number
14 that has been assigned to that individual.

15 “(G) Under such other circumstances as
16 the Attorney General may determine appro-
17 priate in regulations issued under section
18 205(c)(2)(I).

19 “(H) To the extent necessary for use by an
20 established fraud prevention unit that shall use
21 such number only for fraud prevention purposes
22 and each individual member of such unit shall
23 have passed a reasonably effective background
24 check.

1 “(2) DECEASED INDIVIDUALS.—This section
2 does not apply with respect to the social security ac-
3 count number of a deceased individual.

4 “(d) PENALTIES AND ACTIONS FOR VIOLATIONS.—

5 “(1) PENALTY.—Any person that violates this
6 section shall be subject to a civil penalty of not more
7 than \$1,000 per individual social security number
8 per violation.

9 “(2) ACTIONS.—An action to enforce a violation
10 of this section may be brought by the Federal Trade
11 Commission or the appropriate State attorney gen-
12 eral in any appropriate United States district court
13 or any other court of competent jurisdiction.”.

14 “(2) EFFECTIVE DATE.—The amendment made
15 by this subsection shall apply with respect to viola-
16 tions occurring on or after the date that is 1 year
17 after the date of the issuance by the Attorney Gen-
18 eral of the United States of final regulations under
19 section 205(c)(2)(I) of the Social Security Act (as
20 added by subsection (e)(1)).

21 “(e) REGULATORY AUTHORITY OF THE ATTORNEY
22 GENERAL.—

23 “(1) IN GENERAL.—Section 205(c)(2) of the So-
24 cial Security Act (42 U.S.C. 405(c)(2)) is amended

1 by adding at the end the following new subpara-
2 graph:

3 “(I)(i) Regulations issued by the Attorney General
4 pursuant to subparagraphs (A) and (B) of section
5 208A(c)(1) shall be issued in accordance with section 553
6 of title 5, United States Code. In issuing such regulations,
7 the Attorney General shall consult with the Commissioner
8 of Social Security, the Secretary of Homeland Security,
9 the Federal Trade Commission, State attorneys general,
10 and such other governmental agencies and instrumental-
11 ities as the Attorney General considers appropriate.

12 “(ii) In issuing the regulations described in clause (i)
13 pursuant to the provisions of subparagraphs (A) and (B)
14 of section 208A(c)(1) (relating to law enforcement and na-
15 tional security), the Attorney General may authorize the
16 sale, purchase, or display to the general public of social
17 security account numbers only if the Attorney General de-
18 termines that—

19 “(I) such sale, purchase, or display would serve
20 a compelling public interest that cannot reasonably
21 be served through alternative measures, and

22 “(II) such sale, purchase, or display will not
23 pose an undue risk of bodily, emotional, or financial
24 harm to an individual (taking into account any re-
25 strictions and conditions that the Attorney General

1 imposes on the sale, purchase, or disclosure to the
2 general public of social security account numbers).

3 “(iii) If the Attorney General authorizes the sale,
4 purchase, or display to the general public of social security
5 account numbers, in regulations issued pursuant to sub-
6 paragraph (C), (D), (E), (F), (G), or (H) of section
7 208A(c)(1), the Attorney General shall impose restrictions
8 and conditions on the sale, purchase, or display to the gen-
9 eral public to the extent necessary—

10 “(I) to provide reasonable assurances that so-
11 cial security account numbers will not be used to
12 commit or facilitate fraud, deception, or crime, and

13 “(II) to prevent an undue risk of bodily, emo-
14 tional, or financial harm to an individual.

15 “(iv) For purposes of clause (iii), the Attorney Gen-
16 eral shall consider, among other relevant factors—

17 “(I) the cost or burden to the general public,
18 businesses, commercial enterprises, nonprofit organi-
19 zations, and to Federal, State, and local govern-
20 ments of complying with the restrictions and condi-
21 tions imposed by the Attorney General;

22 “(II) the benefit to the general public, busi-
23 nesses, commercial enterprises, nonprofit associa-
24 tions, and to Federal, State, and local governments

1 derived from the imposition of such restrictions and
2 conditions; and

3 “(III) in connection with subclause (II) of
4 clause (iii), the nature, likelihood, and severity of the
5 anticipated harm described in such subclause that
6 could result from the sale, purchase, or display to
7 the general public of social security account num-
8 bers, together with the nature, likelihood, and extent
9 of any benefits that could be realized therefrom.

10 “(v) For purposes of this subparagraph, the terms
11 ‘sell’, ‘purchase’, and ‘display to the general public’ shall
12 have the meanings provided such terms under section
13 208A(a).

14 “(vi) For purposes of this subparagraph, the term
15 ‘social security account number’ includes any derivative of
16 such number.”.

17 (2) REGULATIONS.—The Attorney General shall
18 promulgate regulations required under this sub-
19 section not later than 1 year after the date of enact-
20 ment of this Act.

21 **SEC. 10. INFORMATION SHARING REQUIREMENTS.**

22 (a) DISCLOSURE BOX.—A covered person that re-
23 quests on an online or offline form sensitive personal infor-
24 mation from a customer and intends to sell or transfer
25 such sensitive personal information for anything of value

1 to an unaffiliated third party at any point, shall provide
2 a notification to the customer in accordance with sub-
3 section (b).

4 (b) NOTIFICATION.—

5 (1) IN GENERAL.—The notification required
6 under subsection (a) shall include in a clear and con-
7 spicuous box on the form the following: “This infor-
8 mation be may sold or transferred to an unaffiliated
9 third party without your additional consent.” (re-
10 ferred to in this subsection as a “Disclosure Box”).

11 (2) TYPEFACE AND LOCATION.—The text in the
12 Disclosure Box shall appear in not less than 12-
13 point typeface directly above either the final signa-
14 ture block on a written document or the final online
15 submission button on an online form on which the
16 customer would agree to submit sensitive personal
17 information to the covered person.

18 **SEC. 11. IMPROVING CYBERSECURITY.**

19 (a) SHORT TITLE.—This section may be cited as the
20 “Department of Homeland Security Cybersecurity En-
21 hancement Act of 2005”.

22 (b) ASSISTANT SECRETARY FOR CYBERSECURITY.—

23 (1) IN GENERAL.—Subtitle A of title II of the
24 Homeland Security Act of 2002 (6 U.S.C. 121 et
25 seq.) is amended by adding at the end the following:

1 **“SEC. 203. ASSISTANCE SECRETARY FOR CYBERSECURITY.**

2 “(a) NATIONAL CYBERSECURITY OFFICE.—There
3 shall be in the Directorate for Information Analysis and
4 Infrastructure Protection a National Cybersecurity Office
5 headed by an Assistant Secretary for Cybersecurity (in
6 this section referred to as the ‘Assistant Secretary’), who
7 shall assist the Secretary in promoting cybersecurity for
8 the United States.

9 “(b) GENERAL AUTHORITY.—The Assistant Sec-
10 retary, subject to the direction and control of the Sec-
11 retary, shall have primary authority within the Depart-
12 ment for all cybersecurity-related critical infrastructure
13 protection programs of the Department, including with re-
14 spect to policy formulation and program management.

15 “(c) RESPONSIBILITIES.—The responsibilities of the
16 Assistant Secretary shall include the following:

17 “(1) To establish and manage—

18 “(A) a national cybersecurity response sys-
19 tem that includes the ability to—

20 “(i) analyze the effect of cybersecurity
21 threat information on national critical in-
22 frastructure; and

23 “(ii) aid in the detection and warning
24 of attacks on, and in the restoration of,
25 cybersecurity infrastructure in the after-
26 math of such attacks;

1 “(B) a national cybersecurity threat and
2 vulnerability reduction program that identifies
3 cybersecurity vulnerabilities that would have a
4 national effect on critical infrastructure, per-
5 forms vulnerability assessments on information
6 technologies, and coordinates the mitigation of
7 such vulnerabilities;

8 “(C) a national cybersecurity awareness
9 and training program that promotes
10 cybersecurity awareness among the public and
11 the private sectors and promotes cybersecurity
12 training and education programs;

13 “(D) a government cybersecurity program
14 to coordinate and consult with Federal, State,
15 and local governments to enhance their
16 cybersecurity programs; and

17 “(E) a national security and international
18 cybersecurity cooperation program to help fos-
19 ter Federal efforts to enhance international
20 cybersecurity awareness and cooperation.

21 “(2) To coordinate with the private sector on
22 the program under paragraph (1) as appropriate,
23 and to promote cybersecurity information sharing,
24 vulnerability assessment, and threat warning regard-
25 ing critical infrastructure.

1 “(3) To coordinate with other directorates and
2 offices within the Department on the cybersecurity
3 aspects of their missions.

4 “(4) To coordinate with the Under Secretary
5 for Emergency Preparedness and Response to en-
6 sure that the National Response Plan developed pur-
7 suant to section 502(6) includes appropriate meas-
8 ures for the recovery of the cybersecurity elements
9 of critical infrastructure.

10 “(5) To develop processes for information shar-
11 ing with the private sector, consistent with section
12 214, that—

13 “(A) promote voluntary cybersecurity best
14 practices, standards, and benchmarks that are
15 responsive to rapid technology changes and to
16 the security needs of critical infrastructure; and

17 “(B) consider roles of Federal, State, local,
18 and foreign governments and the private sector,
19 including the insurance industry and auditors.

20 “(6) To coordinate with the Chief Information
21 Officer of the Department in establishing a secure
22 information sharing architecture and information
23 sharing processes, including with respect to the De-
24 partment’s operation centers.

1 “(7) To consult with the Electronic Crimes
2 Task Force of the United States Secret Service on
3 private sector outreach and information activities.

4 “(8) To consult with the Office for Domestic
5 Preparedness to ensure that realistic cybersecurity
6 scenarios are incorporated into tabletop and recovery
7 exercises.

8 “(9) To consult and coordinate, as appropriate,
9 with other Federal agencies on cybersecurity-related
10 programs, policies, and operations.

11 “(10) To consult and coordinate within the De-
12 partment and, where appropriate, with other rel-
13 evant Federal agencies, on security of digital control
14 systems, such as Supervisory Control and Data Ac-
15 quisition (SCADA) systems.

16 “(d) AUTHORITY OVER THE NATIONAL COMMUNICA-
17 TIONS SYSTEM.—The Assistant Secretary shall have pri-
18 mary authority within the Department over the National
19 Communications System.”.

20 (2) CLERICAL AMENDMENT.—The table of con-
21 tents in section 1(b) of the Homeland Security Act
22 of 2002 (6 U.S.C. 101 note) is amended by adding
23 at the end of the items relating to subtitle A of title
24 II the following:

“Sec. 203. Assistance secretary for cybersecurity.”.

1 (c) CYBERSECURITY DEFINED.—Section 2 of the
2 Homeland Security Act of 2002 (6 U.S.C. 101) is amend-
3 ed by adding at the end the following:

4 “(17) CYBERSECURITY.—

5 “(A) IN GENERAL.—The term
6 ‘cybersecurity’ means the prevention of damage
7 to, the protection of, and the restoration of
8 computers, electronic communications systems,
9 electronic communication services, wire commu-
10 nication, and electronic communication, includ-
11 ing information contained therein, to ensure its
12 availability, integrity, authentication, confiden-
13 tiality, and nonrepudiation.

14 “(B) OTHER TERMS.—In this paragraph—

15 “(i) each of the terms ‘damage’ and
16 ‘computer’ have the meanings given such
17 terms in section 1030 of title 18, United
18 States Code; and

19 “(ii) each of the terms ‘electronic
20 communications system’, ‘electronic com-
21 munication service’, ‘wire communication’,
22 and ‘electronic communication’ have the
23 meanings given such terms in section 2510
24 of title 18, United States Code.”.

1 **SEC. 12. PROHIBITION OF POSTING ACCOUNT NUMBERS**
2 **AND INDIVIDUALS' NAMES.**

3 A covered person shall not post in a document that
4 is publically accessible online an individual financial ac-
5 count number of an individual in combination with such
6 individual's name.

7 **SEC. 13. ONLINE INFORMATION SECURITY WORKING**
8 **GROUP.**

9 (a) **ONLINE INFORMATION SECURITY WORKING**
10 **GROUP.**—The Chairman of the Federal Trade Commis-
11 sion shall establish an Online Information Security Work-
12 ing Group (referred to in this section as the “Working
13 Group”) to develop best practices to protect sensitive per-
14 sonal information stored and transferred online. The
15 Working Group shall be composed of industry partici-
16 pants, consumer groups, and other interested parties.

17 (b) **REPORT.**—Not later than 12 months after the
18 date on which the Working Group is established under
19 subsection (a), the Working Group shall submit to Con-
20 gress a report on their findings.

21 **SEC. 14. STUDY TO EXAMINE THE USE OF SOCIAL SECURITY**
22 **NUMBERS BY THE GOVERNMENT.**

23 (a) **IN GENERAL.**—Not later than 9 months after the
24 date of enactment of this Act, the Chairman of the Fed-
25 eral Trade Commission shall submit to Congress a report
26 that contains the results of the study conducted under

1 subsection (b) concerning the use and publication of social
2 security numbers by Federal, State, and local governments
3 and recommendations for the modification by Federal,
4 State, and local governments of their policies for the use
5 of social security numbers in such a way that would pre-
6 vent or reduce identity theft.

7 (b) STUDY.—The Chairman of the Federal Trade
8 Commission shall conduct a study to examine—

9 (1) where and when Federal, State, and local
10 governments publish social security numbers;

11 (2) the reasons that social security numbers are
12 published by Federal, State, and local governments;

13 (3) the individuals and entities that have access
14 to such social security numbers; and

15 (4) the risk for identity theft as a result of the
16 current policies on the publication of such social se-
17 curity numbers.

18 (c) RECOMMENDATIONS.—The recommendation con-
19 tained in the report under subsection (a) shall be provided
20 to all relevant State and local governments.

21 **SEC. 15. ANNUAL IDENTITY THEFT REPORT.**

22 (a) IN GENERAL.—Not later than 1 year after the
23 date of enactment of this Act, and annually thereafter,
24 the Director of the Office of Identity Theft of the Federal

1 Trade Commission shall submit to Congress a report on
2 identity theft.

3 (b) CONTENTS OF REPORT.—The report submitted
4 under subsection (a) shall include—

5 (1) a description of the current trends in iden-
6 tity theft for residents of the United States;

7 (2) the total number of identity-theft enforce-
8 ment actions opened or continued by the Federal
9 Trade Commission in the year for which the report
10 is prepared;

11 (3) a description of the current status and dis-
12 position of the enforcement actions described in
13 paragraph (2);

14 (4) a description of the procedures utilized by
15 the Office of Identity Theft to assist victims of iden-
16 tity theft in re-establishing their identity;

17 (5) with respect to the year for which the report
18 is prepared, data concerning—

19 (A) the number of certifications of identity
20 theft applied for under section 4;

21 (B) the number of such certifications
22 issued; and

23 (C) the common trends with respect to
24 such certification approvals and disapprovals;

25 and

1 (6) a description of the products and services
2 used by identity theft victims to help such victims
3 reestablish their identities.

4 (c) PROVISION OF REPORT.—The report submitted
5 under subsection (a) shall be provided to—

6 (1) the Committee on Banking, Housing, and
7 Urban Affairs of the Senate;

8 (2) the Committee on the Judiciary of the Sen-
9 ate;

10 (3) the Committee on Commerce, Science, and
11 Transportation of the Senate;

12 (4) the Committee on Finance of the Senate;

13 (5) the Committee on Financial Services of the
14 House of Representatives;

15 (6) the Committee on the Judiciary of the
16 House of Representatives;

17 (7) the Committee on Energy and Commerce of
18 the House of Representatives; and

19 (8) the Committee on Ways and Means of the
20 House of Representatives.

21 (d) INTERNATIONAL REPORT.—Not later than 1 year
22 after the date of enactment of this Act, and annually
23 thereafter, the international directorate of the Office of
24 Identity Theft shall submit a report detailing emerging
25 issues in international identity theft, including what action

1 and initiatives have been taken to fight identity theft on
2 a global level. The report shall also spotlight the most suc-
3 cessful steps other countries are taking to fight identity
4 theft and shall rank the top few countries that have the
5 worst record regarding identity theft against victims in the
6 United States.

7 **SEC. 16. PREEMPTION OF STATE LAW.**

8 This Act shall not be construed as superseding, alter-
9 ing, or affecting any statute, regulation, order, or interpre-
10 tation in effect in any State, except to the extent that such
11 statute, regulation, order, or interpretation is inconsistent
12 with the provisions of this Act, and then only to the extent
13 of the inconsistency. A State statute, regulation, order, or
14 interpretation is not inconsistent with the provisions of
15 this Act if the protection such statute, regulation, order,
16 or interpretation affords any resident of the United States
17 is greater than the protection provided under this Act.

18 **SEC. 17. NONINTERFERENCE WITH THE FAIR CREDIT RE-**
19 **PORTING ACT.**

20 Nothing in this Act shall be construed to affect, alter,
21 or supersede the applicability of the Fair Credit Reporting
22 Act (15 U.S.C. 1601 et seq.) with respect to transactions
23 covered under the Fair Credit Reporting Act.