

SOCIAL SECURITY NUMBER PRIVACY AND IDENTITY
THEFT PREVENTION ACT OF 2007

SEPTEMBER 24, 2007.—Committed to the Committee of the Whole House on the
State of the Union and ordered to be printed

Mr. RANGEL, from the Committee on Ways and Means,
submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 3046]

[Including cost estimate of the Congressional Budget Office]

The Committee on Ways and Means, to whom was referred the bill (H.R. 3046) to amend the Social Security Act to enhance Social Security account number privacy protections, to prevent fraudulent misuse of the Social Security account number, and to otherwise enhance protection against identity theft, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
I. Introduction	15
A. Purpose and Summary	15
B. Background	16
C. Legislative History	16
II. Section-by-Section Summary	19
III. Votes of the Committee	42
A. Motion to Report the Bill	42
B. Votes on Amendments	42
IV. Budget Effects of the Bill	43
A. Committee Estimate of Budgetary Effects	43
B. Statement Regarding New Budget Authority and Tax Expenditures	43
C. Cost Estimate Prepared by the Congressional Budget Office	43
V. Other Matters to be Discussed under the Rules of the House	50
A. Committee Oversight Findings and Recommendations	50
B. Earmarks and Tax and Tariff Benefits	50
C. Constitutional Authority Statement	50
D. Information Relating to Unfunded Mandates	50

VI. Changes in Existing Law Made by the Bill, as Reported	50
VII. Additional Views	70

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Social Security Number Privacy and Identity Theft Prevention Act of 2007”.

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

- Sec. 1. Short title and table of contents.
- Sec. 2. Restrictions on the sale or display to the general public of social security account numbers by governmental entities.
- Sec. 3. Prohibition of display of social security account numbers on checks issued for payment by governmental entities.
- Sec. 4. Prohibition of the display of social security account numbers on certain government identification cards or tags.
- Sec. 5. Prohibition of inmate access to social security account numbers.
- Sec. 6. Measures to preclude unauthorized disclosure by governmental entities of social security account numbers and protect the confidentiality of such numbers.
- Sec. 7. Uniform standards for truncation of the social security account number.
- Sec. 8. Prohibition of the sale, purchase, and display to the general public of the social security account number in the private sector.
- Sec. 9. New criminal penalties for misuse of social security account numbers.
- Sec. 10. Extension of civil monetary penalty authority.
- Sec. 11. Criminal penalties for employees of the Social Security Administration who knowingly and fraudulently issue social security cards or social security account numbers.
- Sec. 12. Enhanced penalties in cases of terrorism, drug trafficking, crimes of violence, or prior offenses.
- Sec. 13. Regulatory and enforcement authority with respect to misuse of the social security account number.
- Sec. 14. Study on feasibility of banning social security account number as an authenticator.

SEC. 2. RESTRICTIONS ON THE SALE OR DISPLAY TO THE GENERAL PUBLIC OF SOCIAL SECURITY ACCOUNT NUMBERS BY GOVERNMENTAL ENTITIES.

(a) **IN GENERAL.**—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) is amended by adding at the end the following new clause:

“(x)(I) A governmental entity (as defined in subclause (X)) may not sell or display to the general public any social security account number if such number has been disclosed to such governmental entity pursuant to the assertion by such governmental entity to any person that disclosure of such number is a statutory or regulatory requirement. Notwithstanding the preceding sentence, such number may be sold or displayed to the general public in accordance with the exceptions specified in subclauses (II), (III), (IV), (V), (VI), (VII), and (VIII) (and for no other purpose).

“(II) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that such sale is specifically authorized by this Act or the Privacy Act of 1974.

“(III) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that is necessary or appropriate for law enforcement or national security purposes, as determined under regulations which shall be issued as provided in section 1129C.

“(IV) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that such sale is required to comply with a tax law of the United States or of any State (or political subdivision thereof).

“(V) Notwithstanding subclause (I), a social security account number may be sold by a State department of motor vehicles as authorized under subsection (b) of section 2721 of title 18, United States Code, if such number is to be used pursuant to such sale solely for purposes permitted under paragraph (1), (6), or (9) of such subsection.

“(VI) Notwithstanding subclause (I), a social security account number may be sold or otherwise made available by a governmental entity to a consumer reporting agency (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))) for use or disclosure solely for permissible purposes described in section 604(a) of such Act (15 U.S.C. 1681b(a)).

“(VII) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent necessary for research (other than market research) conducted by any governmental entity for the purpose of advancing the public good, on the condition that the researcher provides adequate assurances that the social security account numbers will not be used to harass, target, or publicly reveal information concerning any identifiable individuals, that information about identifiable individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals, and that the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about identifiable individuals, including procedures to ensure that the social security account numbers will be encrypted or otherwise appropriately secured from unauthorized disclosure. In the case of medical

research, the Commissioner of Social Security shall maintain ongoing consultation with the Office for Civil Rights of the Department of Health and Human Services to ensure that the sale or purchase of social security account numbers which constitute personally identifiable medical information is permitted only in compliance with existing Federal rules and regulations prescribed by the Secretary of Health and Human Services pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (110 Stat. 2033).

“(VIII) Notwithstanding subclause (I), a social security account number may be sold or displayed to the general public by a governmental entity under such other circumstances as may be specified in regulations issued as provided in section 1129C.

“(IX) This clause does not apply with respect to a social security account number of a deceased individual.

“(X) For purposes of this clause, the term ‘governmental entity’ means an executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof, a Federally recognized Indian tribe, or a trustee appointed in a case under title 11, United States Code. Such term includes a person acting as an agent of such an agency or instrumentality, Indian tribe, or trustee. For purposes of this subclause, the term ‘State’ has the meaning provided in subparagraph (D)(iii)(II).

“(XI) For purposes of this clause, the term ‘sell’ means, in connection with a social security account, to obtain, directly or indirectly, anything of value in exchange for such number. Such term does not include the submission of such number as part of the process for applying for any type of Government benefits or programs (such as grants, loans, or welfare or other public assistance programs) or as part of the administration of, or provision of benefits under, an employee benefit plan.

“(XII) For purposes of this clause, the term ‘display to the general public’ shall have the meaning provided such term in section 208A(a)(3)(A). In any case in which a governmental entity requires transmittal to such governmental entity of an individual’s social security account number by means of the Internet without ensuring that such number is encrypted or otherwise appropriately secured from disclosure, any such transmittal of such number as so required shall be treated, for purposes of this clause, as a ‘display to the general public’ of such number by such governmental entity for purposes of this clause.

“(XIII) For purposes of this clause, the term ‘social security account number’ includes any derivative of such number. Notwithstanding the preceding sentence, any expression, contained in or on any item sold or displayed to the general public, shall not be treated as a social security account number solely because such expression sets forth not more than the last 4 digits of such number, if the remainder of such number cannot be determined based solely on such expression or any other matter presented in or on such item.

“(XIV) Nothing in the preceding subclauses of this clause shall be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect under any other Federal or State law, except to the extent that such statute, regulation, order, or interpretation is inconsistent with such subclauses, and then only to the extent of the inconsistency. For purposes of this subclause, a statute, regulation, order, or interpretation is not inconsistent with the preceding subclauses of this clause if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under such subclauses.”.

(b) EFFECTIVE DATE AND RELATED RULES.—

(1) IN GENERAL.—Initial final regulations prescribed to carry out the provisions of section 205(c)(2)(C)(x) of the Social Security Act (added by this section) shall be issued not later than the last date of the 18th calendar month following the date of the enactment of this Act. Such provisions shall take effect, with respect to matters governed by such regulations issued by the Commissioner of Social Security or any other agency or instrumentality of the United States, 1 year after the date of the issuance of such regulations by the Commissioner or such other agency or instrumentality, respectively. Such provisions shall apply in the case of displays to the general public, as defined in section 208A(a)(3) of such Act (added by section 8 of this Act), to such displays originally occurring after such 1-year period. Such provisions shall not apply with respect to any display of a record (containing a social security account number (or any derivative thereof) generated prior to the close of such 1-year period.

(2) SUNSET OF EXCEPTION.—The last sentence of subclause (XIII) of section 205(c)(2)(C)(x) of the Social Security Act (added by this section) shall cease to be effective with respect to sales or displays to the general public occurring after 2 years after the effective date of the initial final regulations prescribed to carry out the provisions of such section 205(c)(2)(C)(x).

SEC. 3. PROHIBITION OF DISPLAY OF SOCIAL SECURITY ACCOUNT NUMBERS ON CHECKS ISSUED FOR PAYMENT BY GOVERNMENTAL ENTITIES.

(a) **IN GENERAL.**—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by section 2 of this Act) is amended further by adding at the end the following new clause:

“(xi) No governmental entity (as defined in clause (x)(X)) may include the social security account number of any individual (or any derivative of such number) on any check issued for any payment by such governmental entity or on any document attached to or accompanying such a check.”.

(b) **EFFECTIVE DATE.**—The amendment made by this section shall apply with respect to checks (and documents attached to or accompanying such checks) issued after 1 year after the date of the enactment of this Act.

SEC. 4. PROHIBITION OF THE DISPLAY OF SOCIAL SECURITY ACCOUNT NUMBERS ON CERTAIN GOVERNMENT IDENTIFICATION CARDS OR TAGS.

(a) **IN GENERAL.**—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by the preceding provisions of this Act) is amended further by adding at the end the following new clause:

“(xii) No governmental entity (as defined in clause (x)(X)), and no other person offering benefits in connection with an employee benefit plan maintained by such governmental entity, may display a social security account number (or any derivative thereof) on any card or tag that is commonly provided—

“(I) to employees of such governmental entity,

“(II) in the case of a governmental entity which is an educational institution, to its students, or

“(III) in the case of a governmental entity which is a medical institution, to its patients,

(or to their family members) for purposes of identification or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number (or derivative thereof). The requirements of this clause shall also apply to the Medicare card issued by the Department of Health and Human Services.”.

(b) **EFFECTIVE DATE.**—The amendment made by this section shall apply with respect to cards or tags issued after 1 year after the date of the enactment of this Act, except that the last sentence of section 205(c)(2)(C)(xii) (as added by this section) shall take effect 2 and one-half years after the date of the enactment of this Act.

SEC. 5. PROHIBITION OF INMATE ACCESS TO SOCIAL SECURITY ACCOUNT NUMBERS.

(a) **IN GENERAL.**—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by the preceding provisions of this Act) is amended further by adding at the end the following new clause:

“(xiii) No governmental entity (as defined in clause (x)(X)) may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals (or any derivatives of such numbers). For purposes of this clause, the term ‘prisoner’ means an individual confined in a jail, prison, or other penal institution or correctional facility.”.

(b) **EFFECTIVE DATE.**—

(1) **IN GENERAL.**—Except as provided in paragraph (2), the amendment made by this section shall apply with respect to employment of prisoners, or entry into contract for the use or employment of prisoners, on or after the date of the enactment of this Act.

(2) **TREATMENT OF CURRENT ARRANGEMENTS.**—In the case of—

(A) prisoners employed as described in clause (xiii) of section 205(c)(2)(C) of the Social Security Act (as added by this section) on the date of the enactment of this Act, and

(B) contracts described in such clause in effect on such date, the amendment made by this section shall take effect 90 days after the date of the enactment of this Act.

SEC. 6. MEASURES TO PRECLUDE UNAUTHORIZED DISCLOSURE BY GOVERNMENTAL ENTITIES OF SOCIAL SECURITY ACCOUNT NUMBERS AND PROTECT THE CONFIDENTIALITY OF SUCH NUMBERS.

(a) **IN GENERAL.**—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by the preceding provisions of this Act) is amended further by adding at the end the following new clause:

“(xiv) Except as otherwise provided in this paragraph, in the case of any governmental entity (as defined in clause (x)(X)) having access to an individual’s social security account number—

“(I) no officer or employee thereof shall have access to such number for any purpose other than the effective administration of the statutory provisions governing its functions,

“(II) such governmental entity shall restrict, to the satisfaction of the Commissioner of Social Security, access to social security account numbers obtained thereby to officers and employees thereof whose duties or responsibilities require access for the administration or enforcement of such provisions, and

“(III) such governmental entity shall provide such other safeguards as the Commissioner determines to be necessary or appropriate to preclude unauthorized access to the social security account number and to otherwise protect the confidentiality of such number.

For purposes of this clause the term ‘social security account number’ includes any derivative thereof.”

(b) EFFECTIVE DATE.—The amendment made by this section shall take effect 1 year after the date of the enactment of this Act.

SEC. 7. UNIFORM STANDARDS FOR TRUNCATION OF THE SOCIAL SECURITY ACCOUNT NUMBER.

(a) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by the preceding provisions of this Act) is amended further by adding at the end the following new clause:

“(xv) The truncation by any governmental entity (as defined in clause (x)(X)) or by any person in the private sector of an individual’s social security account number which is used by such governmental entity or person otherwise in accordance with the requirements of this Act shall be in accordance with a uniform truncation standard which shall be specified in regulations prescribed by the Commissioner of Social Security. Under such standard, the number as truncated shall set forth not more than the last 4 digits of the number. Nothing in this clause shall be construed to authorize any use of the social security account number which is not otherwise authorized by this title or regulations prescribed thereunder.”

(b) EFFECTIVE DATE.—Initial final regulations prescribed to carry out the provisions of section 205(c)(2)(C)(xv) of the Social Security Act (added by this section) shall be issued not later than the last date of the 18th calendar month following the date of the enactment of this Act. Such provisions shall take effect, with respect to matters governed by such regulations issued by the Commissioner or any other agency or instrumentality of the United States, 1 year after the date of the issuance of such regulations by the Commissioner or such other agency or instrumentality, respectively.

SEC. 8. PROHIBITION OF THE SALE, PURCHASE, AND DISPLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PRIVATE SECTOR.

(a) IN GENERAL.—Title II of the Social Security Act is amended by inserting after section 208 (42 U.S.C. 408) the following new section:

“PROHIBITION OF THE SALE, PURCHASE, AND DISPLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PRIVATE SECTOR

“SEC. 208A. (a) DEFINITIONS.—For purposes of this section:

“(1) PERSON.—

“(A) IN GENERAL.—Subject to subparagraph (B), the term ‘person’ means any individual, partnership, corporation, trust, estate, cooperative, association, or any other entity.

“(B) EXCLUSION OF GOVERNMENTAL ENTITIES.—Such term does not include a governmental entity. Nothing in this subparagraph shall be construed to authorize, in connection with a governmental entity, an act or practice otherwise prohibited under this section or section 205(c)(2)(C).

“(2) SELLING AND PURCHASING.—

“(A) IN GENERAL.—Subject to subparagraph (B)—

“(i) SELL.—The term ‘sell’ in connection with a social security account number means to obtain, directly or indirectly, anything of value in exchange for such number.

“(ii) PURCHASE.—The term ‘purchase’ in connection with a social security account number means to provide, directly or indirectly, anything of value in exchange for such number.

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

“(i) the process for applying for any type of Government benefits or programs (such as grants or loans or welfare or other public assistance programs),

- “(ii) the administration of, or provision of benefits under, an employee benefit plan, or
 - “(iii) the sale, lease, merger, transfer, or exchange of a trade or business.
- “(3) DISPLAY TO THE GENERAL PUBLIC.—
- “(A) IN GENERAL.—The term ‘display to the general public’ means, in connection with a social security account number, to intentionally place such number in a viewable manner on an Internet site that is available to the general public or to make such number available in any other manner intended to provide access to such number by the general public.
 - “(B) INTERNET TRANSMISSIONS.—In any case in which a person requires transmittal to such person of an individual’s social security account number by means of the Internet without ensuring that such number is encrypted or otherwise well-secured from disclosure, any such transmittal of such number as so required shall be treated as a ‘display to the general public’ of such number by such person.
- “(4) SOCIAL SECURITY ACCOUNT NUMBER.—
- “(A) IN GENERAL.—The term ‘social security account number’ has the meaning given such term in section 208(e), except that such term includes any derivative of such number.
 - “(B) 4-DIGIT EXPRESSION.—Notwithstanding the preceding sentence, for purposes of subsection (b)(1)(A), any expression, contained in or on any item sold or displayed to the general public, shall not be treated as a social security account number solely because such expression sets forth not more than the last 4 digits of such number, if the remainder of such number cannot be determined based solely on such expression or any other matter presented in or on such item.
- “(5) GOVERNMENTAL ENTITY.—
- “(A) IN GENERAL.—The term ‘governmental entity’ means an executive, legislative, or judicial agency or instrumentality of the Federal Government, a State or political subdivision thereof, a Federally recognized Indian tribe, or a trustee appointed in a case under title 11, United States Code. Such term includes a person acting as an agent of such an agency or instrumentality, Indian tribe, or trustee.
 - “(B) STATE.—The term ‘State’ includes the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, the Commonwealth of the Northern Marianas, and the Trust Territory of the Pacific Islands.
- “(b) PROHIBITION OF SALE, PURCHASE, AND DISPLAY TO THE GENERAL PUBLIC.—
- “(1) IN GENERAL.—Except as provided in paragraph (2), it shall be unlawful for any person to—
 - “(A) sell or purchase a social security account number or display to the general public a social security account number, or
 - “(B) obtain or use any individual’s social security account number for the purpose of locating or identifying such individual with the intent to harass, harm, or physically injure such individual or using the identity of such individual for any illegal purpose.
 - “(2) EXCEPTIONS.—
 - “(A) IN GENERAL.—Notwithstanding paragraph (1), and subject to paragraph (3), a social security account number may be sold or purchased by any person to the extent provided in this subsection (and for no other purpose) as follows:
 - “(i) to the extent necessary for law enforcement, including (but not limited to) the enforcement of a child support obligation, as determined under regulations issued as provided in section 1129C;
 - “(ii) to the extent necessary for national security purposes, as determined under regulations issued as provided in section 1129C;
 - “(iii) to the extent necessary for public health purposes;
 - “(iv) to the extent necessary in emergency situations to protect the health or safety of 1 or more individuals;
 - “(v) to the extent that the sale or purchase is required to comply with a tax law of the United States or of any State (or political subdivision thereof);
 - “(vi) to the extent that the sale or purchase is to or by a consumer reporting agency (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))) for use or disclosure solely for permissible purposes described in section 604(a) of such Act (15 U.S.C. 1681b(a)); and
 - “(vii) to the extent necessary for research (other than market research) conducted by an agency or instrumentality of the United States

or of a State or political subdivision thereof (or a person acting as an agent of such an agency or instrumentality) for the purpose of advancing the public good, on the condition that the researcher provides adequate assurances that—

“(I) the social security account numbers will not be used to harass, target, or publicly reveal information concerning any identifiable individuals;

“(II) information about identifiable individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals; and

“(III) the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about identifiable individuals, including procedures to ensure that the social security account numbers will be encrypted or otherwise appropriately secured from unauthorized disclosure.

“(B) MEDICAL RESEARCH.—In the case of research referred to in subparagraph (A)(vii) consisting of medical research, the Commissioner of Social Security shall maintain ongoing consultation with the Office for Civil Rights of the Department of Health and Human Services to ensure that the sale or purchase of social security account numbers which constitute personally identifiable medical information is permitted only in compliance with existing Federal rules and regulations prescribed by the Secretary of Health and Human Services pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (110 Stat. 2033).

“(3) CONSENT AND OTHER CIRCUMSTANCES DETERMINED BY REGULATION.—Notwithstanding paragraph (1), a social security account number assigned to an individual may be sold or purchased by any person—

“(A) to the extent consistent with such individual’s voluntary and affirmative written consent to the sale or purchase, but only if—

“(i) the terms of the consent and the right to refuse consent are presented to the individual in a clear, conspicuous, and understandable manner,

“(ii) the individual is placed under no obligation to provide consent to any such sale or purchase, and

“(iii) the terms of the consent authorize the individual to limit the sale or purchase to purposes directly associated with the transaction with respect to which the consent is sought, and

“(B) under such circumstances as may be deemed appropriate in regulations issued as provided under section 1129C.

“(c) PROHIBITION OF DISPLAY ON CHECKS.—It shall be unlawful for any person to include the social security account number of any other individual on any check issued for any payment by such person or on any document attached to or accompanying such a check.

“(d) PROHIBITION OF UNAUTHORIZED DISCLOSURE TO GOVERNMENT AGENCIES OR INSTRUMENTALITIES.—

“(1) IN GENERAL.—It shall be unlawful for any person to communicate by any means to any agency or instrumentality of the United States or of any State or political subdivision thereof the social security account number of any individual other than such person without the written permission of such individual, unless the number was requested by the agency or instrumentality. In the case of an individual who is legally incompetent, permission provided by the individual’s legal representatives shall be deemed to be permission provided by such individual.

“(2) EXCEPTIONS.—Paragraph (1) shall not apply to the extent necessary—

“(A) for law enforcement, including (but not limited to) the enforcement of a child support obligation, or

“(B) for national security purposes,

as determined under regulations issued as provided under section 1129C.

“(e) PROHIBITION OF THE DISPLAYS ON CARDS OR TAGS REQUIRED FOR ACCESS TO GOODS, SERVICES, OR BENEFITS.—No person may display a social security account number on any card or tag issued to any other person for the purpose of providing such other person access to any goods, services, or benefits or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number.

“(f) PROHIBITION OF THE DISPLAYS ON EMPLOYEE IDENTIFICATION CARDS OR TAGS.—No person that is an employer, and no other person offering benefits in connection with an employee benefit plan maintained by such employer or acting as an agent of such employer, may display a social security account number on any card or tag that is commonly provided to employees of such employer (or to their family

members) for purposes of identification or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number.

“(g) MEASURES TO PRECLUDE UNAUTHORIZED DISCLOSURE OF SOCIAL SECURITY ACCOUNT NUMBERS AND PROTECT THE CONFIDENTIALITY OF SUCH NUMBERS.—Subject to the preceding provisions of this section, any person having access to the social security account number of any individual other than such person shall, to the extent that such access is maintained for the conduct of such person’s trade or business—

“(1) ensure that no officer or employee thereof has access to such number for any purpose other than as necessary for the conduct of such person’s trade or business,

“(2) restrict, in accordance with regulations of the Commissioner of Social Security, access to social security account numbers obtained thereby to officers and employees thereof whose duties or responsibilities require access for the conduct of such person’s trade or business, and

“(3) provide such safeguards as may be specified, in regulations of the Commissioner of Social Security, to be necessary or appropriate to preclude unauthorized access to the social security account number and to otherwise protect the confidentiality of such number.

“(h) DECEASED INDIVIDUALS.—This section does not apply with respect to the social security account number of a deceased individual.

“(i) APPLICABILITY OF OTHER PROTECTIONS.—Nothing in the preceding subsections of this section shall be construed as superseding, altering, or affecting any statutory provision, regulation, order, or interpretation in effect under any other Federal or State law, except to the extent that such statutory provision, regulation, order, or interpretation is inconsistent with such subsections, and then only to the extent of the inconsistency. For purposes of this subclause, a statutory provision, regulation, order, or interpretation is not inconsistent with the preceding subsections of this section if the protection such statutory provision, regulation, order, or interpretation affords any person is greater than the protection provided under such subsections.”.

(b) EFFECTIVE DATE AND RELATED RULES.—

(1) IN GENERAL.—Initial final regulations prescribed to carry out the provisions of section 208A of the Social Security Act (added by this section) shall be issued not later than the last date of the 18th calendar month following the date of the enactment of this Act. Such provisions shall take effect, with respect to matters governed by such regulations issued by the Commissioner of Social Security or any other agency or instrumentality of the United States, 1 year after the date of the issuance of such regulations by the Commissioner of Social Security or such other agency or instrumentality, respectively. Section 208A(b) of such Act shall apply in the case of displays to the general public (as defined in section 208A(a)(3) of such Act) to such displays to the general public originally occurring after such 1-year period. Such provisions shall not apply with respect to any such display to the general public of a record (containing a social security account number (or any derivative thereof) generated prior to the close of such 1-year period.

(2) SUNSET OF EXCEPTION.—Section 208A(a)(4)(B) of the Social Security Act (added by this section) shall cease to be effective with respect to sales, purchases, or displays to the general public occurring after 2 years after the effective date of the initial final regulations prescribed to carry out the provisions of section 208A of such Act.

SEC. 9. NEW CRIMINAL PENALTIES FOR MISUSE OF SOCIAL SECURITY ACCOUNT NUMBERS.

(a) IN GENERAL.—Section 208 of the Social Security Act (42 U.S.C. 408) is amended—

(1) in subsection (a), by inserting “or” at the end of paragraph (8) and by inserting after paragraph (8) the following new paragraph:

“(9) willfully acts or fails to act so as to cause a violation of section 208A(b)(1)(B);”.

(2) by redesignating subsections (b) through (e) as subsections (c) through (f), respectively;

(3) in subsection (c)(1) (as so redesignated), by inserting “or (b)” after “subsection (a)”; and

(4) by inserting after subsection (a) the following new subsection:

“(b)(1) Whoever—

“(A) knowingly, and with intent to commit, or to aid or abet, any activity that constitutes a violation of Federal law, or a violation of any applicable law of a State or political subdivision thereof if the maximum penalty of such applicable law includes imprisonment for 5 years or more—

“(i) possesses the social security account number of another person without lawful authority, or

“(ii) possesses a social security card, knowing that the social security account number or other identifying information displayed on the card has been altered, counterfeited, or forged or that the card was falsely made, stolen, or obtained from the Social Security Administration by use of false information;

if such activity is committed, or aided or abetted, with intent to use such social security account number, social security card, or other identifying information displayed on such card in furtherance of such violation;

“(B) being—

“(i) an officer or employee of any governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or

“(ii) a person acting as an agent of a governmental entity (as so defined), willfully acts or fails to act so as to cause a violation of clause (vi)(II), (xi), (xii), or (xv) of section 205(c)(2)(C);

“(C) being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (xi) or (xv) of section 205(c)(2)(C); or

“(D) willfully acts or fails to act so as to cause a violation of subsection (c), (d), (e), or (f) of section 208A or, as a person in the private sector, willfully acts or fails to act so as to cause a violation of section 205(c)(2)(C)(xv);

shall be guilty of a misdemeanor and upon conviction thereof shall be fined under title 18, United States Code, or imprisoned for not more than 1 year, or both.

“(2)(A) Whoever—

“(i) with intent to deceive, discloses, sells, or transfers his own social security account number, assigned to him by the Commissioner of Social Security (in the exercise of the Commissioner’s authority under section 205(c)(2) to establish and maintain records), to any person;

“(ii) without lawful authority, offers, for a fee, to acquire for any individual, or to assist in acquiring for any individual, an additional social security account number or a number that is purported to be a social security account number;

“(iii) being—

“(I) an officer or employee of any governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or

“(II) a person acting as an agent of a governmental entity (as so defined), willfully acts or fails to act so as to cause a violation of clause (x), (xiii), or (xiv) of section 205(c)(2)(C);

“(iv) being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (x) or (xiv) of section 205(c)(2)(C); or

“(v) willfully acts or fails to act so as to cause a violation of subsection (b)(1)(A) or (g) of section 208A;

shall be fined, imprisoned, or both, as provided in subparagraph (B).

“(B) A person convicted of a violation described in subparagraph (A) shall—

“(i) be fined under title 18, United States Code, imprisoned not more than 1 year, or both; and

“(ii) if the offense is committed under false pretenses or for commercial advantage, personal gain, or malicious harm, be fined under title 18, United States Code, imprisoned not more than 5 years, or both.”

(b) EFFECTIVE DATES.—The amendments made by this section shall apply with respect to each violation occurring after the date of the enactment of this Act, except that subparagraphs (B), (C), and (D) of section 208(b)(1) of such Act and clauses (iii), (iv), and (v) of section 208(b)(2)(A) of such Act (added by subsection (a)(3)) shall apply, in connection with violations of clause (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C) or section 208A, with respect to each violation occurring on or after the effective date applicable with respect to such violation under section 2, 3, 4, 5, 6, 7, or 8.

SEC. 10. EXTENSION OF CIVIL MONETARY PENALTY AUTHORITY.

(a) APPLICATION OF CIVIL MONEY PENALTIES TO ELEMENTS OF CRIMINAL VIOLATIONS.—Section 1129(a) of the Social Security Act (42 U.S.C. 1320a–8(a)) is amended—

(1) by redesignating paragraphs (2) and (3) as paragraphs (4) and (5), respectively;

(2) by designating the last sentence of paragraph (1) as a new paragraph (2), appearing after and below paragraph (1); and

(3) by inserting after paragraph (2) (as designated under paragraph (2) of this subsection) the following:

“(3) Any person (including an organization, agency, or other entity) who—

“(A) uses a social security account number that such person knows or should know has been assigned by the Commissioner of Social Security (in an exercise of authority under section 205(c)(2) to establish and maintain records) on the basis of false information furnished to the Commissioner by any person;

“(B) falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to any individual, when such person knows or should know that such number is not the social security account number assigned by the Commissioner to such individual;

“(C) with intent to deceive, alters a social security card that the person knows or should know was issued by the Commissioner of Social Security, or possesses such a card with intent to alter it;

“(D) buys or sells a card that such person knows or should know is, or is purported to be, a card issued by the Commissioner of Social Security, or possesses such a card with intent to buy or sell it;

“(E) counterfeits a social security card, or possesses a counterfeit social security card with intent to buy or sell it;

“(F) discloses, uses, compels the disclosure of, or knowingly sells or purchases the social security account number of any person in violation of the laws of the United States;

“(G) with intent to deceive the Commissioner of Social Security as to such person’s true identity (or the true identity of any other person), furnishes or causes to be furnished false information to the Commissioner with respect to any information required by the Commissioner in connection with the establishment and maintenance of the records provided for in section 205(c)(2);

“(H) without lawful authority, offers, for a fee, to acquire for any individual, or to assist in acquiring for any individual, an additional social security account number or a number which is purported to be a social security account number;

“(I) with intent to deceive, discloses, sells, or transfers his own social security account number, assigned to him by the Commissioner of Social Security under section 205(c)(2)(B), to any person;

“(J) knowingly, and with intent to commit, or to aid or abet, any activity that constitutes a violation of Federal law, or a violation of any applicable law of a State or political subdivision thereof if the maximum penalty of such applicable law includes imprisonment for 5 years or more—

“(i) possesses a social security account number of another individual without lawful authority, or

“(ii) possesses a social security card, knowing that the social security account number or other identifying information displayed on the card has been altered, counterfeited, or forged or that the card was falsely made, stolen, or obtained from the Social Security Administration by use of false information,

if such activity is committed, or aided or abetted, with intent to use such social security account number, social security card, or other identifying information displayed on such card in furtherance of such violation;

“(K) being—

“(i) an officer or employee of a governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or

“(ii) a person acting as an agent of a governmental entity (as so defined), willfully acts or fails to act so as to cause a violation of clause (vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C);

“(L) being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (x), (xi), (xiv), or (xv) of section 205(c)(2)(C);

“(M) violates section 208A (relating to prohibition of the sale, purchase, or display of the social security account number in the private sector) or, as a person in the private sector, violates section 205(c)(2)(C)(xv); or

“(N) violates section 208(g) (relating to fraud by social security administration employees);

shall be subject to, in addition to any other penalties that may be prescribed by law, a civil money penalty of not more than \$5,000 for each violation. Such person shall also be subject to an assessment, in lieu of damages sustained by the United States resulting from such violation, of not more than twice the amount of any benefits or payments paid as a result of such violation.”

(b) EFFECTIVE DATES.—The amendments made by this section shall apply with respect to violations committed after the date of the enactment of this Act, except that

subparagraphs (J), (K), (L), and (M) of section 1129(a)(3) of the Social Security Act (added by subsection (a)) shall apply with respect to violations of the provisions of clause (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C) or section 208A occurring on or after the applicable effective date provided in connection with such provisions under section 2, 3, 4, 5, 6, 7, or 8 of this Act.

SEC. 11. CRIMINAL PENALTIES FOR EMPLOYEES OF THE SOCIAL SECURITY ADMINISTRATION WHO KNOWINGLY AND FRAUDULENTLY ISSUE SOCIAL SECURITY CARDS OR SOCIAL SECURITY ACCOUNT NUMBERS.

(a) IN GENERAL.—Section 208 of the Social Security Act (as amended by section 9) is amended further by adding at the end the following new subsection:

“(g)(1) Whoever is an employee of the Social Security Administration and knowingly and fraudulently sells or transfers one or more social security account numbers or social security cards shall, upon conviction, be guilty of a felony and fined under title 18, United States Code, imprisoned as provided in paragraph (2), or both.

“(2) Imprisonment for a violation described in paragraph (1) shall be for—

“(A) not more than 5 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred not more than 50 social security account numbers or social security cards,

“(B) not more than 10 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred more than 50, but not more than 100, social security account numbers or social security cards, or

“(C) not more than 20 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred more than 100 social security account numbers or social security cards.

“(3) For purposes of this subsection—

“(A) The term ‘social security employee’ means any State employee of a State disability determination service, any officer, employee, or contractor of the Social Security Administration, any employee of such a contractor, or any volunteer providing services or assistance in any facility of the Social Security Administration.

“(B) The term ‘social security account number’ means a social security account number assigned by the Commissioner of Social Security under section 205(c)(2)(B) or another number that has not been so assigned but is purported to have been so assigned.

“(C) The term ‘social security card’ means a card issued by the Commissioner of Social Security under section 205(c)(2)(G), another card which has not been so issued but is purported to have been so issued, and banknote paper of the type described in section 205(c)(2)(G) prepared for the entry of social security account numbers, whether fully completed or not.”

(b) EFFECTIVE DATE.—The amendment made by this section shall apply with respect to violations occurring on or after the date of the enactment of this Act.

SEC. 12. ENHANCED PENALTIES IN CASES OF TERRORISM, DRUG TRAFFICKING, CRIMES OF VIOLENCE, OR PRIOR OFFENSES.

(a) AMENDMENTS TO TITLE II.—Section 208 of the Social Security Act (as amended by the preceding provisions of this Act) is amended further—

(1) in subsection (a), by striking “shall be fined” and all that follows and inserting the following: “shall be fined, imprisoned, or both, as provided in subsection (c).”;

(2) in subsection (b)(2)(B)(ii) (as added by section 9), by striking “be fined” and all that follows and inserting the following: “be fined, imprisoned, or both, as provided in subsection (c).”;

(3) by striking subsection (d);

(4) by redesignating subsection (c) as subsection (d); and

(5) by inserting after subsection (b) the following new subsection:

“(c) A person convicted of a violation described in subsection (a) or a violation described in subsection (b)(2)(A) which is subject to subsection (b)(2)(B)(ii) shall be—

“(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial violation, subject to paragraphs (3) and (4),

“(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which occurs after a prior conviction for another offense under subsection (a) becomes final, subject to paragraphs (3) and (4),

“(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is committed to facilitate a drug trafficking crime (as defined in section 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title 18,

United States Code) involving force against the person of another, subject to paragraph (4), and

“(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).”.

(b) AMENDMENTS TO TITLE VIII.—Section 811 of such Act (42 U.S.C. 1011) is amended—

(1) in subsection (a), by striking “shall be fined” and all that follows and inserting “shall be fined, imprisoned, or both, as provided in subsection (b).”;

(2) by redesignating subsection (b) as subsection (c); and

(3) by inserting after subsection (a) the following new subsection:

“(b) PUNISHMENT.—A person convicted of a violation described in subsection (a) shall be—

“(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial violation, subject to paragraphs (3) and (4),

“(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which occurs after a prior conviction for another offense under subsection (a) becomes final, subject to paragraphs (3) and (4),

“(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is committed to facilitate a drug trafficking crime (as defined in section 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title 18, United States Code) involving force against the person of another, subject to paragraph (4), and

“(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).”.

(c) AMENDMENTS TO TITLE XVI.—Section 1632 of such Act (42 U.S.C. 1383a) is amended—

(1) in subsection (a), by striking “shall be fined” and all that follows and inserting “shall be fined, imprisoned, or both, as provided in subsection (b).”;

(2) by redesignating subsections (b) and (c) as subsections (c) and (d), respectively; and

(3) by inserting after subsection (a) the following new subsection:

“(b) A person convicted of a violation described in subsection (a) shall be—

“(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial violation, subject to paragraphs (3) and (4),

“(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which occurs after a prior conviction for another offense under subsection (a) becomes final, subject to paragraphs (3) and (4),

“(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is committed to facilitate a drug trafficking crime (as defined in section 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title 18, United States Code) involving force against the person of another, subject to paragraph (4), and

“(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).”.

(d) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to violations occurring after the date of the enactment of this Act.

SEC. 13. REGULATORY AND ENFORCEMENT AUTHORITY WITH RESPECT TO MISUSE OF THE SOCIAL SECURITY ACCOUNT NUMBER.

Title XI of the Social Security Act is amended by inserting after section 1129B (42 U.S.C. 1320a–7b) the following new section:

“REGULATORY AND ENFORCEMENT AUTHORITY WITH RESPECT TO MISUSE OF THE SOCIAL SECURITY ACCOUNT NUMBER

“SEC. 1129C. (a) REGULATORY AUTHORITY.—

“(1) IN GENERAL.—The Commissioner of Social Security shall prescribe regulations to carry out the provisions of clauses (vi)(II), (x), (xi), (xii), (xiii), (xiv), and

(xv) of section 205(c)(2)(C) and section 208A. Such regulations shall be issued in consultation with the Federal Trade Commission, the Attorney General of the United States, the Secretary of Homeland Security, the Secretary of Health and Human Services, the Secretary of the Treasury, the Federal banking agencies (as defined in section 3 of the Federal Deposit Insurance Act), the National Credit Union Administration, the Securities and Exchange Commission, State attorneys general, and such representatives of the State insurance commissioners as may be designated by the National Association of Insurance Commissioners.

“(2) TREATMENT OF MATTERS RELATING TO LAW ENFORCEMENT AND NATIONAL SECURITY.—In issuing the regulations described in paragraph (1) with respect to the provisions of 205(c)(2)(C)(x)(III), paragraph (A) or (B) of section 208A(b)(2), or section 208A(c)(2) (relating to law enforcement and national security), the sale or purchase of Social Security account numbers may be authorized only if the Commissioner (or the agency or instrumentality delegated authority to issue such regulations under paragraph (5)) determines that—

“(A) such sale or purchase would serve a compelling public interest that cannot reasonably be served through alternative measures, and

“(B) such sale or purchase will not pose an unreasonable risk of identity theft, or bodily, emotional, or financial harm to an individual (taking into account any restrictions and conditions that the agency or instrumentality issuing the regulations imposes on the sale, purchase, or disclosure).

“(3) TREATMENT OF OTHER MATTERS IN GENERAL DISCRETION OF THE COMMISSIONER.—

“(A) IN GENERAL.—In issuing the regulations described in paragraph (1) with respect to the provisions of section 205(c)(2)(C)(x)(VIII) or section 208A(b)(3)(B), the sale, purchase, or display to the general public of social security account numbers may be authorized only after considering, among other relevant factors—

“(i) the extent to which the authorization of the sale, purchase, or display of the social security account number would serve a compelling public interest that cannot reasonably be served through alternative measures,

“(ii) the associated cost or burden of the authorization to the general public, businesses, commercial enterprises, non-profit organizations, and Federal, State, and local governments; and

“(iii) the associated benefit of the authorization to the general public, businesses, commercial enterprises, non-profit associations, and Federal, State, and local governments.

“(B) RESTRICTIONS AND CONDITIONS.—If, after considering the factors in subparagraph (A), the sale, purchase, or display to the general public of social security account numbers is authorized under regulations referred to in subparagraph (A), the Commissioner (or the agency or instrumentality delegated authority to issue such regulations under paragraph (5)) shall impose restrictions and conditions on the sale, purchase, or display to the general public to the extent necessary—

“(i) to provide reasonable assurances that social security account numbers will not be used to commit or facilitate fraud, deceptions, or crime, and

“(ii) to prevent an unreasonable risk of identity theft or bodily, emotional, or financial harm to any individual, considering the nature, likelihood, and severity of the anticipated harm that could result from the sale, purchase, or display to the general public of social security account numbers, together with the nature, likelihood, and extent of any benefits that could be realized.

“(C) 5-YEAR EXPIRATION DATE FOR REGULATIONS.—At the end of the 5-year period beginning on the effective date of any final regulations issued pursuant to this paragraph—

“(i) such regulations shall expire, and

“(ii) new regulations may be issued pursuant to this paragraph.

“(4) ADMINISTRATIVE PROCEDURE.—In the issuance of regulations pursuant to this subsection, notice shall be provided as described in paragraphs (1), (2), and (3) of section 553(b) of title 5, United States Code, and opportunity to participate in the rule making shall be provided in accordance with section 553(c) of such title.

“(5) DELEGATION TO OTHER AGENCIES.—Any agency or instrumentality of the United States may exercise the authority of the Commissioner under this subsection, with respect to matters otherwise subject to regulation by such agency

or instrumentality, to the extent determined appropriate in regulations of the Commissioner.

“(6) CONSULTATION AND COORDINATION.—Each agency and instrumentality exercising authority to issue regulations under this subsection shall consult and coordinate with the other such agencies and instrumentalities for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency or instrumentality are consistent and comparable, as appropriate, with the regulations prescribed by the other such agencies and instrumentalities. The Commissioner shall undertake to facilitate such consultation and coordination.

“(7) DEFINITIONS AND SPECIAL RULES.—

“(A) For purposes of this subsection, the terms ‘sell’, ‘purchase’, and ‘display to the general public’ shall have the meanings provided such terms under section 205(c)(2)(C)(x) or section 208A(a), as applicable.

“(B) For purposes of this subsection, section 205(c)(2)(C)(x)(XI) shall apply.

“(b) COORDINATION OF ENFORCEMENT WITH OTHER AGENCIES.—The Commissioner may provide, by regulation, for enforcement by any other agency or instrumentality of the United States of the provisions of section 208A and regulations prescribed pursuant to subsection (a)(1) with respect to section 208A.

“(c) ACTIONS BY STATES WITH RESPECT TO MISUSE IN PRIVATE SECTOR OR BY STATE AND LOCAL GOVERNMENTS.—

“(1) CIVIL ACTIONS.—In any case in which the attorney general of a State (as defined in section 205(c)(2)(C)(x)(X)) has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice described in paragraph (2), the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction, to—

“(A) enjoin that act or practice;

“(B) enforce compliance with the regulation;

“(C) obtain civil penalties in an amount of \$11,000 per violation not to exceed a total of \$5,000,000; or

“(D) obtain such other legal and equitable relief as the district court may consider to be appropriate.

Before filing an action under this subsection, the attorney general of the State involved shall provide to the Commissioner of Social Security and the Attorney General of the United States a written notice of that action and a copy of the complaint for that action. If the State attorney general determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action, the State attorney general shall provide the written notice and the copy of the complaint as soon after the filing of the complaint as practicable. Any reference in this subsection to the attorney general of a State shall be deemed also to be a reference to any equivalent official of such State.

“(2) ACTS OR PRACTICES SUBJECT TO ENFORCEMENT.—An act or practice described in this paragraph is—

“(A) an act or practice by an executive, legislative, or judicial agency or instrumentality of the State involved or a political subdivision thereof, a person acting as an agent thereof, or any officer or employee of the foregoing or person acting as an agent of the foregoing that violates clause (vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C) or any regulation promulgated thereunder, or

“(B) an act or practice by any person that violates section 208A or any regulation promulgated thereunder.

“(3) ATTORNEY GENERAL AUTHORITY.—On receiving notice under paragraph (1), the Attorney General of the United States shall have the right—

“(A) to move to stay the action, pending the final disposition of a pending Federal matter as described in paragraph (4);

“(B) to intervene in an action under paragraph (1);

“(C) upon so intervening, to be heard on all matters arising therein; and

“(D) to file petitions for appeal.

“(4) PENDING CRIMINAL PROCEEDINGS.—If the Attorney General of the United States has instituted a criminal proceeding under section 208 alleging an act or practice described in paragraph (2) in connection with any State, such State may not, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in the criminal proceeding.

“(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this subsection shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to conduct investigations, administer oaths and

affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

“(6) VENUE; SERVICE OF PROCESS.—Any action brought under paragraph (1) may be brought in any district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. In an action brought under paragraph (1), process may be served in any district in which the defendant is an inhabitant or may be found.

“(d) REMEDIES TO INDIVIDUALS FOR VIOLATIONS BY THE FEDERAL GOVERNMENT OF REQUIREMENTS RELATING TO SOCIAL SECURITY ACCOUNT NUMBERS.—

“(1) CIVIL ACTIONS.—Any individual who is aggrieved by an act or practice by any person acting as an officer, employee, or agent of an agency or instrumentality of the Federal Government in violation of the requirements of clause (vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of subsection (c)(2)(C) with respect to the social security account number assigned to such individual under subsection (c)(2)(B) may commence a civil action for appropriate equitable relief or actual damages.

“(2) VENUE; SERVICE OF PROCESS.—An action under this subsection action may be brought in the district court of the United States for the judicial district in which the plaintiff resides, or has his principal place of business, in which the violation took place, or in which the defendant resides or may be found, and process may be served in any other district in which a defendant resides or may be found.

“(3) JURISDICTION.—The district courts of the United States shall have jurisdiction, without respect to the amount in controversy or the citizenship of the parties, to grant the relief provided for in paragraph (1).

“(4) ATTORNEY’S FEES.—In any action under this subsection, the court in its discretion may allow a reasonable attorney’s fee and costs of action to either party.

“(e) ONGOING GAO REVIEW ON EFFICACY OF REGULATIONS.—

“(1) IN GENERAL.—The Comptroller General of the United States shall conduct an ongoing review of the efficacy of the regulations prescribed by any agency or instrumentality of the United States pursuant to this section. Such review shall consider the extent to which such regulations are consistent with, and in furtherance of the purposes of, the amendments made by the Social Security Number Privacy and Identity Theft Prevention Act of 2007.

“(2) REPORT.—Not later than 4 years after the effective date of any final regulations issued by any agency or instrumentality of the United States pursuant to this section, the Comptroller General shall report to each House of the Congress regarding the results of the review of such regulations conducted under this paragraph. Such report shall include the Comptroller General’s recommendations for such statutory or regulatory changes as the Comptroller General considers appropriate.”

SEC. 14. STUDY ON FEASIBILITY OF BANNING SOCIAL SECURITY ACCOUNT NUMBER AS AN AUTHENTICATOR.

(a) STUDY.—As soon as practicable after the date of the enactment of this Act, the Commissioner of Social Security shall enter into an arrangement with the National Research Council under which the Council shall carry out a study to determine—

- (1) the extent of the use of social security account numbers as a primary means of authenticating identity;
- (2) the extent of the use of social security account numbers for verification in commercial transactions; and
- (3) the feasibility of a prohibition on such use.

The study shall also examine possible alternatives to social security account numbers for verification purposes and uses in authenticating identity.

(b) REPORT.—The arrangement entered into with the Council under this section shall provide for submission by the Council to the Commissioner and to each House of the Congress of a report setting forth the results of the Council’s study under this section, together with the Council’s findings and recommendations, no later than 1 year after the effective date of the initial final regulations issued by the Commissioner pursuant to the amendments made by section 2 of this Act.

I. INTRODUCTION

A. PURPOSE AND SUMMARY

The purpose of the “Social Security Number Privacy and Identity Theft Prevention Act of 2007,” H.R. 3046, is to enhance Social Se-

curity number (SSN) privacy protections, prevent misuse of SSNs, and to otherwise enhance protections against identity theft.

The bill would restrict the sale, purchase and display to the general public of SSNs in the public and private sectors; provide additional measures to protect SSN privacy; and create criminal and civil monetary penalties for persons who misuse SSNs.

B. BACKGROUND

The SSN was created in 1936 to track workers' earnings for the purpose of paying Social Security taxes and determining eligibility and benefit amounts upon retirement, or later upon disability. Since 1936, the Social Security Administration (SSA) has issued more than 400 million SSNs.

Although the SSN was originally created for administering the Social Security program, its use has expanded dramatically throughout both the public and private sectors. Federal use of the SSN was first mandated by President Roosevelt in 1943 with Executive Order 9397. This Executive Order required that any Federal department establishing a new system of permanent account numbers pertaining to an individual must exclusively utilize the SSN and that such personal information must be kept confidential. Today the SSN is required for the administration of a number of government benefit programs and the Federal income tax.

In addition to uses mandated by Federal law, the SSN is also widely used in the public and private sectors for purposes that are neither required nor prohibited by law. As a result, the SSN is generally regarded as the single-most widely used record identifier by both government and private sectors within the United States.

Ubiquitous use of SSNs and the ease with which individuals can access another person's SSN have raised serious concerns over privacy and opportunities for identity theft and fraud. The Federal Trade Commission (FTC), SSA, the SSA Inspector General and others acknowledge that SSNs play a pivotal role in identity theft. Even worse, terrorists may steal, fake, or purchase SSNs in order to operate in our society and abet their nefarious acts. The FTC reported in 2003 that 10 million Americans fell prey to identity theft in the prior year. A more recent survey by Gartner, Inc. estimated the number of identity theft victims at 15 million in 2006. The FTC study found that victims spent an estimated \$5 billion to rehabilitate their good names, and businesses lost over \$50 billion to identity theft-related fraud in a single year. Protecting the privacy of SSNs will help to protect our individual and national security.

The absence of overarching Federal law regulating the sale, purchase, and public display of SSNs, and the growing threat represented by SSN misuse and identity theft, have prompted a need to better protect the privacy and integrity of SSNs.

C. LEGISLATIVE HISTORY

During the 106th Congress, the Subcommittee on Social Security held hearings on Social Security program integrity on March 30, 2000 (106-38); representative payees on May 4, 2000 (106-57); use and misuse of SSNs on May 9 and May 11, 2000 (106-108); and the processing of attorney's fees on June 14, 2000 (106-70). The information gained from these hearings led to the introduction of

H.R. 4857, the “Privacy and Identity Protection Act of 2000,” on July 13, 2000. The bill enhanced privacy protections for individuals, prevented fraudulent misuse of the SSN, and provided additional safeguards for Social Security and Supplemental Security Income (SSI) beneficiaries with representative payees. A further hearing on protecting privacy and preventing misuse of the SSN was held on July 17, 2000 (106–43). On July 20, 2000, the Subcommittee on Social Security ordered favorably reported H.R. 4857, as amended. The Committee on Ways and Means ordered the bill favorably reported, as amended on September 28, 2000 (H. Rept. 106–996 Part 1). The bill was not considered by the full House, as other committees of jurisdiction did not complete consideration of the bill.

During the 107th Congress, the Subcommittee on Social Security held a hearing on protecting privacy and preventing misuse of SSNs on May 22, 2001 (107–31). In response to information gathered at this hearing and previous hearings in the 106th Congress, H.R. 2036, the “Social Security Number Privacy and Identity Theft Prevention Act of 2001,” was introduced on May 25, 2001. The bill restricted the sale, purchase, and display of SSNs, limited dissemination of SSNs by credit reporting agencies, and made it more difficult for businesses to deny services if a customer refused to provide his or her SSN. Further hearings were held on preventing identity theft by terrorists and criminals, held jointly with the Committee on Financial Services, Subcommittee on Oversight and Investigations on November 8, 2001 (107–51); protecting the privacy of SSNs and preventing identity theft on April 29, 2002 (107–71); and preserving the integrity of SSNs and preventing their misuse by terrorists and identity thieves, held jointly with the Committee on Judiciary, Subcommittee on Immigration, Border Security, and Claims on September 19, 2002 (107–81). Neither the House nor the Senate acted on the bill.

During the 108th Congress, the Subcommittee on Social Security held a hearing on the use and misuse of SSNs on July 10, 2003 (108–35). The Government Accountability Office (GAO—then known as the General Accounting Office) witness testified that SSNs are widely utilized in both the public and private sectors as an identifier, and cited numerous examples where public and private databases had been compromised and personal data, including SSNs, had been stolen. They also found that in some cases, the display of SSNs in public records and easily accessible websites provided an opportunity for identity thieves. The SSA Inspector General testified that the most important step in preventing SSN misuse is to limit its easy availability through public records, sale on the open market, and unnecessary use. Consumer advocate witnesses testified regarding the growing crime of identity theft, its impact on victims, and the need to protect the privacy of SSNs. A law enforcement witness testified that SSNs are key to the takeover of another individual’s identity, described difficulties in prosecuting identity theft, and stated the need to restrict SSN use to necessary purposes.

Based on information gathered at this hearing and hearings in previous Congresses, Social Security Subcommittee Chairman E. Clay Shaw, Jr. and Ranking Member Robert T. Matsui introduced H.R. 2971, the “Social Security Number Privacy and Identity Theft

Prevention Act of 2003,” on July 25, 2003. The bill was referred to the Committee on Ways and Means, the Committee on Financial Services, and the Committee on Energy and Commerce. The Subcommittee on Social Security held a further hearing on enhancing SSN privacy on June 15, 2004, and marked up the bill on July 15, 2004. The bill was reported favorably to the full Committee on Ways and Means on July 15, 2004, as amended, by voice vote. On July 21, 2004, the Committee on Ways and Means marked up H.R. 2971, as amended by the Subcommittee. Chairman Thomas offered an amendment in the nature of a substitute, which was agreed to by voice vote. The Committee then ordered favorably reported H.R. 2971, as amended, by a roll call vote of 33 yeas to 0 nays. The bill was not considered by the full House, as other committees of jurisdiction did not complete consideration of the bill.

In addition, during the 106th, 107th, 108th and 109th Congresses, Subcommittee Chairman Shaw and other Members of Congress asked the GAO for a number of reports to inform the debate on SSN privacy and integrity. These reports explained how government agencies and private sector businesses such as consumer reporting agencies, information resellers, and health care organizations collect, utilize, and safeguard SSNs (Social Security: Government and Commercial Use of the Social Security Number is Widespread, GAO/HEHS-99-28; Social Security Numbers: Government Benefits from SSN Use But Could Provide Better Safeguards, GAO-02-352; Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information, GAO 04-11; Social Security Numbers: Use is Widespread and Protections Vary, GAO-04-768T; Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data, GAO-06-674).

During the 109th Congress, the Subcommittee on Social Security held a series of five hearings on SSN high risk issues. The hearings addressed the role of SSNs in abetting identity theft, and discussed the impact of prohibiting or restricting the use, sale, purchase, or display of SSNs by individuals, businesses, or the government. Based on these and prior hearings, Subcommittee Chairman Shaw and Full Committee Ranking Member Charles B. Rangel introduced H.R. 1745, the “Social Security Number Privacy and Identity Theft Protection Act of 2005,” on April 20, 2005. The bill was referred to the Committee on Ways and Means, the Committee on Financial Services, and the Committee on Energy and Commerce. The bill was not reported.

During the 110th Congress, the Subcommittee on Social Security held a hearing on protecting the privacy of the SSN from identity theft on June 21, 2007. The GAO witness testified that SSNs are vulnerable to misuse because there is no Federal standard for truncating SSNs, which allows identity thieves to piece together portions of SSNs from different sources. The SSA Inspector General testified that Federal efforts to protect the SSN should be improved by limiting the use of the SSNs on school and hospital identification cards. An expert on technology and data privacy testified that the SSN should not be used as an identifier or authenticator, that steps should be taken to reduce the use and exposure of SSNs, and that businesses have alternatives to over-reliance on SSNs for record matching and verification. Also during the 110th Congress,

GAO issued a report identifying which Federal agencies provide records containing SSNs to state and local record keepers, and the significant vulnerabilities that remain in the protection of SSNs in public records (Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, GAO-07-752).

Based on information gathered at this hearing and hearings in previous Congresses, Social Security Subcommittee Chairman Michael R. McNulty and Ranking Member Sam Johnson introduced H.R. 3046, the “Social Security Number Privacy and Identity Theft Prevention Act of 2007,” on July 16, 2007. The bill was referred to the Committee on Ways and Means. On July 18, 2007, the Committee marked-up the bill; and Chairman Rangel offered an amendment in the nature of a substitute, which was agreed to by voice vote. The Committee then ordered favorably reported H.R. 3046, as amended, by a rollcall vote of 41 yeas to 0 nays.

II. SECTION-BY-SECTION SUMMARY

Sec. 1. Short title

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

Section 1 provides that the Act may be cited as the “Social Security Number Privacy and Identity Theft Prevention Act of 2007.”

REASON FOR CHANGE

The section identifies the short title for the bill.

Sec. 2. Restrictions on the sale or display to the general public of Social Security account numbers by governmental entities

CURRENT LAW

The SSN is required by law for the administration of a number of Federal programs. In addition, Federal law permits States to require the SSN in the administration of certain State programs, and in other cases Federal law requires the States to use the SSN in the administration of Federal or State programs. No Federal law regulates the overall use of SSNs by Federal, State or local governments. The “Department of Transportation and Related Agencies Appropriations Act” (P.L. 106-346) amended the “Driver’s Privacy Protection Act of 1994” (P.L. 103-322) to require States to obtain express consent of drivers before sharing or selling drivers’ “highly restricted personal information,” including SSNs, except under very limited circumstances.

EXPLANATION OF PROVISION

The bill would restrict the sale or display to the general public of full or partial SSNs by Federal, State or local governmental agencies and their agents, by a Federally recognized Indian tribe, or by a bankruptcy trustee. The sale of SSNs would be permitted as follows:

1. As specifically authorized by the “Social Security Act” (P.L. 74–271) or the “Privacy Act of 1974” (P.L. 93–579), which includes data-matching performed by SSA and reimbursed by other agencies for the administration of programs whose purposes are compatible with the Social Security Act;

2. For law enforcement or national security purposes;

3. For tax compliance;

4. By State departments of motor vehicles for use by a government agency in carrying out its functions; for use by an insurer for claims investigation, anti-fraud activities, and rating or underwriting; and for use by an employer to obtain or verify information about a holder of a commercial driver’s license;

5. To a consumer reporting agency under the “Fair Credit Reporting Act” (FCRA, P.L. 91–508) solely for use or disclosure for permissible purposes under the FCRA as follows: as ordered by a court or a Federal grand jury subpoena; as instructed by the consumer in writing; for the extension of credit based on a consumer’s application; for review or collection of a consumer’s account; for employment purposes; for insurance underwriting based on a consumer’s application; when there is a legitimate business need regarding a transaction the consumer initiates; to review whether a customer meets the terms of his or her account; to determine a consumer’s eligibility for a license or other benefit granted by a government agency; to analyze the credit or prepayment risks associated with an existing credit obligation; and for use by State and local officials for child support payment purposes;

6. For government research advancing the public good.

In addition, the Commissioner of Social Security would be permitted to authorize sale and display to the general public of SSNs in other circumstances as determined appropriate.

The restrictions on sale or display to the general public of SSNs would not apply to SSNs of deceased persons.

The restrictions that would be established under this provision would not override other restrictions or limitations in Federal or State law or regulations in effect to the extent that they provide greater protections for SSNs than would be created under this bill.

The bill would define “governmental entity” as an executive, legislative, or judicial agency or instrumentality of the Federal or State government, including a Federally recognized Indian tribe, a bankruptcy trustee, and agents of the entity.

The bill would define “sell” as obtaining anything of value, directly or indirectly, in exchange for an SSN. However, the submission of the SSN in the process of applying for government benefits or programs, and in the administration of an employee benefit plan, would not be considered a sale.

“Display to the general public” would mean to intentionally place an SSN in a viewable manner on an Internet site that is available to the general public or to provide access to the general public by other means. In addition, requiring an individual to transmit his or her SSN over the Internet without ensuring the number is encrypted or otherwise protected would be considered a prohibited display to the general public.

“Social Security account number” would include a partial SSN. However, the bill would provide a temporary exemption permitting government entities to sell and publicly display the last four digits

of an SSN for two years after the effective date of the final regulations.

REASON FOR CHANGE

The Federal government created the SSN, under the authority of the Social Security Act, and its use has since been required for a broad range of interactions between individuals and the government, including tax administration, many benefit programs, and driver's and professional licenses. While there are laws protecting the privacy of SSNs held by certain agencies or under specific circumstances, there is no comprehensive law protecting the privacy of SSNs held by Federal, State, and local government agencies. As a result, SSNs may be sold, displayed on the Internet, or otherwise made available to the general public on paper, computer disk, or other means to individuals requesting a copy—for example through open court or other government records—and may be obtained by third parties who can subsequently sell or display the information to others.

Since SSNs are the key to accessing an individual's financial and other personal information, the wide accessibility of SSNs has raised serious concerns over privacy. Testimony before the Subcommittee on Social Security highlights the relative ease by which an individual can obtain another person's SSN and use the information to commit identity theft or other crimes. Restricting the display to the general public and sale of SSNs by governments will help curb fraudulent activity by making it more difficult for criminals to access this personal information.

The bill would provide specific exceptions to permit the continuation of SSN exchanges that provide important benefits in the public interest such as law enforcement; administration of government programs, including SSI, Medicaid, and unemployment insurance; administration of employee benefits; limited commercial purposes such as granting credit and insurance; tax administration; and government research advancing the public good.

In addition, authority would be given to the Commissioner to authorize sale and display to the general public of SSNs as determined appropriate under guidelines specified in section 13 of the bill. Since SSN use is so pervasive in both the public and private sectors, is linked to so many government and business transactions, and because of evolving needs regarding SSN utilization and new technologies to facilitate information exchanges, this exception is intended to allow the Commissioner or agencies to which it delegates authority to thoroughly evaluate how SSNs are sold and displayed, the degree to which they are convenient versus essential to such exchanges, and to modify the rules as needed. However, it is expected that this authority would be used extremely judiciously, and not merely for the sake of facilitating transactions or data-matching that could be reasonably accomplished without the use of the SSN. In comparing the costs and benefits of authorizing SSN sale or display to the general public and whether the authorization serves a compelling public interest that cannot reasonably be served through alternative measures, it is expected that the Commissioner and other agencies would give significant weight to the need to maintain individuals' privacy and safety, as well as the bill's purpose of preventing identity theft.

With respect to the exception for research advancing the public good, the intent is to preserve the government's ability to conduct scientific, epidemiological, and social scientific research that would benefit the public. In the case of research involving medical information on individuals, it is expected that SSA will only authorize sale of SSNs in strict compliance with Federal rules and regulations on the privacy of medical information.

The bill also provides a "transition rule," which permits the government to use the last four digits of the SSN where the sale or public display is otherwise prohibited, to provide a period of transition to less reliance overall on the SSN and its derivatives. In combination with the effective date of the implementation rules, this transition rule permits government sale and display of the SSN for four and one-half years after enactment, in order to accommodate the transition to the prohibitions on sale and public display.

The restrictions on sale and display to the general public of SSNs would not apply to the SSNs of deceased persons. This is because the sale and public availability of information on deceased individuals is necessary to prevent waste, fraud, and abuse. SSA compiles a Death Master File (DMF), which contains the name, date of birth, date of death, SSN, and other information for about 70 million individuals. The SSA DMF is used by leading government, financial, investigative, and credit reporting organizations, in medical research and by other industries to verify identity as well as to prevent fraud and comply with the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act, P.L. 107-56).

The restrictions on sale and display by government agencies, trustees, and their agents would only apply to SSNs they require individuals or others to provide. During Social Security Subcommittee hearings on the bill, court and other public records administrators testified they receive numerous documents filed by individuals, businesses, and attorneys that often include SSNs the government did not require to be submitted, and of which they are therefore unaware. They stated redaction of "incidentally" included SSNs would create a serious administrative burden, and it would require significant resources to review each document and redact such incidental SSNs. Therefore, the bill would make government agencies, trustees, and their agents responsible only for those SSNs they require individuals to submit, since they should be able to easily locate and redact them. For example, a court requiring individuals to provide their SSNs on a coversheet for filed documents could remove the coversheet or redact the SSN before selling the court record or displaying it to the general public. With respect to SSNs submitted in court documents absent the court's requirement to do so, the individual communicating the SSN in the document, not the court, would be held responsible according to section 8 of the bill.

The restrictions established under this bill would serve as a floor of protection for SSNs, and are not intended to override SSN protections in Federal or State law or regulations in effect to the extent they provide greater restrictions on SSN sale, purchase, or display to the general public than would be created under the bill. For example, this bill is not intended to circumvent the provision included in section 1735 of the "Food, Agriculture, Conservation, and

Trade Act of 1990” (P.L. 101–624) preventing the disclosure of SSNs maintained as the result of laws enacted on or after October 1, 1990.

EFFECTIVE DATE

Initial final regulations to carry out the provisions would have to be issued by the Commissioner of Social Security or any other agency to which the Commissioner delegates authority within 18 calendar months after the date of enactment. The provisions would take effect one year after issuance of initial final regulations. The provisions would not apply to display of records generated prior to the date the provisions become effective. The temporary exemption to allow sale and display of the last four digits of the SSN would expire two years after the effective date of the initial final regulations.

Sec. 3. Prohibition of display of Social Security account numbers on checks issued for payment by governmental entities

CURRENT LAW

No Federal law regulates the overall use of SSNs by Federal, State, or local governments. However, the “Social Security Number Confidentiality Act of 2000” (P.L. 106–433) specifically directed the Secretary of the Treasury to take necessary action to ensure that SSNs are not visible on or through unopened mailings of checks or other drafts.

EXPLANATION OF PROVISION

The bill would prohibit Federal, State, or local governments, or bankruptcy trustees, from including full or partial SSNs on checks issued for payment or on any documents accompanying checks.

REASON FOR CHANGE

The Subcommittee on Social Security has heard testimony from the Postal Inspection Service and consumer advocates that mail theft and rifling through trash for discarded documents are means by which identity thieves gain access to personal information, including SSNs.

EFFECTIVE DATE

Provision would apply with respect to checks (and documents attached to or accompanying such checks) issued after one year after enactment.

Sec. 4. Prohibition of the display of Social Security account numbers on certain government identification cards or tags

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

The bill would prohibit government agencies and those providing employee benefits for a government agency from displaying an individual’s full or partial SSN on any identification card or tag issued

to employees or employees' family members; on identification cards issued to students at government educational institutions; on identification tags issued to patients at government medical institutions; and on Medicare cards. This would include use of a magnetic strip, bar code, or other means of communication to convey the full or partial SSN.

REASON FOR CHANGE

SSNs are often utilized as employee identification numbers or customer account numbers for the sake of convenience. However, the display of SSNs on military identification tags, employee identification cards, student identification cards, patient identification cards and tags, health benefit cards, the Medicare card, customer cards, and on other cards or tags that are required to be submitted or displayed to others, which are frequently carried in individuals' wallets, unnecessarily increases the risk of identity theft. Similar prohibitions have been enacted under several State laws, and the Centers for Medicare and Medicaid Services and the Department of Defense are both evaluating their use of SSNs in light of identity theft concerns. This provision is not intended to prevent inclusion of encrypted SSNs (those that are transformed by a secret code to appear as other than the nine-digit number assigned by the Commissioner of Social Security when read or otherwise accessed by unauthorized parties).

EFFECTIVE DATE

Provision would apply with respect to cards or tags issued after one year after enactment, except for Medicare cards, for which the prohibition would first apply two and one-half years after enactment.

Sec. 5. Prohibition of inmate access to Social Security account numbers

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

The bill would prohibit Federal, State or local governments from employing prisoners in any capacity that would allow prisoners access to full or partial SSNs of other individuals.

REASON FOR CHANGE

Prisoners, including those who may have been incarcerated for identity theft, should not have access to SSNs or derivatives of SSNs, thereby posing a serious risk of identity theft or fraud. The Subcommittee on Social Security has heard testimony regarding a serious instance where use of prisoner labor to process personal information resulted in a case of stalking (*Beverly Dennis, et al v. Metromail, et al.*, No. 96-04451, District Court, Travis County, Texas).

EFFECTIVE DATE

Provision would apply with respect to employment or entry into contract for employment of prisoners on or after enactment. In the case of employment or contracts for employment in effect on the date of enactment, provision would take effect 90 days after enactment.

Sec. 6. Measures to preclude unauthorized disclosure by governmental entities of Social Security account numbers and protect the confidentiality of such numbers

CURRENT LAW

The Social Security Act requires officers and employees of Federal and State governments to keep SSNs and related records confidential. It also prohibits officers and employees from disclosing SSNs or related records.

The Privacy Act of 1974 requires Federal agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the agencies' systems of records. The term "records" includes any personally identifiable item or information about an individual that is maintained by an agency.

EXPLANATION OF PROVISION

With respect to Federal, State, and local government employees and their agents, the bill would restrict access to SSNs and any derivative thereof to employees whose responsibilities require access for administration or enforcement of the government agency's functions. Government agencies and their agents would be required to provide safeguards to prevent unauthorized access to SSNs and protect their confidentiality.

REASON FOR CHANGE

There have been numerous reported cases of computer hackers obtaining SSNs from universities and other institutions. In addition, the Subcommittee on Social Security has heard testimony on how identity theft rings may plant an employee inside an organization to access SSNs and other personal information. Finally, there have been numerous recent instances where government agencies have failed to adequately secure confidential data which includes SSNs, such as the U.S. Department of Veterans Affairs and the State of Ohio.

Also, the Personal Responsibility and Work Opportunity Act of 1996 (P.L. 105-33) requires state agencies to collect SSNs from applicants for professional licenses, drivers' licenses and marriage licenses. In 1997, the Balanced Budget Act (P.L. 104-193) amended this requirement to include recreational licenses. The goal of these provisions was to enhance the ability of family support agencies to locate parents who were not supporting their children and enforce child support payment orders.

Citizens obtain drivers licenses, professional licenses and marriage licenses in government offices. Hunting, fishing and boating licenses, in addition to being available through government offices or online, are typically sold in retail stores, outdoor marinas, or

public parks, where, according to testimony provided to the Subcommittee on Social Security in 2006, transactions are relatively open; employees processing the sale are often young, seasonal workers with very little training of any type; and data security protocols rarely include more than closing the cover on the receipt book.

The Committee believes that government agencies and their agents (as in the case of retailers of recreational licenses) that ask or require individuals to provide their SSN to obtain benefits or services have a responsibility to safeguard SSNs from unauthorized access by employees or other individuals.

This provision is not intended to prevent government employees or those to whom government agencies contract work from accessing SSNs in cases where it is necessary for performance of their duties, or to impede data exchanges between government agencies that include SSN information and are in accordance with section 2 of the bill. For example, it is not the intent to prevent State unemployment insurance agencies from sending wage records or claim information to other Federal, State, or local government agencies (e.g. for purposes of determining eligibility or benefit amounts for Temporary Assistance to Needy Families, Housing and Urban Development assistance, Food Stamps, SSI, etc.).

EFFECTIVE DATE

Provision would take effect one year after the date of enactment.

Sec. 7. Uniform standards for truncation of the Social Security account number

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

This bill would restrict the sale, purchase, and public display of the SSN, and certain other uses of the SSN, in both the public and private sectors. In situations not regulated by this bill, government entities and the private sector may voluntarily choose to use a truncated version of the SSN. However, if they choose to do so, the bill would require any truncated version of an individual's SSN to be limited to not more than the last four digits of the SSN.

REASON FOR CHANGE

A 2007 report by the GAO (Social Security Numbers: Federal Actions Could Decrease Availability in Public Records, though Other Vulnerabilities Remain, GAO-07-752), recommended that Congress enact truncation standards for SSNs. GAO found that because there are no uniform truncation standards, identity thieves may be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources. This bill would create a uniform truncation standard—limited to no more than the last four digits of the SSN, which are randomly generated—with which government and private sector entities must comply to limit identity thieves' access to full or partial SSNs.

EFFECTIVE DATE

Initial final regulations to carry out the provisions would have to be issued by the Commissioner (or any agency to which it delegates authority) within 18 calendar months after the date of enactment. The provision would take effect one year after issuance of initial final regulations.

Sec. 8. Prohibition of the sale, purchase, and display to the general public of the Social Security account number in the private sector

CURRENT LAW

The Gramm-Leach-Bliley Act (GLBA, P.L. 106–102) restricts the ability of financial institutions to disclose nonpublic personal information about consumers, including SSNs, to nonaffiliated third parties, although consumers must opt-out of such sharing arrangements. Moreover, GLBA allows financial institutions to sell SSNs among their affiliates, who may number in the thousands and may not themselves be financial institutions. Consumers have no opt-out right under GLBA against selling of SSNs to affiliates, which is often done for marketing purposes.

FCRA regulates businesses that regularly provide information about consumers to third parties for purposes of determining eligibility for credit, employment, insurance, and for any other legitimate business need in a transaction initiated by a consumer. Entities that provide such reports on consumers are considered to fall under FCRA's coverage. Moreover, FCRA requires companies that provide such information to abide by certain consumer protections, such as allowing consumers to view and correct inaccuracies in such reports.

The "Health Insurance Portability and Accountability Act" (HIPAA, P.L. 104–191) Privacy Rule limits health plans, health care clearinghouses, and health care providers from disclosing certain protected information, including SSNs. Individuals must give specific authorization before health care providers and other covered entities may disclose protected information in most non-routine circumstances.

However, no Federal law regulates the overall sale, purchase, and display to the general public of SSNs in the private sector.

EXPLANATION OF PROVISION

The bill would prohibit the sale, purchase or display to the general public of a full or partial SSN. It also prohibits using an SSN to find an individual with the intent to harass, harm, or physically injure the individual, or using the individual's identity for illegal purposes.

The bill would provide exceptions to the prohibitions on SSN sale and purchase for law enforcement, including but not limited to enforcement of a child support obligation; national security purposes; public health; in emergency situations to protect the health or safety of one or more individuals; for tax compliance; by or to a consumer reporting agency for use or disclosure for permissible purposes described in FCRA (see Explanation of Provision under section 2 of the bill); and government or publicly-funded research (for

advancing the public good and with restrictions to protect privacy of individuals).

The bill would also provide an exception for sale and purchase of SSNs with the affirmative, written consent of the individual so long as consent is voluntary, the terms are presented clearly and conspicuously, and the individual may limit the sale or purchase to purposes directly associated with the transaction.

In addition, the Commissioner of Social Security would be permitted to authorize sale, purchase or public display of SSNs in other circumstances as deemed appropriate.

The bill would prohibit the display of the full or partial SSN of another person on any check issued for payment or on any documents accompanying checks.

The bill would prohibit the unauthorized disclosure of another person's SSN to a government agency or instrumentality that did not request the SSN.

In addition, the bill would prohibit the display of full or partial SSNs on employee identification cards or tags, or cards or tags businesses and others require individuals to use to access goods and services. The restrictions would also prohibit including the SSN on a magnetic strip, bar code, or other means which would convey the SSN.

The bill would require businesses and other entities that collect and store SSNs to prevent unauthorized access by employees or other individuals.

These prohibitions would not apply to SSNs of deceased persons.

The restrictions that would be established under this provision would not override other restrictions or limitations in Federal or State law or regulations in effect to the extent they provide greater protections for SSNs than would be created under this provision in the bill.

The bill would define a "person" to which these prohibitions apply as any individual, partnership, corporation, trust, estate, co-operation, association, or any other entity, other than a governmental entity.

The bill would define "sell" as obtaining, directly or indirectly, anything of value in exchange for the SSN. "Purchase" would mean to provide, directly or indirectly, anything of value in exchange for the SSN. The terms "sell" and "purchase" would not include submission of the SSN when applying for government benefits or programs, use of SSNs in administration of employee benefit plans, or incidental transmission of SSNs as part of the sale, lease, merger, transfer, or exchange of a trade or business.

The exception for the transfer of an SSN as part of the sale, lease, merger, transfer, or exchange of a trade or business in the definitions of "sell" and "purchase" recognizes that there may be SSNs embedded in data files, employee files or loan documents of legitimate businesses that may be transferred when a business or certain assets are sold, where the transfer of the SSN is incidental to the transaction. The Committee intends that this exception encompasses not only the sale of a trade or business in its entirety, but also the sale of parts of a business and the sale of assets, but only where the primary economic value being transferred is derived from assets other than personally identifiable information such as SSNs. Examples of such a covered transfer of assets include a pro-

posed or actual securitization, secondary market sale, sale of servicing rights, or similar transaction related to mortgages and student loans, where an SSN is embedded in the loan file. If SSNs are included in such a transfer, then the recipient is obligated to safeguard them as required under the bill.

“Display to the general public” would mean to intentionally place an SSN in a viewable manner on an Internet site that is available to the general public or to provide access to the general public by other means. In addition, requiring an individual to transmit his or her SSN over the Internet without ensuring the number is encrypted or otherwise protected would be considered a prohibited display to the general public.

“Social Security account number” would include any derivative of the SSN. However, with respect to the restrictions on sale, purchase or public display of the SSN, the bill would provide a temporary exemption permitting private entities to purchase, sell and publicly display the last four digits of an SSN for two years after the effective date of the final regulations.

REASON FOR CHANGE

Use of SSNs in the private sector has proliferated for purposes unrelated to administration of the Social Security program, collection of taxes, or other purposes authorized under Federal law. Businesses often request SSNs from their customers. For example, information resellers, consumer reporting agencies, and financial institutions obtain SSNs and other personal information from customers, public records, and other sources to determine an individual’s identity and accumulate information about them for certain purposes, which may include for marketing purposes or to provide that information to businesses or others for a fee. As a result, Americans are increasingly concerned that the SSN they disclose for one purpose may be subsequently sold to third parties and used for other purposes without their knowledge or consent. For example, an individual discloses his or her SSN to get a bank loan. The bank sends the information to a consumer reporting agency to request a credit report. The consumer reporting agency assembles information on the individual and associates it with the SSN. Under current law, the consumer reporting agency may then incidentally or purposefully sell the SSN and other information to insurance companies, credit companies, information resellers, law enforcement, government agencies, private investigators, and others.

Financial institutions are allowed under current law to disclose nonpublic personal information they gather from consumers or from other sources such as credit bureaus to their affiliates, which may number in the thousands and may not themselves be financial institutions. Affiliations between businesses and financial institutions may often be based on joint-marketing agreements, thus the sale of nonpublic personal information such as SSNs is often done for marketing purposes.

In addition, such widespread use of SSNs increases the risk that business employees, computer hackers, or others may obtain unauthorized access and misuse SSNs to commit identity theft or other crimes. According to a 2003 survey sponsored by the FTC, among identity theft victims who knew the identity of the criminal, 23 per-

cent said the person responsible worked at a company or financial institution that had access to the victim's personal information.

The bill would restrict the sale, purchase, and display to the general public of SSNs. For example, display to the general public would include making records containing SSNs available on paper, computer disk, or other media, in addition to display over the Internet. The bill would also require that SSNs be appropriately safeguarded when collected and stored. The intent is to limit transmission of SSNs in order to minimize opportunities for SSN misuse and identity theft.

In limiting the transmission of SSNs, it is not the intent to prevent individuals from voluntarily providing their own SSNs to facilitate a transaction that they initiate or to prevent businesses from utilizing SSNs in a transaction that the individual authorizes. For example, if an individual voluntarily gives his or her own SSN to a business so that it may provide goods or services, it is not the intent of the bill to call such an exchange the "sale" or "purchase" of the SSN simply because it is facilitating the transaction.

The prohibition against the sale or purchase of SSNs would not prevent financial institutions from complying with the customer identification program requirements of the USA PATRIOT Act. Under the USA PATRIOT Act, banks, savings associations, credit unions and securities firms are required to verify identification information provided by their customers when establishing an account. Financial institutions that utilize verification services offered by consumer reporting agencies and other information resellers generally are not selling or purchasing their customers' SSNs when they check them against a database because the financial institution and the verification service provider each already possess the SSN. The verification service merely affirms whether the SSN and other identification information provided by the customer to the financial institution match the information in the provider's database. If the SSN itself is not being exchanged for something of value, then the transaction would not be considered a sale or purchase of the SSN.

With respect to the exemption for activities of consumer reporting agencies for purposes described in section 604(a) of FCRA, sales and purchases of SSNs by CRAs that are in furtherance of those specified purposes (such a sale or purchase of an SSN as part of authenticating a customer's identity in order to ensure that he or she receives the correct report, or compiling information used in providing a consumer report) are not intended to constitute a prohibited sale or purchase under the bill.

The exemption for tax compliance recognizes that SSNs are also used in tax administration, and that tax law extends to a wide variety of transactions including, for example, payment of mortgages where interest is tax-deductible, securities sales, and even car loans, where if there is a default and the creditor writes off the loss, the value of the discharged debt must be reported for tax purposes.

In addition, during the course of the Subcommittee on Social Security's consideration of the bill, the Federal Deposit Insurance Corporation (FDIC) and some financial institutions expressed concern that the bill's restrictions on sale and purchase of SSNs could be interpreted to impede the FDIC's resolution or liquidation of

failed insured depository institutions, or other business mergers and acquisitions. The bill's language specifying that "sell" or "purchase" does not include the sale, lease, merger, transfer, or exchange of a trade or business is intended to make clear that the FDIC may share SSNs in carrying out its responsibilities, and SSNs may be conveyed as part of the merger, acquisition, etc. of a business.

With respect to the exception for research advancing the public good, the intent is to preserve the government's ability to conduct scientific, epidemiological, and social scientific research that would benefit the public. It is not intended to facilitate private commercial research for product or service development or marketing. In the case of non-publicly sponsored or funded research advancing the public good, the Commissioner would have the ability to authorize SSN sale and purchase where appropriate, under its general regulatory authority. In the case of research involving medical information on individuals, it is expected that the Commissioner will only authorize sale of SSNs in strict compliance with Federal rules and regulations on the privacy of medical information.

With respect to the exception for affirmative written consent of the individual, the intent is to enable individuals to authorize the sale or purchase of their own SSNs if they determine it is in their own best interest. Businesses and others soliciting such consent from the individual must explain clearly and understandably what giving consent would entail and the uses that might be made of the individual's SSN. Preferably, the explanation and solicitation of consent would be a distinct document or other communication separate from other explanations or solicitations from the business or other persons. The terms of consent, and the explanation of the right to refuse consent or to limit the SSN's exchange solely to a specific transaction, should not be obscured by other explanations, authorizations, solicitations or other text that might be included in the same document. No individual should be obligated to provide consent; however, businesses and others may provide an explanation of the advantages and disadvantages (with equal prominence given to both) of providing versus refusing consent.

With respect to the exception permitting the Commissioner to authorize additional exceptions to the general prohibition on SSN sale, purchase, and display to the general public, for the same reasons discussed under section 2 of the bill, the expectation is that this authority would be used extremely judiciously and only when there are no other reasonable alternative measures that could attain the same objective.

For the same reasons discussed under section 3, the bill would prohibit display of another individual's SSN on any check issued for payment or documents accompanying the checks because identity thieves may gain access to personal information, including SSNs, by rifling through trash for discarded documents.

Section 2 of the bill would prohibit government agencies from selling or displaying to the general public SSNs they require individuals to disclose to the government. However, many of the SSNs that appear in government records—particularly court records, documents from attorneys, title companies, or other businesses and individuals—are the result of including a person's SSN on papers submitted to the court for the sake of convenience. Government

agencies do not have the resources to comb through innumerable documents searching for such “incidental” inclusion of SSNs. As a result, an individual’s SSN could be displayed to the public without the government record-keeper realizing it. Therefore, to prevent inadvertent sale or display of SSNs by government agencies, the bill would prohibit the submission of the SSN to government agencies absent the government agency’s requiring that the number be submitted or the individual’s written consent. Thus, this provision does not prohibit submission of another individual’s SSN for the purpose of applying for benefits on their behalf, such as when a parent files an application on behalf of a child.

Also, for the same reasons discussed under section 4, the bill would prevent private sector employers and those providing employee benefits from displaying an individual’s full or partial SSN on any identification card or tag issued to the employee or an employee’s family member. In addition, the bill would prevent businesses from displaying full or partial SSNs on cards or tags used to access goods and services. Individuals who must carry such cards and tags with their SSNs are at greater risk of identity theft should their wallets or purses be stolen or lost. According to an FTC-sponsored survey, 14 percent of identity theft victims said their personal information was obtained from a lost or stolen wallet or checkbook. This provision is not intended to prevent inclusion of encrypted SSNs (those that are transformed by a secret code to appear as other than the nine-digit number assigned by the Commissioner of Social Security when read or otherwise accessed by unauthorized parties).

The restrictions on private sector sale, purchase, and display to the general public of SSNs would not apply to the SSNs of deceased persons. This is because the sale and public availability of information on deceased individuals is necessary to prevent fraud. As mentioned in the discussion under section 2 of the bill, the SSA DMF is used by both public and private sector entities to prevent fraud and comply with the USA PATRIOT Act. By methodically running financial, credit, payment and other applications against the DMF, the financial community, insurance companies, security firms and State and local governments are better able to identify and prevent identity fraud. The USA PATRIOT Act requires an effort to verify the identity of customers, including procedures to verify customer identity and maintaining records of information used to verify identity.

As discussed under section 2, this bill is intended to serve as a floor of protection for SSNs and is not intended to override SSN protections in Federal or State law or regulations in effect to the extent they provide greater restrictions. For example, this bill is not intended to enable SSN sale, purchase, or display to the general public by health providers that would otherwise be prohibited under the HIPAA Privacy Rule.

EFFECTIVE DATE

Initial final regulations to carry out the provisions would have to be issued by the Commissioner or any other agency to which the Commissioner delegates authority within 18 calendar months after the date of enactment. The provisions would take effect one year after issuance of initial final regulations. The prohibition on public

display of SSNs would only apply with respect to records generated after the effective date of the regulations. The temporary exemption to allow purchase, sale and display of the last four digits of the SSN would expire two years after the effective date of the initial final regulations.

Sec. 9. New criminal penalties for misuse of Social Security account numbers

CURRENT LAW

Section 208 of the Social Security Act provides criminal penalties for fraudulently obtaining an SSN from SSA or the misuse of an SSN. In such cases, section 208 specifies that persons shall be guilty of a felony and upon conviction shall be fined under Title 18, United States Code (up to \$250,000 for an individual and up to \$500,000 for an organization) and/or imprisoned for up to five years.

In addition, depending upon the facts, certain sections under Title 18 of the United States Code are applicable to the misuse of SSNs, including 18 U.S.C. § 1028(a)(7), the “Identity Theft and Assumption Deterrence Act of 1998” (P.L. 105–318), which prohibits the knowing transfer or use of another person’s SSN without lawful authority. The “Internet False Identification Prevention Act of 2000” (P.L. 106–578) closed some loopholes in the “Identity Theft and Assumption Deterrence Act of 1998” by prohibiting the transfer of a false identification document by electronic means, including on a template or computer file or disk.

Lastly, the “Identity Theft Penalty Enhancement Act” (P.L. 108–275) establishes penalties for aggravated identity theft. The law prescribes sentences, to be imposed in addition to the punishments provided for the related felonies, of: (1) two years’ imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations; and (2) five years’ imprisonment for knowingly taking such action with respect to a means of identification or a false identification document during and in relation to specified felony violations pertaining to terrorist acts. The law also prohibits a court from: (1) placing any person convicted of such a violation on probation; (2) reducing any sentence for the related felony to take into account the sentence imposed for such a violation; or (3) providing for concurrent terms of imprisonment for a violation of this Act and a violation under any other Act.

The law also expands the existing identify theft prohibition to: (1) cover possession of a means of identification of another with intent to commit specified unlawful activity; (2) increase penalties for violations; and (3) include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism. Finally, the law modifies provisions regarding embezzlement and theft of public money, property, or records to provide for combining amounts from all the counts for which the defendant is convicted in a single case for purposes of determining which penalties apply.

EXPLANATION OF PROVISION

The bill would expand the types of SSN misuse to which criminal penalties apply and would establish a two-tier penalty structure that creates new categories of misdemeanor and felony violations.

The bill would provide for criminal misdemeanor penalties, which are subject to fines under Title 18 of the United States Code and/or imprisonment for up to one year. It would apply to government employees and private sector individuals who: (1) display SSNs on checks issued for payment; (2) display SSNs on identification cards; or (3) violate the uniform truncation standards. It would apply to private sector entities who communicate another person's SSN to a government entity when not required. It would apply to government employees who display SSNs on drivers' licenses and vehicle registrations. Finally, the misdemeanor penalty would apply to the knowing unlawful possession of another person's SSN card or a fraudulent SSN card with an intent to use the SSN in furtherance of a violation of law.

The bill would also provide for criminal felony penalties, which are subject to fines under Title 18 of the United States Code and/or imprisonment for up to five years. The felony provision would apply to individuals who obtain or use an SSN with intent to harass, harm or physically injure another person.

The bill would also create enhanced penalties for repeat offenders and for violations committed to facilitate drug trafficking or terrorism.

Finally, the bill would provide for both criminal misdemeanor and felony penalties for certain violations. These penalties apply to persons who sell their own SSN with the intent to deceive, or assist an individual in acquiring an additional SSN for a fee. It would apply to government entities that: (1) sell or display the SSN in violation of section 2 of the bill; (2) give inmates access to SSNs; or (3) fail to protect SSNs as required under section 6 of the bill. It would also apply to private sector entities who: (1) sell, purchase or display the SSN in violation of section 8 of the bill; or (2) fail to protect the confidentiality of the SSN in violation of section 8 of the bill. These violations would be subject to a felony charge if they are committed under false pretenses, or for commercial advantage, personal gain, or malicious harm.

REASON FOR CHANGE

Identity theft often begins with the misuse of an SSN. While advances have been made to prosecute those individuals who assist another person to improperly acquire an additional SSN or a number that purports to be an SSN, SSA Inspector General and the Department of Justice have continued to encounter some problems, for example in prosecuting individuals who operate over the Internet or at a flea market. It is appropriate to close loopholes to prevent individuals assisting another person to improperly acquire an additional SSN or a number that purports to be an SSN. In addition, it is appropriate to establish penalties for those who violate the prohibitions on sale, purchase and display to the general public established under this bill.

In addition, the SSA Inspector General has investigated individuals who have sold or transferred their own SSN to a third person

with intent to deceive and has encountered problems in the prosecution. While such an individual may potentially be prosecuted under the criminal statutes involving conspiracy or aiding and abetting, because of the gravity of SSN misuse, it is appropriate to address this problem head on and provide criminal penalties when an individual sells or transfers his or her own SSN with intent to deceive.

With respect to violations that are punishable as either a misdemeanor or a felony, this two-tier structure is intended to provide prosecutors with additional flexibility in charging violators. The “aggravating” circumstances under which a violation would be a felony rather than a misdemeanor are drawn from the HIPAA Privacy Rule, which also contains a multi-tiered structure of penalties.

EFFECTIVE DATE

The criminal penalties would apply to violations that occur after enactment, except for violations of prohibitions created under this bill. In such cases, the criminal penalties would apply to violations that occur on or after the applicable effective dates.

Sec. 10. Extension of civil monetary penalty authority

CURRENT LAW

Section 1129 of the Social Security Act authorizes the Commissioner to impose civil monetary penalties and assessments on any person who makes a false statement or representation of a material fact, or omits a material fact while providing a statement, for use in determining eligibility for Social Security or SSI benefits or the benefit amount. The Commissioner may impose a civil monetary penalty of up to \$5,000 for each violation, and an assessment of up to twice the amount of benefits or payments paid as a result of such violation.

Currently, an individual who improperly obtains an SSN from SSA or misuses another person’s SSN is not subject to civil monetary penalties and assessments under section 1129, except in cases of SSN misuse related to the receipt of Social Security or SSI benefits.

EXPLANATION OF PROVISION

The bill would expand the types of activities to which civil monetary penalties and assessments apply. Specifically, it would authorize the Commissioner to impose (in addition to any other penalties that may apply) civil monetary penalties and assessments on persons who: (1) use an SSN obtained through false information; (2) falsely represent an SSN to be their own; (3) with intent to deceive, alter an SSN card; (4) buy or sell an SSN card or a card purported to be an SSN card; (5) counterfeit an SSN card; (6) disclose, use or compel the disclosure of the SSN of any person in violation of any Federal law; (7) provide false information to obtain an SSN; (8) offer to acquire, for a fee, an additional SSN for an individual; (9) disclose, sell or transfer a person’s own SSN with intent to deceive; (10) knowingly possess an SSN unlawfully or possess an altered or counterfeited SSN with the intent to commit a felony; (11) as a government officer, violate prohibitions on display of SSNs on drivers’ licenses, sale and display of SSNs, displaying SSNs on checks and

identification cards, inmate access to SSNs, security and protection of SSNs, or truncation standards; (12) as a bankruptcy trustee, sell or display SSNs, display SSNs on checks, fail to protect the confidentiality of SSNs, or violate truncation standards; (13) sell, purchase or display SSNs, or violate truncation standards; or (14) as an SSA employee, violate section 11 of the bill (relating to fraudulent issuance of SSNs).

REASON FOR CHANGE

SSN misuse, not related to the determination of eligibility for, or the amount of, Social Security or SSI benefits, can also result in considerable costs for the government, the private sector, and individuals who are victims of fraud. In many cases, the costs of SSN misuse extend beyond monetary losses.

The SSN is a valuable commodity today for criminals. As the Subcommittee on Social Security has heard in testimony, the use of the SSN has grown so that it is interwoven into many aspects of every day life. It has become the de facto national identifier, used as a “breeder document” to obtain a driver’s license or a credit card, open a bank account or secure a loan.

Because of the prevalence of the use of the SSN in society and the gravity of SSN misuse, it is appropriate to provide for civil monetary penalties and assessments for violations of the law relating to SSN misuse in general.

EFFECTIVE DATE

The civil monetary penalties would apply to violations that occur after enactment, except with respect to violations of prohibitions created under this bill. In such cases, the civil monetary penalties would apply to violations that occur on or after the applicable effective date.

Sec. 11. Criminal penalties for employees of the Social Security Administration who knowingly and fraudulently issue Social Security cards or Social Security account numbers

CURRENT LAW

SSA employees who fraudulently sell SSNs to third parties may be tried under a number of criminal statutes, including but not limited to 18 U.S.C. 371 (conspiracy) and 18 U.S.C. § 641 (theft of government property).

EXPLANATION OF PROVISION

The bill would provide for criminal penalties for SSA employees (including contract workers, State Disability Determination Service workers and volunteers in an SSA facility) who knowingly and fraudulently sell or transfer SSNs or Social Security cards, with the penalty based on the number of SSNs or Social Security cards fraudulently issued, as follows: (1) up to 50 SSNs or cards: up to 5 years imprisonment; (2) 51 to 100 SSNs or cards: up to 10 years imprisonment; or (3) 101 or more SSNs or cards: up to 20 years imprisonment.

REASON FOR CHANGE

Crimes of fraud against the integrity of the SSN are of great concern because of the far-reaching implication such crimes have upon the integrity of SSA, the potential impact on innocent individuals due to identity theft, and possible misuse of SSNs in terrorist activities. This is especially true when the crime is perpetrated, at least in part, by an SSA employee. SSA employees issuing SSNs are in a position of trust. When this trust is violated, the effect on SSA's programs and operations and on the public in general can be devastating. Fortunately, the number of SSA employees taking part in these crimes is small, but participation in such crimes by any SSA employee to any extent cannot be tolerated.

SSA and the SSA Inspector General are concerned that current laws do not provide an adequate deterrent to SSA employees tempted to facilitate these crimes. In several recent investigations involving SSA employees, the employee when caught has received little, if any, prison time though the employee may have fraudulently issued hundreds of SSNs. The Committee is concerned because the SSNs issued have usually not previously been issued to anyone else. Even a thorough credit check would not show this SSN to be fraudulent. This could allow a criminal to more easily assimilate into our society. Therefore, it is appropriate to provide for enhanced criminal penalties for SSA employees who abuse their position of trust and assist in the fraudulent issuance of SSNs.

EFFECTIVE DATE

The penalties would apply to violations that occur on or after enactment.

Sec. 12. Enhanced penalties in cases of terrorism, drug trafficking, crimes of violence, or prior offenses

CURRENT LAW

Sections 208, 811 and 1632 of the Social Security Act (regarding Social Security benefits, Special Benefits for Certain World War II Veterans and SSI benefits, respectively) provide that persons who willingly and knowingly commit fraud shall be guilty of a felony and upon conviction shall be fined under Title 18, United States Code, and/or imprisoned for up to five years.

Examples of violations to which penalties apply include making false statements or representations of fact to obtain benefits or increase benefit payments; failing to disclose an event that affects an individual's initial or continued right to receive benefits; and engaging in various types of SSN misuse or fraud (such as using an SSN obtained on the basis of false information; falsely representing an SSN to be one's own with intent to deceive; buying or selling an SSN card; counterfeiting an SSN card; or disclosing, using or compelling the disclosure of the SSN of any person in violation of any Federal law).

Penalties apply to violations committed by individuals (or organizations) acting in the capacity of a representative payee (or prospective representative payee) for a beneficiary other than the individual's spouse. If the court determines that the violation also in-

cludes willful misuse of funds, the court may require full or partial restitution of funds to the beneficiary.

EXPLANATION OF PROVISION

The bill would enhance criminal penalties under sections 208, 811 and 1632 of the Social Security Act with respect to (a) repeat offenders and (b) violations committed to facilitate a drug trafficking crime, a crime of violence, or an act of international or domestic terrorism.

Specifically, the bill would provide for: (1) fines and/or imprisonment for up to five years for first offenders; (2) fines and/or imprisonment for up to 10 years for repeat offenders; (3) fines or imprisonment for up to 20 years for persons convicted of violations for the purpose of facilitating a drug trafficking crime or a crime of violence against persons; and (4) fines or imprisonment for up to 25 years for persons convicted of violations for the purpose of facilitating an act of international or domestic terrorism.

REASON FOR CHANGE

The expanded use of the SSN in today's society has made it a very valuable commodity for criminals. As the Subcommittee on Social Security has heard in several hearings, the SSN is considered a prime "breeder document," a valuable commodity used to obtain a driver's license or credit card, as well as open a bank account or obtain a loan. In addition to being a lynchpin for identity theft crimes, the SSN also assists terrorists in assimilating into our society and avoiding detection.

The integrity of the SSN is vital. Its importance in both identity theft and homeland security is universally recognized. Providing new, enhanced, structured penalties appropriately reflects the vital importance of the SSN and the commitment of the Congress, SSA and the SSA Inspector General to its protection.

EFFECTIVE DATE

The penalties would apply to violations that occur after enactment.

Sec. 13. Regulatory and enforcement authority with respect to misuse of the Social Security account number

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

The bill would direct the Commissioner of Social Security to issue regulations regarding the sale, purchase, or display to the general public of SSNs and to provide an opportunity for public comment on regulations in accordance with the "Administrative Procedure Act" (P.L. 79-404). The Commissioner would be required to consult with the Attorney General of the United States, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Secretary of the Treasury, the Federal Trade Commission, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Board of Governors of the Federal Reserve

System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Securities and Exchange Commission, State Attorneys General and representatives of the State insurance commissioners as designated by the National Association of Insurance Commissioners.

When authorizing the sale, purchase, or display of SSNs for law enforcement or national security purposes, the Commissioner would be required to find that the sale, purchase or display would serve a compelling public interest that cannot reasonably be served through alternative measures, and would not pose an unreasonable risk of identity theft, or harm to an individual.

The Commissioner would be able to authorize the sale, purchase, or display to the general public of SSNs for purposes other than law enforcement or national security, only after considering whether the authorization serves a compelling public interest and considering the costs and benefits to the general public, businesses, commercial enterprises, non-profit associations, and governments. If the Commissioner authorizes the sale, purchase, or display to the general public of SSNs, he or she would be required to impose restrictions and conditions to reduce the likelihood of fraud and crime and to prevent an unreasonable risk of identity theft or bodily, emotional or financial harm to individuals.

The Committee intends that any exceptions made under this section of the bill by SSA, or any other agency to which rulemaking authority is delegated, would conform to the purposes of this Act: to prevent SSN misuse and identity theft by reducing the availability of SSNs in documents obtainable by identity thieves. The Committee expects SSA or other agencies to consider an exception to allow the sale or purchase of SSNs to the extent necessary to prevent fraud in financial transactions initiated by a consumer. FCRA requires information sellers to comply with certain consumer protections if they are compiling and selling consumer information for determining consumer eligibility for credit, employment, insurance, licensing and other government benefits, or for any other legitimate business need in transactions initiated by the consumer. Any further exceptions promulgated by an agency regarding fraud should be tailored narrowly to the purpose of detecting and investigating fraud in violation of civil or criminal statutes and/or regulations or identity theft. Furthermore, they should be written in such manner that does not allow sellers or buyers of SSNs to circumvent the requirements and applicability of FCRA by selling or buying SSNs for purposes already covered by the exception relating to section 604(a) of FCRA, but doing so in a way that does not subject them to FCRA's regulations. Finally, SSNs sold or bought under such an exception should be restricted from use for any secondary purposes not related to the transaction.

The Commissioner would have the authority to delegate rulemaking to other Federal agencies, as appropriate. The Commissioner would delegate this authority to any agency or instrumentality which would otherwise have regulatory authority over such matters. The Commissioner would also facilitate coordination and consistent rulemaking and enforcement by other agencies.

With respect to any regulation issued under the Commissioner's general authority to provide for an exemption from the bill's prohibition on sale, purchase or display, such regulations would expire

five years after their effective dates. One year prior to the expiration of the regulations, GAO would be required to conduct a review of the efficacy of the regulations and the extent to which such regulations are consistent with and in furtherance of the purpose of this bill. The Commissioner may use the results of the review to issue new regulations consistent with the guidelines provided in this bill, as listed above.

This bill would authorize any State Attorney General to bring a civil action in a United States district court to enforce compliance with the statute and related regulations by State and local governments and the private sector. An Attorney General may bring an action when he or she has reason to believe that an interest of the State's residents is threatened or adversely affected by State or local governments or private entities that violate this statute. Attorneys General may seek to enjoin the act or practice, enforce compliance with the regulation, obtain limited civil penalties of \$11,000 per violation not to exceed a total of \$5,000,000, or other appropriate legal and equitable relief.

In addition, this bill would give individuals limited standing to sue a Federal agency for violations of prohibitions and requirements established under this bill. An individual would be allowed to sue a Federal agency in a United States district court only if the individual's SSN was involved in the violation. The individual would only be allowed to sue for injunctive relief and actual damages, and could recover attorney's fees and costs of the action.

REASON FOR CHANGE

The SSN is widely used throughout the public and private sectors. Some uses are authorized or required under law, others are to facilitate data-matching and record-keeping, and still others are simply for the sake of convenience. The development of coordinated regulations regarding SSN sale, purchase, and display across such diverse agencies and businesses makes it necessary to centralize regulatory authority with SSA (which is responsible for issuing SSNs).

In addition, to address concerns that the limited statutory list of exceptions does not enumerate all instances in which the sale, purchase, and display of SSNs may be essential and irreplaceable for government and business transactions, the Commissioner would be given authority to authorize the sale, purchase or display to the general public of SSNs. The bill provides guidelines to ensure SSNs are exchanged only when there is no other alternative that could reasonably accomplish the objective, and with due consideration for the unintended and potentially harmful consequences to individuals, government agencies, and businesses that may result.

SSNs are used widely in government and the private sectors for many diverse purposes, and in industry sectors that maybe overseen by their own regulatory bodies, such as the financial services industry. To most effectively issue regulations that address these various concerns, the Commissioner has the authority to delegate, by regulation, rulemaking and enforcement of these provisions to other agencies. Agencies tasked with this authority may be better suited to issue and enforce regulations within the domain of their jurisdiction and expertise.

This bill would encourage private sector entities to change their business practices to reduce reliance on the SSN. As business models change and as research progresses to employ authentication devices other than the SSN, the regulations should be reviewed and revised as appropriate to ensure that the regulations meet the goals of this bill. To ensure that the regulations authorized by the Commissioner are consistent with the goals of this statute, any final regulation issued under the regulator's general exemption authority will expire five years after its effective date. This provision ensures that regulations issued under this bill will undergo regular and consistent reviews to ensure that the regulations effectively and functionally limit the sale, purchase and display of the SSN in the private sector and discourage excessive use of and reliance on the SSN. The GAO assessment would also provide Congress and regulators the opportunity to review the effectiveness of regulations granting permissible sale, purchase and display of SSNs and the extent to which they are consistent with the purpose of this bill.

State Attorneys General would assist in enforcement efforts under this bill through civil actions. As in other areas of Federal law, State Attorneys General can support compliance with Federal law by supplementing the enforcement resources of Federal agencies, and they are well-positioned to be aware of unlawful acts and practices in their states. State Attorneys General would be required to inform SSA and the U.S. Attorney General of any enforcement actions they intend to undertake, and State action would be precluded where the Federal government has initiated a criminal proceeding.

Federal agencies, like State and local governments, have unique and frequent access to SSNs. Federal agencies are commonly required by law to use the SSN as an identifier and often use the SSN for record-keeping purposes in the administration of government benefits. Therefore, it is just as important for Federal agencies to protect the confidentiality of the SSN, as well as limit its sale and display, as it is for State and local government agencies. This bill would strengthen enforcement against Federal agencies that are not in compliance with the bill by allowing individuals to take action against Federal agencies in limited situations where they may be harmed.

EFFECTIVE DATE

The regulatory authority would be effective upon enactment.

Sec. 14. Study on feasibility of banning Social Security account number as an authenticator

CURRENT LAW

No provision.

EXPLANATION OF PROVISION

This bill would direct the Commissioner of Social Security to enter into an arrangement with the National Research Council for the Council to conduct a study to determine the extent to which SSNs are used as a primary means of authenticating identity and the extent to which SSNs are used for verification in commercial transactions. It would also require the Council to determine the

feasibility of prohibiting use of the SSN as an authenticator and possible alternatives to the SSN for verification purposes and uses in authenticating identity.

REASON FOR CHANGE

Identity theft is facilitated by the fact that the SSN is used by business and governments as an identifier, to distinguish one person from another, as well as an authenticator, or evidence that a person is who they say they are. This insecure practice is analogous to someone using the same element for their user ID as for their password in order to gain access to a computer network. At a hearing before the Subcommittee on Social Security, a witness for the Association for Computing Machinery explained that knowledge of an SSN is not sufficient to reliably authenticate any party in a transaction, but this use is commonplace.

While some businesses have begun to discontinue the use of SSNs as passwords on their phone and online accessible networks, many businesses still depend on the SSN as an authenticator of identity. This practice continues to make the SSN a primary instrument of identity theft, since once the SSN is acquired, access to an individual's sensitive information is easily obtainable. When the SSN is used as a password, a cancelled check and an SSN can provide a criminal sufficient information to gain access to a person's account online or by phone.

This provision authorizes the Commissioner to arrange for the National Research Council to conduct a study on the prevalence of this practice and whether it can be reduced. The Committee also intends that the examination of possible alternatives to SSNs for verification purposes and uses in authenticating identity include the last four digits of the SSN.

EFFECTIVE DATE

Under its arrangement with the Commissioner, the Council would be required to submit a report to the Commissioner and to each House of the Congress no later than one year after the effective date of the initial final regulations issued under section 2 of the bill (that is, three and one-half years after enactment).

III. VOTES OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the following statements are made concerning the vote of the Committee on Ways and Means in its consideration of the bill, H.R. 3046.

MOTION TO REPORT THE BILL

The bill, H.R. 3046, as amended, was ordered favorably reported by a rollcall vote of 41 yeas to 0 nays (with a quorum being present). The vote was as follows:

Representatives	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Rangel	X	Mr. McCrery	X
Mr. Stark	X	Mr. Herger	X
Mr. Levin	X	Mr. Camp	X
Mr. McDermott	X	Mr. Ramstad	X
Mr. Lewis (GA)	X	Mr. Johnson	X

Representatives	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Neal	X	Mr. English	X
Mr. McNulty	X	Mr. Weller	X
Mr. Tanner	X	Mr. Hulshof	X
Mr. Becerra	X	Mr. Lewis (KY)	X
Mr. Doggett	X	Mr. Brady	X
Mr. Pomeroy	X	Mr. Reynolds	X
Mrs. Tubbs Jones	X	Mr. Ryan	X
Mr. Thompson	X	Mr. Cantor	X
Mr. Larson	X	Mr. Linder	X
Mr. Emanuel	X	Mr. Nunes	X
Mr. Blumenauer	X	Mr. Tiberi	X
Mr. Kind	X	Mr. Porter	X
Mr. Pascrell	X				
Ms. Berkley	X				
Mr. Crowley	X				
Mr. Van Hollen	X				
Mr. Meek	X				
Ms. Schwartz	X				
Mr. Davis (AL)	X				

IV. BUDGET EFFECTS OF THE BILL

A. COMMITTEE ESTIMATE OF BUDGETARY EFFECTS

In compliance with clause 3(d)(2) of rule XIII of the Rules of the House of Representatives, the following statement is made concerning the effects on the budget of this bill, H.R. 3046, as amended and reported: The Committee agrees with the estimate prepared by the Congressional Budget Office (CBO), which is included below.

B. STATEMENT REGARDING NEW BUDGET AUTHORITY AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee states that H.R. 3046 does not include any new budget authority or tax expenditures.

C. COST ESTIMATE PREPARED BY THE CONGRESSIONAL BUDGET OFFICE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, requiring a cost estimate prepared by the Congressional Budget Office, the following report by CBO is provided:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 30, 2007.

Hon. CHARLES B. RANGEL,
*Chairman, Committee on Ways and Means,
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3046, the Social Security Number Privacy and Identity Theft Prevention Act of 2007.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Sheila Dacey (for fed-

eral costs), Lisa Ramirez-Branum (for the state and local impact), and Paige Piper-Bach (for the private-sector impact).

Sincerely,

ROBERT A. SUNSHINE
(For Peter R. Orszag, Director).

Enclosure.

H.R. 3046—Social Security Number Privacy and Identity Theft Prevention Act of 2007

Summary: H.R. 3046 would provide new safeguards for the use of Social Security numbers (SSNs) and penalties for SSN misuse. The bill would:

- Bar the sale, purchase, or display of the SSN in both the public and private sectors, with certain exceptions;
- Prohibit the display of SSNs (including magnetic strips or bar codes that contain them) on government checks, employer-issued identification cards or tags, and Medicare cards;
- Require government and private entities to limit access to SSNs and assure that they have safeguards to prevent breaches of confidentiality;
- Require the Government Accountability Office (GAO) and the Social Security Administration (SSA) to study the effectiveness of regulations related to this bill and the feasibility of additional safeguards; and
- Create or expand civil and criminal penalties for SSN misuse.

Enacting H.R. 3046 could affect direct spending and revenues, but CBO estimates that any such effects would not be significant. Complying with the bill's standards would cause federal agencies to incur additional administrative expenses. Those costs—which CBO estimates at \$43 million over the 2008–2012 period—would generally come from agencies' salary and expense budgets, which are subject to annual appropriation.

H.R. 3046 contains a number of intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), including limitations on the sale, display, and use of SSNs by state, local, and tribal governments. CBO estimates that the aggregated costs of complying with those mandates would probably exceed the threshold established in UMRA for intergovernmental mandates (\$66 million in 2007, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

H.R. 3046 also would impose private-sector mandates as defined in UMRA. CBO cannot determine whether the aggregate direct costs of complying with those mandates would exceed the annual threshold for private-sector mandates established by UMRA (\$131 million in 2007, adjusted annually for inflation) because such costs would depend on the specific regulations that would be issued under the bill.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 3046 is shown in the following table. The costs of the legislation fall primarily in budget functions 050 (national defense), 570 (Medicare), 650 (Social Security), and 700 (veterans benefits and services), but could affect numerous other budget functions as well. As explained below, CBO cannot estimate some po-

tential costs in cases where agencies do not yet know how they would implement certain provisions.

Basis of estimate: Federal agencies already comply, or are moving to comply, with most requirements of H.R. 3046. The bill's budgetary effects would stem from a few provisions that would change agencies' practices or assign new enforcement responsibilities. For this estimate, CBO assumes that the bill will be enacted in the fall of 2007.

Spending subject to appropriation

CBO estimates that implementing H.R. 3046 would cost \$43 million over the 2008–2012 period, assuming that the necessary amounts will be appropriated near the start of each fiscal year and that spending will follow historical patterns for similar activities.

	By fiscal year, in millions of dollars—				
	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION ¹					
Prohibiting Display of SSN on Government ID Tags or Cards:					
Estimated Authorization Level	16	*	6	10	10
Estimated Outlays	11	5	5	10	10
Regulation and Enforcement:					
Estimated Authorization Level	1	*	*	*	*
Estimated Outlays	1	*	*	*	*
Studies:					
Estimated Authorization Level	*	*	1	*	*
Estimated Outlays	*	*	1	*	*
Total Changes:					
Estimated Authorization Level	17	*	7	10	10
Estimated Outlays	12	5	6	10	10

¹ Enacting H.R. 3046 also could affect direct spending and revenues, but CBO estimates that any such effects would not be significant. Note.—SSN = Social Security number; * = less than \$500,000.

Prohibiting Display of SSN on ID Tags or Cards. The bill would prohibit government agencies from displaying SSNs (including magnetic strips or bar codes that contain them) on certain government-issued identification cards or tags. Government agencies could not display an SSN on employee, student, or patient identification tags or on Medicare cards. The requirement would affect cards or tags issued one year after the date of enactment, or in the case of Medicare cards, two and one-half years after enactment. In total, CBO estimates that implementing the provision would cost \$41 million over the 2008–2012 period, subject to the availability of appropriated funds. The estimated costs to major agencies are described below.

Department of Defense. The Geneva Convention calls for military personnel to have a number displayed on their identification cards, and the Department of Defense (DoD) has chosen to use the SSN. Under the bill, DoD would have to revamp its records and cards to use another unique identifier for 6.5 million personnel. Based on information from DoD, CBO estimates that implementing this provision would cost \$2 million over the 2008–2009 period, assuming the availability of appropriated funds. Subsequent ongoing costs would be negligible.

Veterans Affairs. The bill would prohibit the Department of Veterans Affairs (VA) from using a patient's SSN on the identity cards or tags used by its medical facilities. Based on information from the department, CBO estimates that it would cost \$9 million to make

the necessary changes to its computer systems. In addition, VA would plan to replace older, but still valid, cards at a cost of \$5 million. Assuming appropriation of the estimated amounts, CBO estimates that VA would spend \$10 million in 2008 and \$4 million in 2009 to implement the requirement.

Medicare. The Medicare program uses the SSN as the basis of its Health Insurance Claim Number and displays that number on the Medicare card. Over 42 million Medicare beneficiaries have a Medicare card and several million new beneficiaries are added to the Medicare rolls annually.

Under H.R. 3046, CBO assumes that the Centers for Medicare and Medicaid Services (CMS) would continue to use the SSN-based claim number to process and pay claims, but would remove the number from the Medicare card. CBO estimates that CMS would increase spending on beneficiary outreach and provider education in 2009, but that such costs would total less than \$500,000. In 2010, CMS would begin to issue Medicare cards that do not display a claim number to new enrollees and beneficiaries who request a replacement card. CBO estimates that it would cost CMS \$5 million in 2010, and \$10 million in each of fiscal years 2011 and 2012 to implement the changes. The bulk of the new costs would stem from handling additional inquiries from beneficiaries and providers who would be confused by the change. Based on information provided by CMS and SSA, CBO estimates that up to 10 million beneficiaries would be affected by the change annually and that 10 percent of them would contact the agencies with questions. In addition, the agencies would incur small costs for replacement cards for beneficiaries who request them.

CMS could choose to adopt a different strategy and change the claim number so that it is no longer based on the SSN. That strategy would require changes to CMS computer systems that would be more expensive than removing the claim number from the card.

Regulation and Enforcement. The Social Security Administration would take the lead in drafting regulations to govern compliance with the new law in both the public and private sectors and would prosecute violations. CBO estimates the agency's new tasks would cost \$1 million in 2008, assuming the availability of appropriated funds. Costs would be less than \$500,000 in other years.

Some additional costs are likely, however. H.R. 3046 would require all federal agencies to demonstrate to SSA that they allow access only to employees who need SSNs to carry out their statutory responsibilities and have safeguards to prevent unauthorized access and breaches of confidentiality. That provision would apply to all SSNs in the agencies' possession, including paper records. Its implications for contractors (who handle key responsibilities, especially in the areas of welfare and child support enforcement) are unclear. According to GAO, every federal agency uses the SSN in some way. CBO cannot estimate the cost of this provision to SSA or to other agencies because it would depend on SSA's approach to implementing the bill's requirements.

Studies. H.R. 3046 would authorize two new studies. It would require the Commissioner of SSA to contract with the National Research Council to study the feasibility of banning the SSN as a primary means of authenticating identity. It also would require GAO to conduct a review of the effectiveness of the regulations issued

pursuant to this legislation and report on the results. CBO estimates that the combined cost of the studies would total about \$1 million in 2010, but would be less than \$500,000 in other years.

Direct spending and revenues

Implementing H.R. 3046 could affect direct spending and revenues, but CBO estimates that any such effects would not be significant.

Civil Actions. H.R. 3046 would permit individuals to sue the federal government in federal district court for violations relating to the privacy of SSNs. Under the bill, if a plaintiff prevailed in such lawsuit, payment for damages and attorneys fees would be made by the Treasury's Judgment Fund. Payments from that fund are considered increases in direct spending. Considering current governmentwide practices regarding privacy and identity theft, CBO estimates that enacting H.R. 3046 would lead to an increase in the number of civil actions against the government and an increase in direct spending to pay claims, but that such costs would likely be less than \$500,000 in each year.

Civil and Criminal Penalties. H.R. 3046 could increase federal revenues and direct spending as a result of the collection of additional civil and criminal penalties assessed for misuse of SSNs. Collections of civil penalties are recorded in the budget as revenues and deposited in the Treasury. Collections of criminal penalties are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO estimates that any additional revenues and direct spending would not be significant because of the relatively small number of cases likely to be involved.

Child Support Enforcement. Requiring government agencies to remove SSNs from checks could raise administrative costs to the child support enforcement (CSE) program and/or delay distribution of collections. Many states currently use SSNs as their primary identifier when distributing child support, and the federal government covers the bulk of states' costs for administering CSE. CBO expects that the bill's requirement would have an additional cost to the federal government but that cost would be small because of the widespread and increasing use of electronic funds transfers to distribute payments rather than checks.

Estimated impact on state, local, and tribal governments: H.R. 3046 contains a number of intergovernmental mandates as defined in UMRA. Specifically, the bill would restrict or prohibit government agencies from:

- Selling or displaying SSNs that have been disclosed to the agency because of a mandatory requirement (applies only to documents issued after the requirements become effective);
- Displaying SSNs on checks or check stubs;
- Placing SSNs on student or employee identification cards or coding them into magnetic strips or bar codes on those documents; and
- Allowing prisoners access to SSNs of other individuals.

The bill also would require state and local governments to restrict access to SSNs and their derivatives to employees whose access is essential to effective administration of programs. In addition, the governments would have to implement safeguards to pre-

clude unauthorized access to SSNs and their derivatives and to protect individual confidentiality.

While state and local governments have taken steps to reduce the use of SSNs, many continue to use them for a variety of purposes. Based on information from GAO and from state and local officials, CBO estimates that the costs of complying with the mandates in the bill would probably exceed the intergovernmental threshold established in UMRA (\$66 million in 2007, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

The bill would allow exceptions for the display or sale of SSNs when such use or display is authorized by the Social Security Act, necessary for law enforcement, national security or tax law purposes, done in compliance with certain motor vehicle laws, or used for consumer reporting practices and nonmarket research for advancing the public good. The bill's restrictions on the sale or display (which includes Internet transmissions that are not encrypted or otherwise secured) of SSNs would be prospective, and would not require state and local governments to redact SSNs from existing documents that are publicly available.

However, if state and local governments do not currently have a system in place to safeguard SSNs, any such governments would have to implement a new system for handling any documents issued when the regulations become effective (up to two and a half years following enactment). If state or local governments use SSNs on checks and check-stubs as part of their recordkeeping and tracking procedures, they would have to alter those systems and remove the SSNs. They also would have to implement systems for removing SSNs from many documents that currently include SSNs and that are available to the public. Likewise, some public institutions of higher education might have to alter their document systems for identification cards or tags to remove SSNs that are coded electronically onto a magnetic strip or digitized as part of a bar code. Finally, any government agency that uses SSNs would have to implement safeguards to preclude unauthorized access to SSNs and their derivatives and to protect confidentiality.

Because of the large number of governments affected by these provisions (particularly municipal governments), even small changes to existing systems would result in total costs that exceed the threshold established in UMRA. There are over 75,000 municipal governments, so even small one-time costs—for example, as little as \$5,000—would add up to costs over \$66 million in a given year. Counties and states, on the other hand, while fewer in number (there are about 3,600 counties in the United States), are more dependent on SSNs for various recordkeeping and identification purposes and would thus be likely to face significantly higher costs because of the complexity and scope of their recordkeeping systems. (Some counties estimate that altering their systems to use identifiers other than SSNs or to eliminate display of SSNs would result in one-time costs ranging from \$40,000 to over \$1 million, depending on the county and the scope of the changes that would need to be made).

Estimated impact on the private sector: H.R. 3046 would impose private-sector mandates, as defined in UMRA, on certain private entities. CBO cannot determine the direct costs of complying with

those mandates because such costs would depend on the specific regulations that would be issued under the bill. Consequently, CBO cannot determine whether the aggregate direct costs of complying with those mandates would exceed the annual threshold for private-sector mandates established by UMRA (\$131 million in 2007, adjusted annually for inflation).

The bill would impose private-sector mandates on certain private entities by generally prohibiting the purchase, sale, or display of an SSN to the general public, including on the Internet, with some exceptions. In addition, the bill would establish a uniform truncation standard requiring that truncated SSNs be limited to the last four digits of the number. Private entities also would be prohibited from:

- Making unnecessary disclosures of another individual's SSN to government agencies;
- Displaying an SSN on checks;
- Displaying an SSN on cards or tags issued to employees, family members, or other individuals; and
- Displaying an SSN on any card or tag issued to another person to access goods, services, or benefits.

Private entities that maintain SSNs in their records for the conduct of their business would be required to limit access to those records and institute safeguards to protect the confidentiality of those records. The Commissioner of Social Security would be required to issue regulations to implement the requirements, safeguards, and standards imposed by the bill. The direct cost to private entities of complying with those mandates would depend on regulations issued under the bill.

Previous CBO estimate: On May 25, 2007, CBO transmitted a cost estimate for H.R. 948, the Social Security Number Protection Act of 2007, as ordered reported by the House Committee on Energy and Commerce on May 10, 2007. That bill has similar provisions regarding the sale, purchase, or display of SSNs by entities in the private sector, but fewer requirements on government agencies. CBO estimated that H.R. 948 would not have a significant impact on spending subject to appropriation.

H.R. 948 also contains provisions that would impose intergovernmental mandates on state and local governments. However, because the Federal Trade Commission, the federal agency directed to carry out the provisions relating to the use of SSNs, does not have jurisdiction over those governments or public universities, the cost of mandates in H.R. 948 would be below the threshold established in UMRA.

The mandates on the private sector in H.R. 948 are similar to those in H.R. 3046, except that the Federal Trade Commission would be required—under H.R. 948—to issue the regulations prohibiting an entity in the private sector from selling or purchasing a Social Security number.

Estimate prepared by: Federal Costs: Social Security Administration—Sheila Dacey; Veterans Affairs—Sunita D'Monte; Treasury—Matthew Pickford; Defense—Jason Wheelock. Federal Revenues: Emily Schlect. Impact on State, Local, and Tribal Governments: Lisa Ramirez-Branum. Impact on the Private Sector: Paige Piper-Bach, Ralph Smith.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

V. OTHER MATTERS TO BE DISCUSSED UNDER THE RULES OF THE HOUSE

A. COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives (relating to oversight findings), the Committee, based on public hearing testimony, concludes that it is appropriate and timely to consider the bill as reported.

B. EARMARKS AND TAX AND TARIFF BENEFITS

With respect to clause 9 of rule XXI of the Rules of the House, H.R. 3046, as amended, does not contain any Congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

C. CONSTITUTIONAL AUTHORITY STATEMENT

With respect to clause (3)(d)(1) of rule XIII of the Rules of the House of Representatives, relating to Constitutional Authority, the Committee states that the Committee’s action in reporting the bill is derived from Article I of the Constitution, Section 8 (“The Congress shall have power to lay and collect taxes, duties, imposts, and excises, to pay the debts and to provide for * * * the general Welfare of the United States.”)

D. INFORMATION RELATING TO UNFUNDED MANDATES

This information is provided in accordance with Section 423 of the Unfunded Mandates Reform Act of 1995 (P.L. 104–4).

The Committee has determined that the bill does impose a Federal intergovernmental mandate on State, local, or tribal governments. The Committee has determined that the bill does contain Federal mandates on the private sector.

VI. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

SOCIAL SECURITY ACT

* * * * *

TITLE II—FEDERAL OLD-AGE, SURVIVORS, AND DISABILITY INSURANCE BENEFITS

* * * * *

EVIDENCE, PROCEDURE, AND CERTIFICATION FOR PAYMENT

SEC. 205. (a) * * *

* * * * *

(c)(1) * * *

(2)(A) * * *

* * * * *

(C)(i) * * *

* * * * *

(x)(I) A governmental entity (as defined in subclause (X)) may not sell or display to the general public any social security account number if such number has been disclosed to such governmental entity pursuant to the assertion by such governmental entity to any person that disclosure of such number is a statutory or regulatory requirement. Notwithstanding the preceding sentence, such number may be sold or displayed to the general public in accordance with the exceptions specified in subclauses (II), (III), (IV), (V), (VI), (VII), and (VIII) (and for no other purpose).

(II) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that such sale is specifically authorized by this Act or the Privacy Act of 1974.

(III) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that is necessary or appropriate for law enforcement or national security purposes, as determined under regulations which shall be issued as provided in section 1129C.

(IV) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent that such sale is required to comply with a tax law of the United States or of any State (or political subdivision thereof).

(V) Notwithstanding subclause (I), a social security account number may be sold by a State department of motor vehicles as authorized under subsection (b) of section 2721 of title 18, United States Code, if such number is to be used pursuant to such sale solely for purposes permitted under paragraph (1), (6), or (9) of such subsection.

(VI) Notwithstanding subclause (I), a social security account number may be sold or otherwise made available by a governmental entity to a consumer reporting agency (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))) for use or disclosure solely for permissible purposes described in section 604(a) of such Act (15 U.S.C. 1681b(a)).

(VII) Notwithstanding subclause (I), a social security account number may be sold by a governmental entity to the extent necessary for research (other than market research) conducted by any governmental entity for the purpose of advancing the public good, on the condition that the researcher provides adequate assurances that the social security account numbers will not be used to harass, target, or publicly reveal information concerning any identifiable individuals, that information about identifiable individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals, and that the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about identifiable

individuals, including procedures to ensure that the social security account numbers will be encrypted or otherwise appropriately secured from unauthorized disclosure. In the case of medical research, the Commissioner of Social Security shall maintain ongoing consultation with the Office for Civil Rights of the Department of Health and Human Services to ensure that the sale or purchase of social security account numbers which constitute personally identifiable medical information is permitted only in compliance with existing Federal rules and regulations prescribed by the Secretary of Health and Human Services pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (110 Stat. 2033).

(VIII) Notwithstanding subclause (I), a social security account number may be sold or displayed to the general public by a governmental entity under such other circumstances as may be specified in regulations issued as provided in section 1129C.

(IX) This clause does not apply with respect to a social security account number of a deceased individual.

(X) For purposes of this clause, the term “governmental entity” means an executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof, a Federally recognized Indian tribe, or a trustee appointed in a case under title 11, United States Code. Such term includes a person acting as an agent of such an agency or instrumentality, Indian tribe, or trustee. For purposes of this subclause, the term “State” has the meaning provided in subparagraph (D)(iii)(II).

(XI) For purposes of this clause, the term “sell” means, in connection with a social security account, to obtain, directly or indirectly, anything of value in exchange for such number. Such term does not include the submission of such number as part of the process for applying for any type of Government benefits or programs (such as grants, loans, or welfare or other public assistance programs) or as part of the administration of, or provision of benefits under, an employee benefit plan.

(XII) For purposes of this clause, the term “display to the general public” shall have the meaning provided such term in section 208A(a)(3)(A). In any case in which a governmental entity requires transmittal to such governmental entity of an individual’s social security account number by means of the Internet without ensuring that such number is encrypted or otherwise appropriately secured from disclosure, any such transmittal of such number as so required shall be treated, for purposes of this clause, as a “display to the general public” of such number by such governmental entity for purposes of this clause.

(XIII) For purposes of this clause, the term “social security account number” includes any derivative of such number. Notwithstanding the preceding sentence, any expression, contained in or on any item sold or displayed to the general public, shall not be treated as a social security account number solely because such expression sets forth not more than the last 4 digits of such number, if the remainder of such number cannot be determined based solely on such expression or any other matter presented in or on such item.

(XIV) Nothing in the preceding subclauses of this clause shall be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect under any other Federal or

State law, except to the extent that such statute, regulation, order, or interpretation is inconsistent with such subclauses, and then only to the extent of the inconsistency. For purposes of this subclause, a statute, regulation, order, or interpretation is not inconsistent with the preceding subclauses of this clause if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under such subclauses.

(xi) No governmental entity (as defined in clause (x)(X)) may include the social security account number of any individual (or any derivative of such number) on any check issued for any payment by such governmental entity or on any document attached to or accompanying such a check.

(xii) No governmental entity (as defined in clause (x)(X)), and no other person offering benefits in connection with an employee benefit plan maintained by such governmental entity, may display a social security account number (or any derivative thereof) on any card or tag that is commonly provided—

(I) to employees of such governmental entity,

(II) in the case of a governmental entity which is an educational institution, to its students, or

(III) in the case of a governmental entity which is a medical institution, to its patients,

(or to their family members) for purposes of identification or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number (or derivative thereof). The requirements of this clause shall also apply to the Medicare card issued by the Department of Health and Human Services.

(xiii) No governmental entity (as defined in clause (x)(X)) may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals (or any derivatives of such numbers). For purposes of this clause, the term “prisoner” means an individual confined in a jail, prison, or other penal institution or correctional facility.

(xiv) Except as otherwise provided in this paragraph, in the case of any governmental entity (as defined in clause (x)(X)) having access to an individual’s social security account number—

(I) no officer or employee thereof shall have access to such number for any purpose other than the effective administration of the statutory provisions governing its functions,

(II) such governmental entity shall restrict, to the satisfaction of the Commissioner of Social Security, access to social security account numbers obtained thereby to officers and employees thereof whose duties or responsibilities require access for the administration or enforcement of such provisions, and

(III) such governmental entity shall provide such other safeguards as the Commissioner determines to be necessary or appropriate to preclude unauthorized access to the social security account number and to otherwise protect the confidentiality of such number.

For purposes of this clause the term “social security account number” includes any derivative thereof.

(xv) The truncation by any governmental entity (as defined in clause (x)(X)) or by any person in the private sector of an individual’s social security account number which is used by such govern-

mental entity or person otherwise in accordance with the requirements of this Act shall be in accordance with a uniform truncation standard which shall be specified in regulations prescribed by the Commissioner of Social Security. Under such standard, the number as truncated shall set forth not more than the last 4 digits of the number. Nothing in this clause shall be construed to authorize any use of the social security account number which is not otherwise authorized by this title or regulations prescribed thereunder.

* * * * *

PENALTIES

SEC. 208. (a) Whoever—

(1) * * *

* * * * *

(8) discloses, uses, or compels the disclosure of the social security number of any person in violation of the laws of the United States; or

(9) *willfully acts or fails to act so as to cause a violation of section 208A(b)(1)(B);*

shall be guilty of a felony and upon conviction thereof [shall be fined under title 18, United States Code, or imprisoned for not more than five years, or both.] *shall be fined, imprisoned, or both, as provided in subsection (c).*

(b)(1) *Whoever—*

(A) *knowingly, and with intent to commit, or to aid or abet, any activity that constitutes a violation of Federal law, or a violation of any applicable law of a State or political subdivision thereof if the maximum penalty of such applicable law includes imprisonment for 5 years or more—*

(i) *possesses the social security account number of another person without lawful authority, or*

(ii) *possesses a social security card, knowing that the social security account number or other identifying information displayed on the card has been altered, counterfeited, or forged or that the card was falsely made, stolen, or obtained from the Social Security Administration by use of false information;*

if such activity is committed, or aided or abetted, with intent to use such social security account number, social security card, or other identifying information displayed on such card in furtherance of such violation;

(B) *being—*

(i) *an officer or employee of any governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or*

(ii) *a person acting as an agent of a governmental entity (as so defined),*

willfully acts or fails to act so as to cause a violation of clause (vi)(II), (xi), (xii), or (xv) of section 205(c)(2)(C);

(C) *being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (xi) or (xv) of section 205(c)(2)(C); or*

(D) *willfully acts or fails to act so as to cause a violation of subsection (c), (d), (e), or (f) of section 208A or, as a person in*

the private sector, willfully acts or fails to act so as to cause a violation of section 205(c)(2)(C)(xv); shall be guilty of a misdemeanor and upon conviction thereof shall be fined under title 18, United States Code, or imprisoned for not more than 1 year, or both.

(2)(A) Whoever—

(i) with intent to deceive, discloses, sells, or transfers his own social security account number, assigned to him by the Commissioner of Social Security (in the exercise of the Commissioner's authority under section 205(c)(2) to establish and maintain records), to any person;

(ii) without lawful authority, offers, for a fee, to acquire for any individual, or to assist in acquiring for any individual, an additional social security account number or a number that is purported to be a social security account number;

(iii) being—

(I) an officer or employee of any governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or

(II) a person acting as an agent of a governmental entity (as so defined),

willfully acts or fails to act so as to cause a violation of clause (x), (xiii), or (xiv) of section 205(c)(2)(C);

(iv) being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (x) or (xiv) of section 205(c)(2)(C); or

(v) willfully acts or fails to act so as to cause a violation of subsection (b)(1)(A) or (g) of section 208A;

shall be fined, imprisoned, or both, as provided in subparagraph (B).

(B) A person convicted of a violation described in subparagraph (A) shall—

(i) be fined under title 18, United States Code, imprisoned not more than 1 year, or both; and

(ii) if the offense is committed under false pretenses or for commercial advantage, personal gain, or malicious harm, be fined, imprisoned, or both, as provided in subsection (c).

(c) A person convicted of a violation described in subsection (a) or a violation described in subsection (b)(2)(A) which is subject to subsection (b)(2)(B)(ii) shall be—

(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial violation, subject to paragraphs (3) and (4),

(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which occurs after a prior conviction for another offense under subsection (a) becomes final, subject to paragraphs (3) and (4),

(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is committed to facilitate a drug trafficking crime (as defined in section 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title 18, United States Code) involving force against the person of another, subject to paragraph (4), and

(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).

[(b)] *(d)(1) Any Federal court, when sentencing a defendant convicted of an offense under subsection (a) or (b), may order, in addition to or in lieu of any other penalty authorized by law, that the defendant make restitution to the victims of such offense specified in paragraph (4).*

* * * * *

[(c)] *Any person or other entity who is convicted of a violation of any of the provisions of this section, if such violation is committed by such person or entity in his role as, or in applying to become, a certified payee under section 205(j) on behalf of another individual (other than such person's spouse), upon his second or any subsequent such conviction shall, in lieu of the penalty set forth in the preceding provisions of this section, be guilty of a felony and shall be fined under title 18, United States Code, or imprisoned for not more than five years, or both.*

[(d)] *(e) Any individual or entity convicted of a felony under this section or under section 1632(b) may not be certified as a payee under section 205(j). For the purpose of subsection (a)(7), the terms "social security number" and "social security account number" mean such numbers as are assigned by the Commissioner of Social Security under section 205(c)(2) whether or not, in actual use, such numbers are called social security numbers.*

[(e)] *(f)(1) * * **

* * * * *

(g)(1) Whoever is an employee of the Social Security Administration and knowingly and fraudulently sells or transfers one or more social security account numbers or social security cards shall, upon conviction, be guilty of a felony and fined under title 18, United States Code, imprisoned as provided in paragraph (2), or both.

(2) Imprisonment for a violation described in paragraph (1) shall be for—

(A) not more than 5 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred not more than 50 social security account numbers or social security cards,

(B) not more than 10 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred more than 50, but not more than 100, social security account numbers or social security cards, or

(C) not more than 20 years, in the case of an employee of the Social Security Administration who has fraudulently sold or transferred more than 100 social security account numbers or social security cards.

(3) For purposes of this subsection—

(A) The term "social security employee" means any State employee of a State disability determination service, any officer, employee, or contractor of the Social Security Administration, any employee of such a contractor, or any volunteer providing

services or assistance in any facility of the Social Security Administration.

(B) The term “social security account number” means a social security account number assigned by the Commissioner of Social Security under section 205(c)(2)(B) or another number that has not been so assigned but is purported to have been so assigned.

(C) The term “social security card” means a card issued by the Commissioner of Social Security under section 205(c)(2)(G), another card which has not been so issued but is purported to have been so issued, and banknote paper of the type described in section 205(c)(2)(G) prepared for the entry of social security account numbers, whether fully completed or not.

PROHIBITION OF THE SALE, PURCHASE, AND DISPLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PRIVATE SECTOR

SEC. 208A. (a) DEFINITIONS.—For purposes of this section:

(1) PERSON.—

(A) IN GENERAL.—Subject to subparagraph (B), the term “person” means any individual, partnership, corporation, trust, estate, cooperative, association, or any other entity.

(B) EXCLUSION OF GOVERNMENTAL ENTITIES.—Such term does not include a governmental entity. Nothing in this subparagraph shall be construed to authorize, in connection with a governmental entity, an act or practice otherwise prohibited under this section or section 205(c)(2)(C).

(2) SELLING AND PURCHASING.—

(A) IN GENERAL.—Subject to subparagraph (B)—

(i) SELL.—The term “sell” in connection with a social security account number means to obtain, directly or indirectly, anything of value in exchange for such number.

(ii) PURCHASE.—The term “purchase” in connection with a social security account number means to provide, directly or indirectly, anything of value in exchange for such number.

(B) EXCEPTIONS.—The terms “sell” and “purchase” in connection with a social security account number do not include the submission of such number as part of—

(i) the process for applying for any type of Government benefits or programs (such as grants or loans or welfare or other public assistance programs),

(ii) the administration of, or provision of benefits under, an employee benefit plan, or

(iii) the sale, lease, merger, transfer, or exchange of a trade or business.

(3) DISPLAY TO THE GENERAL PUBLIC.—

(A) IN GENERAL.—The term “display to the general public” means, in connection with a social security account number, to intentionally place such number in a viewable manner on an Internet site that is available to the general public or to make such number available in any other manner intended to provide access to such number by the general public.

(B) *INTERNET TRANSMISSIONS.*—*In any case in which a person requires transmittal to such person of an individual’s social security account number by means of the Internet without ensuring that such number is encrypted or otherwise well-secured from disclosure, any such transmittal of such number as so required shall be treated as a “display to the general public” of such number by such person.*

(4) *SOCIAL SECURITY ACCOUNT NUMBER.*—

(A) *IN GENERAL.*—*The term “social security account number” has the meaning given such term in section 208(e), except that such term includes any derivative of such number.*

(B) *4-DIGIT EXPRESSION.*—*Notwithstanding the preceding sentence, for purposes of subsection (b)(1)(A), any expression, contained in or on any item sold or displayed to the general public, shall not be treated as a social security account number solely because such expression sets forth not more than the last 4 digits of such number, if the remainder of such number cannot be determined based solely on such expression or any other matter presented in or on such item.*

(5) *GOVERNMENTAL ENTITY.*—

(A) *IN GENERAL.*—*The term “governmental entity” means an executive, legislative, or judicial agency or instrumentality of the Federal Government, a State or political subdivision thereof, a Federally recognized Indian tribe, or a trustee appointed in a case under title 11, United States Code. Such term includes a person acting as an agent of such an agency or instrumentality, Indian tribe, or trustee.*

(B) *STATE.*—*The term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, the Commonwealth of the Northern Marianas, and the Trust Territory of the Pacific Islands.*

(b) *PROHIBITION OF SALE, PURCHASE, AND DISPLAY TO THE GENERAL PUBLIC.*—

(1) *IN GENERAL.*—*Except as provided in paragraph (2), it shall be unlawful for any person to—*

(A) *sell or purchase a social security account number or display to the general public a social security account number, or*

(B) *obtain or use any individual’s social security account number for the purpose of locating or identifying such individual with the intent to harass, harm, or physically injure such individual or using the identity of such individual for any illegal purpose.*

(2) *EXCEPTIONS.*—

(A) *IN GENERAL.*—*Notwithstanding paragraph (1), and subject to paragraph (3), a social security account number may be sold or purchased by any person to the extent provided in this subsection (and for no other purpose) as follows:*

(i) *to the extent necessary for law enforcement, including (but not limited to) the enforcement of a child support obligation, as determined under regulations issued as provided in section 1129C;*

(ii) to the extent necessary for national security purposes, as determined under regulations issued as provided in section 1129C;

(iii) to the extent necessary for public health purposes;

(iv) to the extent necessary in emergency situations to protect the health or safety of 1 or more individuals;

(v) to the extent that the sale or purchase is required to comply with a tax law of the United States or of any State (or political subdivision thereof);

(vi) to the extent that the sale or purchase is to or by a consumer reporting agency (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))) for use or disclosure solely for permissible purposes described in section 604(a) of such Act (15 U.S.C. 1681b(a)); and

(vii) to the extent necessary for research (other than market research) conducted by an agency or instrumentality of the United States or of a State or political subdivision thereof (or a person acting as an agent of such an agency or instrumentality) for the purpose of advancing the public good, on the condition that the researcher provides adequate assurances that—

(I) the social security account numbers will not be used to harass, target, or publicly reveal information concerning any identifiable individuals;

(II) information about identifiable individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals; and

(III) the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about identifiable individuals, including procedures to ensure that the social security account numbers will be encrypted or otherwise appropriately secured from unauthorized disclosure.

(B) *MEDICAL RESEARCH.*—In the case of research referred to in subparagraph (A)(vii) consisting of medical research, the Commissioner of Social Security shall maintain ongoing consultation with the Office for Civil Rights of the Department of Health and Human Services to ensure that the sale or purchase of social security account numbers which constitute personally identifiable medical information is permitted only in compliance with existing Federal rules and regulations prescribed by the Secretary of Health and Human Services pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (110 Stat. 2033).

(3) *CONSENT AND OTHER CIRCUMSTANCES DETERMINED BY REGULATION.*—Notwithstanding paragraph (1), a social security account number assigned to an individual may be sold or purchased by any person—

(A) to the extent consistent with such individual's voluntary and affirmative written consent to the sale or purchase, but only if—

(i) the terms of the consent and the right to refuse consent are presented to the individual in a clear, conspicuous, and understandable manner,

(ii) the individual is placed under no obligation to provide consent to any such sale or purchase, and

(iii) the terms of the consent authorize the individual to limit the sale or purchase to purposes directly associated with the transaction with respect to which the consent is sought, and

(B) under such circumstances as may be deemed appropriate in regulations issued as provided under section 1129C.

(c) **PROHIBITION OF DISPLAY ON CHECKS.**—It shall be unlawful for any person to include the social security account number of any other individual on any check issued for any payment by such person or on any document attached to or accompanying such a check.

(d) **PROHIBITION OF UNAUTHORIZED DISCLOSURE TO GOVERNMENT AGENCIES OR INSTRUMENTALITIES.**—

(1) **IN GENERAL.**—It shall be unlawful for any person to communicate by any means to any agency or instrumentality of the United States or of any State or political subdivision thereof the social security account number of any individual other than such person without the written permission of such individual, unless the number was requested by the agency or instrumentality. In the case of an individual who is legally incompetent, permission provided by the individual's legal representatives shall be deemed to be permission provided by such individual.

(2) **EXCEPTIONS.**—Paragraph (1) shall not apply to the extent necessary—

(A) for law enforcement, including (but not limited to) the enforcement of a child support obligation, or

(B) for national security purposes,
as determined under regulations issued as provided under section 1129C.

(e) **PROHIBITION OF THE DISPLAYS ON CARDS OR TAGS REQUIRED FOR ACCESS TO GOODS, SERVICES, OR BENEFITS.**—No person may display a social security account number on any card or tag issued to any other person for the purpose of providing such other person access to any goods, services, or benefits or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number.

(f) **PROHIBITION OF THE DISPLAYS ON EMPLOYEE IDENTIFICATION CARDS OR TAGS.**—No person that is an employer, and no other person offering benefits in connection with an employee benefit plan maintained by such employer or acting as an agent of such employer, may display a social security account number on any card or tag that is commonly provided to employees of such employer (or to their family members) for purposes of identification or include on such card or tag a magnetic strip, bar code, or other means of communication which conveys such number.

(g) **MEASURES TO PRECLUDE UNAUTHORIZED DISCLOSURE OF SOCIAL SECURITY ACCOUNT NUMBERS AND PROTECT THE CONFIDEN-**

TIALITY OF SUCH NUMBERS.—Subject to the preceding provisions of this section, any person having access to the social security account number of any individual other than such person shall, to the extent that such access is maintained for the conduct of such person's trade or business—

(1) ensure that no officer or employee thereof has access to such number for any purpose other than as necessary for the conduct of such person's trade or business,

(2) restrict, in accordance with regulations of the Commissioner of Social Security, access to social security account numbers obtained thereby to officers and employees thereof whose duties or responsibilities require access for the conduct of such person's trade or business, and

(3) provide such safeguards as may be specified, in regulations of the Commissioner of Social Security, to be necessary or appropriate to preclude unauthorized access to the social security account number and to otherwise protect the confidentiality of such number.

(h) DECEASED INDIVIDUALS.—This section does not apply with respect to the social security account number of a deceased individual.

(i) APPLICABILITY OF OTHER PROTECTIONS.—Nothing in the preceding subsections of this section shall be construed as superseding, altering, or affecting any statutory provision, regulation, order, or interpretation in effect under any other Federal or State law, except to the extent that such statutory provision, regulation, order, or interpretation is inconsistent with such subsections, and then only to the extent of the inconsistency. For purposes of this subclause, a statutory provision, regulation, order, or interpretation is not inconsistent with the preceding subsections of this section if the protection such statutory provision, regulation, order, or interpretation affords any person is greater than the protection provided under such subsections.

* * * * *

TITLE VIII—SPECIAL BENEFITS FOR CERTAIN WORLD WAR II VETERANS

* * * * *

SEC. 811. PENALTIES FOR FRAUD.

(a) IN GENERAL.—Whoever—

*(1) * * **

* * * * *

[shall be fined under title 18, United States Code, imprisoned not more than 5 years, or both.] shall be fined, imprisoned, or both, as provided in subsection (b).

(b) PUNISHMENT.—A person convicted of a violation described in subsection (a) shall be—

(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial violation, subject to paragraphs (3) and (4),

(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which

occurs after a prior conviction for another offense under subsection (a) becomes final, subject to paragraphs (3) and (4),

(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is committed to facilitate a drug trafficking crime (as defined in section 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title 18, United States Code) involving force against the person of another, subject to paragraph (4), and

(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).

[(b)] (c) COURT ORDER FOR RESTITUTION.—

(1) * * *

* * * * *

TITLE XI—GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION

PART A—GENERAL PROVISIONS

* * * * *

SEC. 1129. CIVIL MONETARY PENALTIES AND ASSESSMENTS FOR TITLES II, VIII AND XVI.

(a)(1) * * *

* * * * *

(2) In addition, the Commissioner of Social Security may make a determination in the same proceeding to recommend that the Secretary exclude, as provided in section 1128, such a person who is a medical provider or physician from participation in the programs under title XVIII.

(3) Any person (including an organization, agency, or other entity) who—

(A) uses a social security account number that such person knows or should know has been assigned by the Commissioner of Social Security (in an exercise of authority under section 205(c)(2) to establish and maintain records) on the basis of false information furnished to the Commissioner by any person;

(B) falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to any individual, when such person knows or should know that such number is not the social security account number assigned by the Commissioner to such individual;

(C) with intent to deceive, alters a social security card that the person knows or should know was issued by the Commissioner of Social Security, or possesses such a card with intent to alter it;

(D) buys or sells a card that such person knows or should know is, or is purported to be, a card issued by the Commissioner of Social Security, or possesses such a card with intent to buy or sell it;

(E) counterfeits a social security card, or possesses a counterfeit social security card with intent to buy or sell it;

(F) discloses, uses, compels the disclosure of, or knowingly sells or purchases the social security account number of any person in violation of the laws of the United States;

(G) with intent to deceive the Commissioner of Social Security as to such person's true identity (or the true identity of any other person), furnishes or causes to be furnished false information to the Commissioner with respect to any information required by the Commissioner in connection with the establishment and maintenance of the records provided for in section 205(c)(2);

(H) without lawful authority, offers, for a fee, to acquire for any individual, or to assist in acquiring for any individual, an additional social security account number or a number which is purported to be a social security account number;

(I) with intent to deceive, discloses, sells, or transfers his own social security account number, assigned to him by the Commissioner of Social Security under section 205(c)(2)(B), to any person;

(J) knowingly, and with intent to commit, or to aid or abet, any activity that constitutes a violation of Federal law, or a violation of any applicable law of a State or political subdivision thereof if the maximum penalty of such applicable law includes imprisonment for 5 years or more—

(i) possesses a social security account number of another individual without lawful authority, or

(ii) possesses a social security card, knowing that the social security account number or other identifying information displayed on the card has been altered, counterfeited, or forged or that the card was falsely made, stolen, or obtained from the Social Security Administration by use of false information,

if such activity is committed, or aided or abetted, with intent to use such social security account number, social security card, or other identifying information displayed on such card in furtherance of such violation;

(K) being—

(i) an officer or employee of a governmental entity (as defined in section 205(c)(2)(C)(x)(X)), or

(ii) a person acting as an agent of a governmental entity (as so defined),

willfully acts or fails to act so as to cause a violation of clause (vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C);

(L) being a trustee appointed in a case under title 11, United States Code (or an officer or employee thereof or a person acting as an agent thereof), willfully acts or fails to act so as to cause a violation of clause (x), (xi), (xiv), or (xv) of section 205(c)(2)(C);

(M) violates section 208A (relating to prohibition of the sale, purchase, or display of the social security account number in the private sector) or, as a person in the private sector, violates section 205(c)(2)(C)(xv); or

(N) violates section 208(g) (relating to fraud by social security administration employees);

shall be subject to, in addition to any other penalties that may be prescribed by law, a civil money penalty of not more than \$5,000 for each violation. Such person shall also be subject to an assess-

ment, in lieu of damages sustained by the United States resulting from such violation, of not more than twice the amount of any benefits or payments paid as a result of such violation.

[(2)] (4) For purposes of this section, a material fact is one which the Commissioner of Social Security may consider in evaluating whether an applicant is entitled to benefits under title II or title VIII, or eligible for benefits or payments under title XVI.

[(3)] (5) Any person (including an organization, agency, or other entity) who, having received, while acting in the capacity of a representative payee pursuant to section 205(j), 807, or 1631(a)(2), a payment under title II, VIII, or XVI for the use and benefit of another individual, converts such payment, or any part thereof, to a use that such person knows or should know is other than for the use and benefit of such other individual shall be subject to, in addition to any other penalties that may be prescribed by law, a civil money penalty of not more than \$5,000 for each such conversion. Such person shall also be subject to an assessment, in lieu of damages sustained by the United States resulting from the conversion, of not more than twice the amount of any payments so converted.

* * * * *

REGULATORY AND ENFORCEMENT AUTHORITY WITH RESPECT TO
MISUSE OF THE SOCIAL SECURITY ACCOUNT NUMBER

SEC. 1129C. (a) REGULATORY AUTHORITY.—

(1) IN GENERAL.—The Commissioner of Social Security shall prescribe regulations to carry out the provisions of clauses (vi)(II), (x), (xi), (xii), (xiii), (xiv), and (xv) of section 205(c)(2)(C) and section 208A. Such regulations shall be issued in consultation with the Federal Trade Commission, the Attorney General of the United States, the Secretary of Homeland Security, the Secretary of Health and Human Services, the Secretary of the Treasury, the Federal banking agencies (as defined in section 3 of the Federal Deposit Insurance Act), the National Credit Union Administration, the Securities and Exchange Commission, State attorneys general, and such representatives of the State insurance commissioners as may be designated by the National Association of Insurance Commissioners.

(2) TREATMENT OF MATTERS RELATING TO LAW ENFORCEMENT AND NATIONAL SECURITY.—In issuing the regulations described in paragraph (1) with respect to the provisions of 205(c)(2)(C)(x)(III), paragraph (A) or (B) of section 208A(b)(2), or section 208A(c)(2) (relating to law enforcement and national security), the sale or purchase of Social Security account numbers may be authorized only if the Commissioner (or the agency or instrumentality delegated authority to issue such regulations under paragraph (5)) determines that—

(A) such sale or purchase would serve a compelling public interest that cannot reasonably be served through alternative measures, and

(B) such sale or purchase will not pose an unreasonable risk of identity theft, or bodily, emotional, or financial harm to an individual (taking into account any restrictions and conditions that the agency or instrumentality issuing the regulations imposes on the sale, purchase, or disclosure).

(3) TREATMENT OF OTHER MATTERS IN GENERAL DISCRETION OF THE COMMISSIONER.—

(A) *IN GENERAL.*—In issuing the regulations described in paragraph (1) with respect to the provisions of section 205(c)(2)(C)(x)(VIII) or section 208A(b)(3)(B), the sale, purchase, or display to the general public of social security account numbers may be authorized only after considering, among other relevant factors—

(i) the extent to which the authorization of the sale, purchase, or display of the social security account number would serve a compelling public interest that cannot reasonably be served through alternative measures,

(ii) the associated cost or burden of the authorization to the general public, businesses, commercial enterprises, non-profit organizations, and Federal, State, and local governments; and

(iii) the associated benefit of the authorization to the general public, businesses, commercial enterprises, non-profit associations, and Federal, State, and local governments.

(B) *RESTRICTIONS AND CONDITIONS.*—If, after considering the factors in subparagraph (A), the sale, purchase, or display to the general public of social security account numbers is authorized under regulations referred to in subparagraph (A), the Commissioner (or the agency or instrumentality delegated authority to issue such regulations under paragraph (5)) shall impose restrictions and conditions on the sale, purchase, or display to the general public to the extent necessary—

(i) to provide reasonable assurances that social security account numbers will not be used to commit or facilitate fraud, deceptions, or crime, and

(ii) to prevent an unreasonable risk of identity theft or bodily, emotional, or financial harm to any individual, considering the nature, likelihood, and severity of the anticipated harm that could result from the sale, purchase, or display to the general public of social security account numbers, together with the nature, likelihood, and extent of any benefits that could be realized.

(C) *5-YEAR EXPIRATION DATE FOR REGULATIONS.*—At the end of the 5-year period beginning on the effective date of any final regulations issued pursuant to this paragraph—

(i) such regulations shall expire, and

(ii) new regulations may be issued pursuant to this paragraph.

(4) *ADMINISTRATIVE PROCEDURE.*—In the issuance of regulations pursuant to this subsection, notice shall be provided as described in paragraphs (1), (2), and (3) of section 553(b) of title 5, United States Code, and opportunity to participate in the rule making shall be provided in accordance with section 553(c) of such title.

(5) *DELEGATION TO OTHER AGENCIES.*—Any agency or instrumentality of the United States may exercise the authority of the Commissioner under this subsection, with respect to matters otherwise subject to regulation by such agency or instrumentality, to the extent determined appropriate in regulations of the Commissioner.

(6) *CONSULTATION AND COORDINATION.*—Each agency and instrumentality exercising authority to issue regulations under

this subsection shall consult and coordinate with the other such agencies and instrumentalities for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency or instrumentality are consistent and comparable, as appropriate, with the regulations prescribed by the other such agencies and instrumentalities. The Commissioner shall undertake to facilitate such consultation and coordination.

(7) DEFINITIONS AND SPECIAL RULES.—

(A) For purposes of this subsection, the terms “sell”, “purchase”, and “display to the general public” shall have the meanings provided such terms under section 205(c)(2)(C)(x) or section 208A(a), as applicable.

(B) For purposes of this subsection, section 205(c)(2)(C)(x)(XI) shall apply.

(b) COORDINATION OF ENFORCEMENT WITH OTHER AGENCIES.—*The Commissioner may provide, by regulation, for enforcement by any other agency or instrumentality of the United States of the provisions of section 208A and regulations prescribed pursuant to subsection (a)(1) with respect to section 208A.*

(c) ACTIONS BY STATES WITH RESPECT TO MISUSE IN PRIVATE SECTOR OR BY STATE AND LOCAL GOVERNMENTS.—

(1) CIVIL ACTIONS.—*In any case in which the attorney general of a State (as defined in section 205(c)(2)(C)(x)(X)) has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice described in paragraph (2), the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction, to—*

(A) enjoin that act or practice;

(B) enforce compliance with the regulation;

(C) obtain civil penalties in an amount of \$11,000 per violation not to exceed a total of \$5,000,000; or

(D) obtain such other legal and equitable relief as the district court may consider to be appropriate.

Before filing an action under this subsection, the attorney general of the State involved shall provide to the Commissioner of Social Security and the Attorney General of the United States a written notice of that action and a copy of the complaint for that action. If the State attorney general determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action, the State attorney general shall provide the written notice and the copy of the complaint as soon after the filing of the complaint as practicable. Any reference in this subsection to the attorney general of a State shall be deemed also to be a reference to any equivalent official of such State.

(2) ACTS OR PRACTICES SUBJECT TO ENFORCEMENT.—*An act or practice described in this paragraph is—*

(A) an act or practice by an executive, legislative, or judicial agency or instrumentality of the State involved or a political subdivision thereof, a person acting as an agent thereof, or any officer or employee of the foregoing or person acting as an agent of the foregoing that violates clause

(vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of section 205(c)(2)(C) or any regulation promulgated thereunder, or
 (B) an act or practice by any person that violates section 208A or any regulation promulgated thereunder.

(3) *ATTORNEY GENERAL AUTHORITY.*—On receiving notice under paragraph (1), the Attorney General of the United States shall have the right—

(A) to move to stay the action, pending the final disposition of a pending Federal matter as described in paragraph (4);

(B) to intervene in an action under paragraph (1);

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

(D) to file petitions for appeal.

(4) *PENDING CRIMINAL PROCEEDINGS.*—If the Attorney General of the United States has instituted a criminal proceeding under section 208 alleging an act or practice described in paragraph (2) in connection with any State, such State may not, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in the criminal proceeding.

(5) *RULE OF CONSTRUCTION.*—For purposes of bringing any civil action under paragraph (1), nothing in this subsection shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to conduct investigations, administer oaths and affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

(6) *VENUE; SERVICE OF PROCESS.*—Any action brought under paragraph (1) may be brought in any district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. In an action brought under paragraph (1), process may be served in any district in which the defendant is an inhabitant or may be found.

(d) *REMEDIES TO INDIVIDUALS FOR VIOLATIONS BY THE FEDERAL GOVERNMENT OF REQUIREMENTS RELATING TO SOCIAL SECURITY ACCOUNT NUMBERS.*—

(1) *CIVIL ACTIONS.*—Any individual who is aggrieved by an act or practice by any person acting as an officer, employee, or agent of an agency or instrumentality of the Federal Government in violation of the requirements of clause (vi)(II), (x), (xi), (xii), (xiii), (xiv), or (xv) of subsection (c)(2)(C) with respect to the social security account number assigned to such individual under subsection (c)(2)(B) may commence a civil action for appropriate equitable relief or actual damages.

(2) *VENUE; SERVICE OF PROCESS.*—An action under this subsection may be brought in the district court of the United States for the judicial district in which the plaintiff resides, or has his principal place of business, in which the violation took place, or in which the defendant resides or may be found, and process may be served in any other district in which a defendant resides or may be found.

(3) *JURISDICTION.*—The district courts of the United States shall have jurisdiction, without respect to the amount in con-

trov­ersy or the cit­iz­en­ship of the parties, to grant the relief pro­vided for in para­graph (1).

(4) ATTORNEY’S FEES.—In any action under this subsection, the court in its discretion may allow a reasonable attorney’s fee and costs of action to either party.

(e) ONGOING GAO REVIEW ON EFFICACY OF REGULATIONS.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct an ongoing review of the efficacy of the reg­u­la­tions pre­scribed by any agency or instrumentality of the United States pursuant to this section. Such review shall con­sid­er the extent to which such regulations are consistent with, and in fur­ther­ance of the purposes of, the amend­ments made by the Social Security Number Privacy and Identity Theft Pre­ven­tion Act of 2007.

(2) REPORT.—Not later than 4 years after the effective date of any final regulations issued by any agency or instrumentality of the United States pursuant to this section, the Comptroller General shall report to each House of the Congress regarding the results of the review of such regulations conducted under this paragraph. Such report shall include the Comptroller Gen­eral’s recom­men­da­tions for such statutory or regulatory changes as the Comptroller General considers appropriate.

* * * * *

TITLE XVI—SUPPLEMENTAL SECURITY INCOME FOR THE AGED, BLIND, AND DISABLED

* * * * *

PART B—PROCEDURAL AND GENERAL PROVISIONS

* * * * *

PENALTIES FOR FRAUD

SEC. 1632. (a) Whoever—

(1) * * *

* * * * *

[shall be fined under title 18, United States Code, imprisoned not more than 5 years, or both,] shall be fined, imprisoned, or both, as provided in subsection (b).

(b) A person convicted of a violation described in subsection (a) shall be—

(1) fined under title 18, United States Code, or imprisoned for not more than 5 years, or both, in the case of an initial viola­tion, subject to paragraphs (3) and (4),

(2) fined under title 18, United States Code, or imprisoned for not more than 10 years, or both, in the case of a violation which occurs after a prior conviction for another offense under sub­sec­tion (a) becomes final, subject to paragraphs (3) and (4),

(3) fined under title 18, United States Code, or imprisoned for not more than 20 years, in the case of a violation which is com­mitted to facilitate a drug trafficking crime (as defined in sec­tion 929(a)(2) of title 18, United States Code) or in connection with a crime of violence (as defined in section 924(c)(3) of title

18, United States Code) involving force against the person of another, subject to paragraph (4), and

(4) fined under title 18, United States Code, or imprisoned for not more than 25 years, in the case of a violation which is committed to facilitate an act of international or domestic terrorism (as defined in paragraphs (1) and (5), respectively, of section 2331 of title 18, United States Code).

[(b)] (c)(1) * * *

* * * * *

[(c)] (d) Any person or entity convicted of a violation of subsection (a) of this section or of section 208 may not be certified as a representative payee under section 1631(a)(2).

* * * * *

VII. ADDITIONAL VIEWS

ADDITIONAL VIEWS OF HON. KENNY C. HULSHOF

The absence of overarching Federal law regulating the sale, purchase, and display to the general public of Social Security numbers (SSNs), and the growing threat represented by SSN misuse and identity theft, have prompted a need to better protect the privacy and integrity of SSNs. The purpose of the “Social Security Number Privacy and Identity Theft Prevention Act of 2007,” H.R. 3046, is to enhance Social Security number privacy protections and to otherwise enhance protections against identity theft.

Concerns have been raised that the provisions in H.R. 3046 would harm a consumer’s ability to obtain benefits such as credit as stipulated by the Fair Credit Reporting Act (FCRA).

The bill addresses these concerns by providing exceptions to the prohibitions on SSN sale and purchase, as follows: (1) by or to a consumer reporting agency for use or disclosure for permissible purposes described in the FCRA; (2) with affirmative written consent; and (3) under other circumstances determined appropriate according to regulations. Also, to permit accurate data-matching to continue without jeopardizing SSN privacy, the bill provides for the sale and display to the general public of the last four digits of the SSN for two years after the effective date of the final regulation. This authority may be extended with action by Congress.

As the bill advances through the legislative process, continued efforts should be made to protect the accuracy of credit reports and other consumer reports, along with the legitimate uses of the SSN by financial institutions.

KENNY C. HULSHOF.

ADDITIONAL VIEWS OF HON. PATRICK J. TIBERI

I agree with the goal of H.R. 3046, the “Social Security Number Privacy and Identity Theft Prevention Act of 2007.” We, as holders of the public trust, need to do everything within our power to ensure our constituents’ personal information remains exactly that—personal. We need to make sure that key information, like a Social Security number, is used in a responsible and protected way. Chairman McNulty and Ranking Member Johnson deserve a great deal of credit for their dedication and hard work on this bill.

During markup of this legislation I expressed a concern about the balance between restricting the use of Social Security numbers where there is no compelling purpose, and allowing continued use where they may be needed for important and legitimate purposes. I would like to take this opportunity to elaborate on my comments.

The bill prohibits the sale, purchase, and display of Social Security numbers, with limited exceptions: for law enforcement purposes, national security purposes, public health purposes, emergency situations, compliance with a tax law, use or disclosure by a consumer reporting agency for the permissible purposes of section 604(a) of the Fair Credit Reporting Act (FCRA), certain research, and when the consumer has consented.

The committee did not explicitly allow the use of Social Security numbers for the detection and prevention of fraud or to verify a person’s identity in connection with financial transactions. Banks are mandated by Section 326 of the USA PATRIOT Act to have a Customer Identification Program, intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. It is obviously important that the identity verification process produces a high degree of confidence in the person’s identity.

The bill authorizes the Social Security Administration to provide additional exceptions by regulation. As a former Member of the Committee on Financial Services, I note that these uses are allowed under the Gramm-Leach-Bliley Act for all “nonpublic personal information,” which includes Social Security numbers. It also permits the use of Social Security numbers only for FCRA section 604(a), rather than for all of the permissible purposes under that Act. Without specific attention to this matter, I’m concerned that H.R. 3046 could, in fact, overturn Gramm-Leach-Bliley to prohibit the use of Social Security numbers for legitimate purposes. They should be provided for by statute, rather than left to the chances of a regulatory process.

I appreciate Chairman Rangel's offer to work with me to resolve this issue and hope that it can be addressed as the bill moves forward.

PATRICK J. TIBERI.

