2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1627

At the request of Mr. LIEBERMAN, the name of the Senator from New York (Mr. SCHUMER) was added as a cosponsor of amendment No. 1627 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1628

At the request of Mr. CARDIN, his name was added as a cosponsor of amendment No. 1628 proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1633

At the request of Mr. GRAHAM, the name of the Senator from Georgia (Mr. CHAMBLISS) was added as a cosponsor of amendment No. 1633 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1634

At the request of Mr. MCCAIN, the name of the Senator from Texas (Mrs. HUTCHISON) was added as a cosponsor of amendment No. 1634 proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1636

At the request of Mr. INOUYE, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of amendment No. 1636 proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1644

At the request of Mr. BROWNBACK, the name of the Senator from Nebraska (Mr. NELSON) was added as a cosponsor of amendment No. 1644 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1653

At the request of Mr. CORNYN, the names of the Senator from Connecticut (Mr. LIEBERMAN) and the Senator from Nebraska (Mr. JOHANNS) were added as cosponsors of amendment No. 1653 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1659

At the request of Mr. SANDERS, the name of the Senator from Maryland (Ms. MIKULSKI) was added as a cosponsor of amendment No. 1659 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1661

At the request of Mr. KERRY, the names of the Senator from Rhode Island (Mr. WHITEHOUSE) and the Senator from New Jersey (Mr. LAUTENBERG) were added as cosponsors of amendment No. 1661 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1670

At the request of Mr. MENENDEZ, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of amendment No. 1670 intended to be proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1676

At the request of Mr. BEGICH, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of amendment No. 1676 proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 1677

At the request of Mr. BEGICH, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of amendment No. 1677 proposed to S. 1390, an original bill to authorize appropriations for fiscal year 2010 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LEAHY:

S. 1490. A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; to the Committee on the Judiciary.

Mr. LEAHY. Mr. President, today, I am pleased to reintroduce the Personal Data Privacy and Security Act. The recent and troubling cyber attack on U.S. Government computers is clear evidence that developing a comprehensive national strategy for data privacy and cybersecurity is one of the most challenging and important issues facing our nation. The Personal Data Privacy and Security Act will help to meet this challenge, by better protecting Americans from the growing threats of data breaches and identity theft.

When Senator SPECTER and I first introduced this bill 4 years ago, we had high hopes of bringing urgently needed data privacy reforms to the American people. Although the Judiciary Committee favorably reported this bill twice, in 2005 and again in 2007, the legislation languished on the Senate calendar and the Senate adjourned without passing comprehensive data privacy legislation.

While the Congress has waited to act, the dangers to our privacy, economic prosperity and national security posed by data breaches have not gone away. Just this week, the Government Accountability Office released a report finding that almost all of our major federal agencies have systemic weaknesses in the information security controls. According to the Privacy Rights Clearinghouse, more than 250 million records containing sensitive personal information have been involved in data security breaches since 2005.

This loss of privacy is not just a grave concern for American consumers; it is also a serious threat to the economic security of American businesses. The President's recent report on Cyberspace Policy Review noted that industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion.

The FBI's Internet Fraud Complaint Center also recently reported that

complaints of Internet fraud increased by 33 percent in 2008. These troubling reports are all compelling examples of why we need to promptly pass the Personal Data Privacy and Security Act.

Earlier this year, the Judiciary Committee held an important hearing on the privacy risks associated with electronic health records as the Nation moves towards a national health IT system. I am pleased that many of the privacy principles developed during that hearing have been enacted as part of the President's economic recovery package.

The Personal Data Privacy and Security Act requires that data brokers let consumers know what sensitive personal information they have about them, and to allow individuals to correct inaccurate information. The bill also requires that companies that have databases with sensitive personal information on Americans establish and implement data privacy and security programs.

In addition, the bill requires notice when sensitive personal information has been compromised. This bill also provides for tough criminal penalties for anyone who would intentionally and willfully conceal the fact that a data breach has occurred when the breach causes economic damage to consumers. Finally, the bill addresses the important issue of the government's use of personal data by requiring that federal agencies notify affected individuals when government data breaches occur, and placing privacy and security front and center when federal agencies evaluate whether data brokers can be trusted with government contracts that involve sensitive information about the American people.

Of course, Senator SPECTER and I have no monopoly on good ideas to solve the serious problems of identity theft and lax cybersecurity. But, we have put forth some meaningful solutions to this problem in this bill.

We have drafted this bill after long and thoughtful consultation with many of the stakeholders on this issue, including the privacy, consumer protection and business communities. We have also worked closely with other Senators, including Senators FEINSTEIN, FEINGOLD, and SCHUMER.

This is a comprehensive bill that not only deals with the need to provide Americans with notice when they have been victims of a data breach, but that also deals with the underlying problem of lax security and lack of accountability to help prevent data breaches from occurring in the first place. Passing this comprehensive data privacy legislation is one of my highest legislative priorities as Chairman of the Judiciary Committee, and I hope all Senators will support this measure.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1490

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Personal Data Privacy and Security Act of 2009''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Definitions.
TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY
Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
Sec. 103. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.
Sec. 104. Effects of identity theft on bankruptcy proceedings.
TITLE II—DATA BROKERS
Sec. 201. Transparency and accuracy of data collection.
Sec. 202. Enforcement.
Sec. 203. Relation to State laws.
Sec. 204. Effective date.
TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION
Subtitle A—A Data Privacy and Security Program
Sec. 301. Purpose and applicability of data privacy and security program.
Sec. 302. Requirements for a personal data privacy and security program.
Sec. 303. Enforcement.
Sec. 304. Relation to other laws.
Subtitle B—Security Breach Notification
Sec. 311. Notice to individuals.
Sec. 312. Exemptions.
Sec. 313. Methods of notice.
Sec. 314. Content of notification.
Sec. 315. Coordination of notification with credit reporting agencies.
Sec. 316. Notice to law enforcement.
Sec. 317. Enforcement.
Sec. 318. Enforcement by State attorneys general.
Sec. 319. Effect on Federal and State law.
Sec. 320. Authorization of appropriations.
Sec. 321. Reporting on risk assessment exemptions.
Sec. 322. Effective date.
Subtitle C—Office of Federal Identity Protection
Sec. 331. Office of Federal Identity Protection.
TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA
Sec. 401. General services administration review of contracts.
Sec. 402. Requirement to audit information security practices of contractors and third party business entities.
Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.
Sec. 404. Implementation of chief privacy officer requirements.

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the Nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;

(3) over 9,300,000 individuals were victims of identity theft in America last year;

(4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;

(5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(7) data brokers have assumed a significant role in providing identification, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations;

(8) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(9) there is a need to insure that data brokers conduct their operations in a manner that prioritizes fairness, transparency, accuracy, and respect for the privacy of consumers;

(10) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(11) because government use of commercial data containing personal information potentially affects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551 of title 5, United States Code.

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028 of title 18, United States Code.

(5) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

(6) DATA FURNISHER.—The term ''data furnisher'' means any agency, organization,

corporation, trust, partnership, sole proprietorship, unincorporated association, or nonprofit that serves as a source of information for a data broker.

(7) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(8) PERSONAL ELECTRONIC RECORD.—

(A) IN GENERAL.—The term ''personal electronic record'' means data associated with an individual contained in a database, networked or integrated databases, or other data system that is provided to nonaffiliated third parties and includes sensitive personally identifiable information about that individual.

(B) EXCLUSIONS.—The term ''personal electronic record'' does not include—

(i) any data related to an individual's past purchases of consumer goods; or

(ii) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual.

(9) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United States Code.

(10) PUBLIC RECORD SOURCE.—The term ''public record source'' means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(11) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.

(B) EXCLUSION.—The term ''security breach'' does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure; or

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(12) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes—

(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:

(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother's maiden name, if identified as such.

(III) Month, day, and year of birth.

(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(B) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting ''section 1030(a)(2)(D) (relating to fraud and related activity in connection with unauthorized access to sensitive personally identifiable information as defined in the Personal Data Privacy and Security Act of 2009,'' before ''section 1084''.

SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

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

''§ 1041. Concealment of security breaches involving sensitive personally identifiable information

''(a) Whoever, having knowledge of a security breach and of the obligation to provide notice of such breach to individuals under title III of the Personal Data Privacy and Security Act of 2009, and having not otherwise qualified for an exemption from providing notice under section 312 of such Act, intentionally and willfully conceals the fact of such security breach and which breach causes economic damage to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

''(c) Any person seeking an exemption under section 312(b) of the Personal Data Privacy and Security Act of 2009 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 312(b)(3) of such Act''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of security breaches involving personally identifiable information.''.

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service shall have the authority to investigate offenses under this section.

(2) NONEXCLUSIVITY.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.

SEC. 103. REVIEW AND AMENDMENT OF FEDERAL SENTENCING GUIDELINES RELATED TO FRAUDULENT ACCESS TO OR MISUSE OF DIGITIZED OR ELECTRONIC PERSONALLY IDENTIFIABLE INFORMATION.

(a) REVIEW AND AMENDMENT.—The United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines (including its policy statements) applicable to persons convicted of using fraud to access, or misuse of, digitized or electronic personally identifiable information, including identity theft or any offense under—

(1) sections 1028, 1028A, 1030, 1030A, 2511, and 2701 of title 18, United States Code; and

(2) any other relevant provision.

(b) REQUIREMENTS.—In carrying out the requirements of this section, the United States Sentencing Commission shall—

(1) ensure that the Federal sentencing guidelines (including its policy statements) reflect—

(A) the serious nature of the offenses and penalties referred to in this Act;

(B) the growing incidences of theft and misuse of digitized or electronic personally identifiable information, including identity theft; and

(C) the need to deter, prevent, and punish such offenses;

(2) consider the extent to which the Federal sentencing guidelines (including its policy statements) adequately address violations of the sections amended by this Act to—

(A) sufficiently deter and punish such offenses; and

(B) adequately reflect the enhanced penalties established under this Act;

(3) maintain reasonable consistency with other relevant directives and sentencing guidelines;

(4) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(5) consider whether to provide a sentencing enhancement for those convicted of the offenses described in subsection (a), if the conduct involves—

(A) the online sale of fraudulently obtained or stolen personally identifiable information;

(B) the sale of fraudulently obtained or stolen personally identifiable information to an individual who is engaged in terrorist activity or aiding other individuals engaged in terrorist activity; or

(C) the sale of fraudulently obtained or stolen personally identifiable information to finance terrorist activity or other criminal activities;

(6) make any necessary conforming changes to the Federal sentencing guidelines to ensure that such guidelines (including its policy statements) as described in subsection (a) are sufficiently stringent to deter, and adequately reflect crimes related to fraudulent access to, or misuse of, personally identifiable information; and

(7) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing under section 3553(a)(2) of title 18, United States Code.

(c) EMERGENCY AUTHORITY TO SENTENCING COMMISSION.—The United States Sentencing Commission may, as soon as practicable, promulgate amendments under this section in accordance with procedures established in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that Act had not expired.

SEC. 104. EFFECTS OF IDENTITY THEFT ON BANKRUPTCY PROCEEDINGS.

(a) DEFINITIONS.—Section 101 of title 11, United States Code, is amended—

(1) by redesignating paragraph (27B) as paragraph (27D); and

(2) by inserting after paragraph (27A) the following:

''(27) The term 'identity theft' means a fraud committed or attempted using the personally identifiable information of another person.

''(28) The term 'identity theft victim' means a debtor who, as a result of an identify theft in any consecutive 12-month period during the 3-year period before the date on which a petition is filed under this title, had claims asserted against such debtor in excess of the least of—

''(A) $20,000;

''(B) 50 percent of all claims asserted against such debtor; or

''(C) 25 percent of the debtor's gross income for such 12-month period.''.

(b) PROHIBITION.—Section 707(b) of title 11, United States Code, is amended by adding at the end the following:

''(8) No judge, United States trustee (or bankruptcy administrator, if any), trustee, or other party in interest may file a motion under paragraph (2) if the debtor is an identity theft victim.''.

TITLE II—DATA BROKERS

SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any product or service offered to third parties that allows access or use of sensitive personally identifiable information.

(b) LIMITATION.—Notwithstanding any other provision of this title, this section shall not apply to—

(1) any product or service offered by a data broker engaging in interstate commerce where such product or service is currently subject to, and in compliance with, access and accuracy protections similar to those under subsections (c) through (f) of this section under the Fair Credit Reporting Act (Public Law 91–508);

(2) any data broker that is subject to regulation under the Gramm-Leach-Bliley Act (Public Law 106–102);

(3) any data broker currently subject to and in compliance with the data security requirements for such entities under the Health Insurance Portability and Accountability Act (Public Law 104–191), and its implementing regulations;

(4) information in a personal electronic record that—

(A) the data broker has identified as inaccurate, but maintains for the purpose of aiding the data broker in preventing inaccurate information from entering an individual's personal electronic record; and

(B) is not maintained primarily for the purpose of transmitting or otherwise providing that information, or assessments based on that information, to nonaffiliated third parties; and

(5) information concerning proprietary methodologies, techniques, scores, or algorithms relating to fraud prevention not normally provided to third parties in the ordinary course of business.

(c) DISCLOSURES TO INDIVIDUALS.—

(1) IN GENERAL.—A data broker shall, upon the request of an individual, disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained specifically for disclosure to third parties that request information on that individual in the ordinary course of business in the databases or systems of the data broker at the time of such request.

(2) INFORMATION ON HOW TO CORRECT INACCURACIES.—The disclosures required under paragraph (1) shall also include guidance to individuals on procedures for correcting inaccuracies.

(d) DISCLOSURE TO INDIVIDUALS OF ADVERSE ACTIONS TAKEN BY THIRD PARTIES.—

(1) IN GENERAL.—In addition to any other rights established under this Act, if a person takes any adverse action with respect to any individual that is based, in whole or in part, on any information contained in a personal electronic record that is maintained, updated, or otherwise owned or possessed by a data broker, such person, at no cost to the affected individual, shall provide—

(A) written or electronic notice of the adverse action to the individual;

(B) to the individual, in writing or electronically, the name, address, and telephone number of the data broker that furnished the information to the person;

(C) a copy of the information such person obtained from the data broker; and

(D) information to the individual on the procedures for correcting any inaccuracies in such information.

(2) ACCEPTED METHODS OF NOTICE.—A person shall be in compliance with the notice requirements under paragraph (1) if such person provides written or electronic notice in the same manner and using the same methods as are required under section 313(1) of this Act.

(e) ACCURACY RESOLUTION PROCESS.—

(1) INFORMATION FROM A PUBLIC RECORD OR LICENSOR.—

(A) IN GENERAL.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information disclosed to such individual under subsection (c) that is obtained from a public record source or a license agreement, such data broker shall determine within 30 days whether the information in its system accurately and completely records the information available from the licensor or public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems does not accurately and completely record the information available from a public record source or licensor, the data broker shall—

(i) correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) provide such individual with the contact information of the public record or licensor.

(2) INFORMATION NOT FROM A PUBLIC RECORD SOURCE OR LICENSOR.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information not from a public record or licensor that was disclosed to the individual under subsection (c), the data broker shall, within 30 days of receiving notice of such dispute—

(A) review and consider free of charge any information submitted by such individual that is relevant to the completeness or accuracy of the disputed information; and

(B) correct any information found to be incomplete or inaccurate and provide notice to such individual of whether and what information was corrected, if any.

(3) EXTENSION OF REVIEW PERIOD.—The 30-day period described in paragraph (1) may be extended for not more than 30 additional days if a data broker receives information from the individual during the initial 30-day period that is relevant to the completeness or accuracy of any disputed information.

(4) NOTICE IDENTIFYING THE DATA FURNISHER.—If the completeness or accuracy of any information not from a public record source or licensor that was disclosed to an individual under subsection (c) is disputed by such individual, the data broker shall provide, upon the request of such individual, the contact information of any data furnisher that provided the disputed information.

(5) DETERMINATION THAT DISPUTE IS FRIVOLOUS OR IRRELEVANT.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) through (3), a data broker may decline to investigate or terminate a review of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or intended to perpetrate fraud.

(B) NOTICE.—A data broker shall notify an individual of a determination under subparagraph (A) within a reasonable time by any means available to such data broker.

SEC. 202. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) PENALTIES.—Any data broker that violates the provisions of section 201 shall be subject to civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A data broker that intentionally or willfully violates the provisions of section 201 shall be subject to additional penalties in the amount of $1,000 per violation per day, to a maximum of an additional $250,000 per violation, while such violations persist.

(3) EQUITABLE RELIEF.—A data broker engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any data broker shall have the provisions of this title enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a data broker that violate this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title; or

(C) obtain civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in subparagraph (A) before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

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

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or civil action for a violation of this title, no attorney general of a State may, during the pendency of such proceeding or civil action, bring an action under this subsection against any defendant named in such civil action for any violation that is alleged in that civil action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title 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—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title establishes a private cause of action against a data broker for violation of any provision of this title.

SEC. 203. RELATION TO STATE LAWS.

No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 201, relating to individual access to, and correction of, personal electronic records held by data brokers.

SEC. 204. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 302 for protecting sensitive personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) subject to—

(i) examinations for compliance with the requirements of this Act by a Federal Functional Regulator or State Insurance Authority (as those terms are defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(ii) compliance with part 314 of title 16, Code of Federal Regulations.

(2) HIPPA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity is acting as a ''business associate'' as that term is defined in the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with requirements imposed under that Act and its implementing regulations.

(3) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a news report or periodical.

(d) SAFE HARBORS.—

(1) IN GENERAL.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information involved in the ordinary course of business of such business entity.

(2) LIMITATION.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of sensitive personally identifying information;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and

(C) protect against unauthorized access to use of sensitive personally identifying information that could result in substantial harm or inconvenience to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information;

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information; and

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—

(A) design its personal data privacy and security program to control the risks identified under paragraph (3); and

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information ;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals; and

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO SERVICE PROVIDERS.—In the event a business entity subject to this subtitle engages service providers not subject to this subtitle, such business entity shall—

(1) exercise appropriate due diligence in selecting those service providers for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(2) require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to section 301, this section, and subtitle B.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 303. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 301 or 302 shall be subject to civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 301 or 302 shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any data broker shall have the provisions of this subtitle enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a data broker that violate this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such violations persist, up to a maximum of $500,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

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

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this subtitle 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—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 304. RELATION TO OTHER LAWS.

(a) IN GENERAL.—No State may require any business entity subject to this subtitle to comply with any requirements with respect to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information.

(b) LIMITATIONS.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its implementing regulations, including those adopted or enforced by States.

Subtitle B—Security Breach Notification

SEC. 311. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, and restore the reasonable integrity of the data system and provide notice to law enforcement when required.

(3) BURDEN OF PROOF.—The agency, business entity, owner, or licensee required to provide notification under this section shall have the burden of demonstrating that all notifications were made as required under this subtitle, including evidence demonstrating the reasons for any delay.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement agency determines that the notification required under this section would impede a criminal investigation, such notification shall be delayed upon written notice from such Federal law enforcement agency to the agency or business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any law enforcement agency for acts relating to the delay of notification for law enforcement purposes under this subtitle.

SEC. 312. EXEMPTIONS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 311 shall not apply to an agency or business entity if the agency or business entity certifies, in writing, that notification of the security breach as required by section 311 reasonably could be expected to—

(A) cause damage to the national security; or

(B) hinder a law enforcement investigation or the ability of the agency to conduct law enforcement investigations.

(2) LIMITS ON CERTIFICATIONS.—An agency or business entity may not execute a certification under paragraph (1) to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a business entity, organization, or agency; or

(C) restrain competition.

(3) NOTICE.—In every case in which an agency or business agency issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the certification, shall be immediately provided to the United States Secret Service.

(4) SECRET SERVICE REVIEW OF CERTIFICATIONS.—

(A) IN GENERAL.—The United States Secret Service may review a certification provided by an agency under paragraph (3), and shall review a certification provided by a business entity under paragraph (3), to determine whether an exemption under paragraph (1) is merited. Such review shall be completed not later than 10 business days after the date of receipt of the certification, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review under subparagraph (A) the United States Secret Service shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

(C) TIMING.—If the United States Secret Service requests additional information under subparagraph (A), the United States Secret Service shall notify the agency or business entity not later than 10 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) SAFE HARBOR.—An agency or business entity will be exempt from the notice requirements under section 311, if—

(1) a risk assessment concludes that—

(A) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the encryption of such information establishing a presumption that no significant risk exists; or

(B) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the rendering of such sensitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, establishing a presumption that no significant risk exists;

(2) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the United States Secret Service, the agency or business entity notifies the United States Secret Service, in writing, of—

(A) the results of the risk assessment; and

(B) its decision to invoke the risk assessment exemption; and

(3) the United States Secret Service does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 311 if the business entity utilizes or participates in a security program that—

(A) is designed to block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption by this subsection does not apply if—

(A) the information subject to the security breach includes sensitive personally identifiable information, other than a credit card or credit card security code, of any type of the sensitive personally identifiable information identified in section 3; or

(B) the security breach includes both the individual's credit card number and the individual's first and last name.

SEC. 313. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 311 if it provides both:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person exceeds 5,000.

SEC. 314. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 313, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(b) ADDITIONAL CONTENT.—Notwithstanding section 319, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 311(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 316. NOTICE TO LAW ENFORCEMENT.

(a) SECRET SERVICE.—Any business entity or agency shall notify the United States Secret Service of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been acquired by an unauthorized person exceeds 10,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide;

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

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.—The United States Secret Service shall be responsible for notifying—

(1) the Federal Bureau of Investigation, if the security breach involves espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code;

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

(3) the attorney general of each State affected by the security breach.

(c) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 14 days after discovery of the events requiring notice.

(2) Notice under subsection (b) shall be delivered not later than 14 days after the Service receives notice of a security breach from an agency or business entity.

SEC. 317. ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The Attorney General may bring a civil action in the appropriate United States

district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(c) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and shall not affect any other rights and remedies available under law.

(d) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting '', or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised,'' after ''identity theft report''.

SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle; or

(C) civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 317 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subtitle against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 319. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach, except as provided in section 314(b).

SEC. 320. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this subtitle.

SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

The United States Secret Service shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 312(b) and the response of the United States Secret Service to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 312(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service pursuant to this subtitle.

SEC. 322. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

Subtitle C—Office of Federal Identity Protection

SEC. 331. OFFICE OF FEDERAL IDENTITY PROTECTION.

(a) ESTABLISHMENT.—There is established in the Federal Trade Commission an Office of Federal Identity Protection.

(b) DUTIES.—The Office of Federal Identity Protection shall be responsible for assisting each consumer with—

(1) addressing the consequences of the theft or compromise of the personally identifiable information of that consumer;

(2) accessing remedies provided under Federal law and providing information about remedies available under State law;

(3) restoring the accuracy of—

(A) the personally identifiable information of that consumer; and

(B) records containing the personally identifiable information of that consumer that were stolen or compromised; and

(4) retrieving any stolen or compromised personally identifiable information of that consumer.

(c) ACTIVITIES.—In order to perform the duties required under subsection (b), the Office of Federal Identity Protection shall carry out the following activities:

(1) Establish a website, easily and conspicuously accessible from ftc.gov, dedicated to assisting consumers with the retrieval of the stolen or compromised personally identifiable information of the consumer.

(2) Maintain a toll-free phone number to help answer questions concerning identity theft from consumers.

(3) Establish online and offline consumer-service teams to assist consumers seeking the retrieval of the personally identifiable information of the consumer.

(4) Provide guidance and information to service organizations or pro bono legal services programs that offer individualized assistance or counseling to victims of identity theft.

(5) Establish a reasonable standard for determining when an individual becomes a victim of identity theft.

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

(7) Permit an individual to use the Office of Federal Identity Protection certification—

(A) in all Federal, State, and local jurisdictions, in lieu of a police report or any other document required by State or local law, as a prerequisite to accessing business records of transactions done by someone claiming to be the individual; and

(B) to establish the eligibility of that individual for—

(i) the fraud alert protections under section 605A of the Fair Credit Reporting Act (15 U.S.C. 1681c–1); and

(ii) the reporting protections under section 605B(a) of the Fair Credit Reporting Act (15 U.S.C. 1681c–2(a)).

(8) Coordinate, as the Office determines necessary, with the designated Chief Privacy Officer of each Federal agency, or any other designated senior official in such agency in charge of privacy, in order to meet the duties of assisting consumers as required under subsection (b).

(9) In addition to the requirements in paragraphs (1) through (7), the Federal Trade

Commission shall promulgate regulations that enable the Office of Federal Identity Protection to help consumers restore their stolen or otherwise compromised personally identifiable information quickly and inexpensively.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the Office of Federal Identity Protection such sums as are necessary for fiscal year 2010 and each of the 4 succeeding fiscal years.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards totaling more than $500,000 and entered into after the date of enactment of this Act with data brokers, the Administrator of the General Services Administration shall evaluate—

(1) the data privacy and security program of a data broker to ensure the privacy and security of data containing personally identifiable information, including whether such program adequately addresses privacy and security threats created by malicious software or code, or the use of peer-to-peer file sharing software;

(2) the compliance of a data broker with such program;

(3) the extent to which the databases and systems containing personally identifiable information of a data broker have been compromised by security breaches; and

(4) the response by a data broker to such breaches, including the efforts by such data broker to mitigate the impact of such security breaches.

(b) COMPLIANCE SAFE HARBOR.—The data privacy and security program of a data broker shall be deemed sufficient for the purposes of subsection (a), if the data broker complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of personally identifiable information involved in the ordinary course of business of such data broker.

(c) PENALTIES.—In awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, the Administrator of the General Services Administration shall—

(1) include monetary or other penalties—

(A) for failure to comply with subtitles A and B of title III; or

(B) if a contractor knows or has reason to know that the personally identifiable information being provided is inaccurate, and provides such inaccurate information; and

(2) require a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(A) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(B) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(C) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(d) LIMITATION.—The penalties under subsection (c) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source or licensor.

SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECURITY PRACTICES OF CONTRACTORS AND THIRD PARTY BUSINESS ENTITIES.

Section 3544(b) of title 44, United States Code, is amended—

(1) in paragraph (7)(C)(iii), by striking ''and'' after the semicolon;

(2) in paragraph (8), by striking the period and inserting ''; and''; and

(3) by adding at the end the following:

''(9) procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information (as that term is defined in section 3 of the Personal Data Privacy and Security Act of 2009) and ensuring remedial action to address any significant deficiencies.''.

SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 208(b)(1) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) in subparagraph (A)(i), by striking ''or''; and

(2) in subparagraph (A)(ii), by striking the period and inserting ''; or''; and

(3) by inserting after clause (ii) the following:

''(iii) purchasing or subscribing for a fee to personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2009).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 1 year after the date of enactment of this Act, no Federal agency may enter into a contract with a data broker to access for a fee any database consisting primarily of personally identifiable information concerning United States persons (other than news reporting or telephone directories) unless the head of such department or agency—

(1) completes a privacy impact assessment under section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note), which shall subject to the provision in that Act pertaining to sensitive information, include a description of—

(A) such database;

(B) the name of the data broker from whom it is obtained; and

(C) the amount of the contract for use;

(2) adopts regulations that specify—

(A) the personnel permitted to access, analyze, or otherwise use such databases;

(B) standards governing the access, analysis, or use of such databases;

(C) any standards used to ensure that the personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal agency;

(D) standards limiting the retention and redisclosure of personally identifiable information obtained from such databases;

(E) procedures ensuring that such data meet standards of accuracy, relevance, completeness, and timeliness;

(F) the auditing and security measures to protect against unauthorized access, analysis, use, or modification of data in such databases;

(G) applicable mechanisms by which individuals may secure timely redress for any adverse consequences wrongly incurred due to the access, analysis, or use of such databases;

(H) mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies, or guidelines; and

(I) an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or illegitimate access or use of databases; and

(3) incorporates into the contract or other agreement totaling more than $500,000, provisions—

(A) providing for penalties—

(i) for failure to comply with title III of this Act; or

(ii) if the entity knows or has reason to know that the personally identifiable information being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; and

(B) requiring a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(ii) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study and audit and prepare a report on Federal agency actions to address the recommendations in the Government Accountability Office's April 2006 report on agency adherence to key privacy principles in using data brokers or commercial databases containing personally identifiable information.

(2) REPORT.—A copy of the report required under paragraph (1) shall be submitted to Congress.

SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER REQUIREMENTS.

(a) DESIGNATION OF THE CHIEF PRIVACY OFFICER.—Pursuant to the requirements under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (division H of Public Law 108–447; 118 Stat. 3199) that each agency designate a Chief Privacy Officer, the Department of Justice shall implement such requirements by designating a department-wide Chief Privacy Officer, whose primary role shall be to fulfill the duties and responsibilities of Chief Privacy Officer and who shall report directly to the Deputy Attorney General.

(b) DUTIES AND RESPONSIBILITIES OF CHIEF PRIVACY OFFICER.—In addition to the duties and responsibilities outlined under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (division H of Public Law 108–447; 118 Stat. 3199), the Department of Justice Chief Privacy Officer shall—

(1) oversee the Department of Justice's implementation of the requirements under section 403 to conduct privacy impact assessments of the use of commercial data containing personally identifiable information by the Department; and

(2) coordinate with the Privacy and Civil Liberties Oversight Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), in implementing this section.

By Mr. LEVIN (for himself and Mr. MCCAIN):

S. 1491. A bill to amend the Internal Revenue Code of 1986 to provide that corporate tax benefits based upon stock option compensation expenses be consistent with accounting expenses shown in corporate financial statements for such compensation; to the Committee on Finance.

Mr. LEVIN. Mr. President, Senator MCCAIN and I are introducing today a bill to eliminate Federal corporate tax breaks that give special tax treatment to corporations that pay their executives with stock options. It is called the Ending excessive Corporate Deductions for Stock Options Act, and it has been endorsed by OMB Watch, the Consumer Federation of America, the Tax Justice Network-USA, and the AFL–CIO.

We are in a financial crisis. We are spending hundreds of billions of taxpayer dollars to try to stop the housing bust and prop up Wall Street. Too many of the middle class are watching the American dream slip away, while executives are getting mutli-million dollar compensation packages.

At the same time, mismatched stock option accounting and tax rules are shortchanging the Treasury to the tune of billions of dollars each year, while fueling the growing chasm between executive pay and average worker pay. The mismatch is this: companies are allowed to report one set of stock option compensation expenses to investors and the public through their public financial statements, and a completely different set of expenses to the Internal Revenue Service, IRS, on their tax returns. Put simply, our precious tax dollars are being wasted by an outdated and unfair corporate tax loophole that encourages corporations to hand out massive stock option grants to their executives. It is time to put an end to the excessive tax deductions being reaped by corporations at taxpayers' expense.

J.P. Morgan once said that executive pay should not exceed 20 times average worker pay. In the United States, in 1990, average pay for the chief executive officer of a large U.S. corporation was 100 times average worker pay. Recently, CEO pay was nearly 400 times that of the average worker.

The single biggest factor responsible for this massive pay gap is stock options. Stock options are a huge contributor to executive pay. A key factor encouraging companies to pay their executives with stock options is the misguided Federal tax system that favors stock options over other types of compensation. Stock options give employees the right to buy company stock at a set price for a specified period of time, often 5 or 10 years. Virtually every CEO in America is paid with stock options, which are a major contributor to sky-high executive pay. According to Forbes magazine, in 2008, the CEOs at the 500 largest U.S. companies took home a combined $5.7 billion, averaging $11.4 million each.

For example, according to an Equilar Inc. analysis of 2008 filings with the Securities and Exchange Commission, SEC, Oracle Corporation's CEO was granted options estimated in value at more than $71 million just last year. That grant was on top of the pay he received from vested and exercised stock options given to him by his company in the past. In 2008 alone, those stock options amounted to a personal gain of more than $543 million. That is $543 million in stock option gains in a single year. Stunningly, his company gets to deduct this outlandish ''compensation'' from its taxes—even though the company never paid him that amount, and even though the existing tax code generally limits corporate deductions for executive pay to $1 million per executive.

Oracle's CEO was not alone. Equilar has identified dozens of U.S. executives who obtained tens of millions or even hundreds of millions of dollars from stock options in 2008. For example, the CEO of Qualcomm Inc., had $209 million in stock options gains in 2008, while the CEO of Occidental Petroleum had gains of $184 million.

Between the repricing of some stock options and grants being made while stock prices are low, the recent stock market recovery will likely mean that many executives will continue to reap astronomical stock option-related compensation, and their companies will continue to reap unwarranted tax deductions from stock options gains.

Why do corporate executives have so many stock options to cash in? A key reason is that U.S. accounting rules allow companies to report their stock option expenses one way on the corporate books, while Federal tax rules require them to report the same stock options a completely different way on their tax returns. In most cases, the resulting book expense is far smaller than the resulting tax deduction. That means, under current U.S. accounting and tax rules, stock option tax deductions taken by corporations often far exceed the recorded stock option expenses shown on the companies' books. The result is a tax windfall.

Stock options are the only type of compensation where the Federal tax code permits companies to claim a bigger deduction on their tax returns than the corresponding expense on their books. For all other types of compensation—cash, stock, bonuses, and more—the tax return deduction equals the book expense. In fact, companies cannot deduct more than the compensation expense shown on their books, because that would be tax fraud. The sole exception to this rule is stock options. In the case of stock options, the tax code allows companies to claim a tax deduction that can be two, three, ten or one hundred times larger than the expense shown on their books.

When a company's compensation committee learns that stock options can produce a low compensation expense on the books, while generating a generous tax deduction that is multiple times larger, it creates a temptation for the company to pay its executives with stock options instead of cash or stock. It is a classic case of U.S. tax policy creating an unintended incentive for corporations to act in a particular way.

This bill is particularly timely given the new administration's stated goals to close unfair corporate tax loopholes, strengthen tax fairness, and reign in excessive executive compensation. Given the current financial crisis, staggering health care costs, and ongoing defense needs, now more than ever, we cannot afford this multi-billion dollar loss to the Treasury.

To understand why this bill is needed it helps to understand how stock option accounting and tax rules got so out of kilter with each other in the first place.

Calculating the cost of stock options may sound straightforward, but for years, companies and their accountants engaged the Financial Accounting Standards Board (FASB) in an all-out, knock-down battle over how companies should record stock option compensation expenses on their books.

U.S. publicly traded corporations are required by law to follow Generally Accepted Accounting Principles, GAAP, issued by FASB, which is overseen by the SEC. For many years, GAAP allowed U.S. companies to issue stock options to employees and, unlike any other type of compensation, report a zero compensation expense on their books, so long as, on the grant date, the stock option's exercise price equaled the market price at which the stock could be sold.

Assigning a zero value to stock options that routinely produce huge amounts of executive pay provoked deep disagreements within the accounting community. In 1993, FASB proposed assigning a ''fair value'' to stock options on the date they are granted to an employee, using mathematical valuation tools. FASB proposed further that companies include that amount as a compensation expense on their financial statements. A battle over stock option expensing followed, involving the accounting profession, corporate executives, FASB, the SEC, and Congress.

In the end, after years of fighting and negotiation, FASB issued a new accounting standard, Financial Accounting Standard, FAS, 123R, which was endorsed by the SEC and became mandatory for all publicly traded corporations in 2005. In essence, FAS 123R requires all companies to record a compensation expense equal to the fair value on grant date of all stock options provided to an employee in exchange for the employee's services.

The details of this accounting rule are complex, because they reflect an effort to accommodate varying viewpoints on the true cost of stock options. Companies are allowed to use a variety of mathematical models, for

example, to calculate a stock option's fair value. Option grants that vest over time are expensed over the specified period so that, for example, a stock option which vests over four years results in 25 percent of the cost being expensed each year. If a stock option grant never vests, the rule allows any previously booked expense to be recovered. On the other hand, stock options that do vest are required to be fully expensed, even if never exercised, because the compensation was actually awarded. These and other provisions of this hard-fought accounting rule reflect painstaking judgments on how to show a stock option's value.

Opponents of the new accounting rule had predicted that, if implemented, it would severely damage U.S. capital markets. They warned that stock option expensing would eliminate corporate profits, discourage investment, depress stock prices, and stifle innovation. 2006 was the first year in which all U.S. publicly traded companies were required to expense stock options. Instead of tumbling, both the New York Stock Exchange and Nasdaq turned in strong performances, as did initial public offerings by new companies. The dire predictions were wrong. Stock option expensing has been fully implemented without any detrimental impact to the markets.

During the years the battle raged over stock option accounting, relatively little attention was paid to the taxation of stock options. Section 83 of the tax code, first enacted in 1969 and still in place after four decades, is the key statutory provision. It essentially provides that, when an employee exercises compensatory stock options, the employee must report as income the difference between what the employee paid to exercise the options and the market value of the stock received. The corporation can then take a mirror deduction for whatever amount of income the employee realized.

For example, suppose a company gave an executive options to buy 1 million shares of the company stock at $10 per share. Suppose, 5 years later, the executive exercised the options when the stock was selling at $30 per share. The executive's income would be $20 per share for a total of $20 million. The executive would declare $20 million as ordinary income, and in the same year, the company would take a corresponding tax deduction for $20 million.

The two main problems with this approach are that: the deduction amount is significantly greater than the value of what the company gave away, often years earlier, and the $20 million in income obtained by the executive did not come out of the company's coffers. In most cases, the $20 million was paid by unrelated parties on the stock market. Yet the tax code allowed the corporation to declare the $20 million as a business expense and take it as a tax deduction. The reasoning was that the exercise date value was the only way to get a clear figure for stock option tax deduction purposes. That reasoning lost its persuasive character, however, once consensus was reached on how to calculate stock option expenses when granted.

Stock option accounting and tax rules have evolved separately over the years and are now at odds with each other. Accounting rules require companies to expense stock options on their books on the grant date. Tax rules provide that companies deduct stock option expenses on the exercise date. Companies have to report the grant date expense to investors on their financial statements, and the exercise date expense on their tax returns. The financial statements report on all stock options granted during the year, while the tax returns report on all stock options exercised during the year. In short, company financial statements and tax returns identify expenses for different groups of stock options, using different valuation methods, and resulting in widely divergent stock option expenses for the same year.

To examine the nature and consequences of the stock option book-tax differences, the Permanent Subcommittee on Investigations, which I chair, initiated an investigation and held a hearing 2 years ago, in June 2007. Here is what we found.

To test just how far the book and tax figures for stock options diverge, the Subcommittee contacted a number of companies to compare the stock option expenses they reported for accounting and tax purposes. The Subcommittee asked each company to identify stock options that had been exercised by one or more of its executives from 2002 to 2006. The Subcommittee then asked each company to identify the compensation expense they reported on their financial statements versus the compensation expense on their tax returns. In addition, we asked the companies' help in estimating what effect the new accounting rule would have had on their book expense if it had been in place when their stock options were granted. At the hearing, we disclosed the resulting stock option data for 9 companies, including three companies that were asked to testify. The Subcommittee very much appreciated the cooperation and assistance provided by the nine companies we worked with.

The data provided by the companies showed that, under then existing rules, the nine companies showed a zero expense on their books for that stock options that had been awarded to their executives, but claimed millions of dollars in tax deductions for the same compensation. The one exception was Occidential Petroleum which, in 2005, began voluntarily expensing its stock options, but even this company reported significantly greater tax deductions than the stock option expenses shown on its books. When the Subcommittee asked the companies what their book expense would have been if the new FASB rule had been in effect, all nine calculated book expenses that remained dramatically lower than their tax deductions. Altogether the 9 companies calculated that they would have claimed $1 billion more in stock option tax deductions than they would have shown as book expenses, even using the tougher new accounting rule. Let me repeat that—just nine companies produced a stock option book-tax difference of more than $1 billion.

KB Home, for example, is a company that builds residential homes. Its stock price had more than quadrupled over the past 10 years. Over the same time period, it had repeatedly granted stock options to its then CEO. Company records show that, over five years, KB Home gave him 5.5 million stock options of which, by 2006, he had exercised more than 3 million.

With respect to those 3 million stock options, KB Home recorded a zero expense on its books. Had the new accounting rule been in effect, KB Home calculated that it would have reported on its books a compensation expense of about $11.5 million. KB Home also disclosed that the same 3 million stock options enabled it to claim compensation expenses on its tax returns totaling about $143.7 million. In other words, KB Home claimed a $143 million tax deduction for expenses that on its books, under current accounting rules, would have totaled $11.5 million. That's a tax deduction 12 times bigger than the book expense.

Occidental Petroleum disclosed a similar book-tax discrepancy. This company's stock price had also skyrocketed, dramatically increasing the value of the 16 million stock options granted to its CEO since 1993. Of the 12 million stock options the CEO actually exercised over a five-year period, Occidental Petroleum claimed a $353 million tax deduction for a book expense that, under current accounting rules, would have totaled just $29 million. That's a book-tax difference of more than 1200 percent.

Similar book-tax discrepancies applied to the other companies we examined. Cisco System's CEO exercised nearly 19 million stock options over 5 years, and provided the company with a $169 million tax deduction for a book expense which, under current accounting rules, would have totaled about $21 million. UnitedHealth's former CEO exercised over 9 million stock options in 5 years, providing the company with a $318 million tax deduction for a book expense which would have totaled about $46 million. Safeway's CEO exercised over 2 million stock options, providing the company with a $39 million tax deduction for a book expense which would have totaled about $6.5 million.

Altogether, these nine companies took stock option tax deductions totaling $1.2 billion, a figure 5 times larger than the $217 million that their combined stock option book expenses would have been. The resulting $1 billion in excess tax deductions represents

a tax windfall for these companies simply because they issued lots of stock options to their CEOs.

Tax rules that produce huge tax deductions that are many times larger than the related stock option book expenses give companies an incentive to issue massive stock option grants, because they know the stock options will produce a relatively small hit to the profits shown on their books, while also knowing that they are likely to get a much larger tax deduction that can dramatically lower their taxes.

The data we gathered for nine companies alone disclosed stock option tax deductions that were five times larger than their book expenses, generating over $1 billion in excess tax deductions. To gauge whether the same tax gap applied to stock options across the country as a whole, the Subcommittee asked the IRS to perform an analysis of some newly obtained stock option data.

For the first time in 2004, large corporations were required to file a new tax Schedule M–3 with their tax returns. The M–3 Schedule asks companies to identify differences in how they report corporate income to investors versus what they report to Uncle Sam, so that the IRS can track and analyze significant book-tax differences.

This data shows that, for corporate tax returns filed form July 1, 2005 to June 30, 2006, the first full year in which it was available, companies' stock option tax deductions totaled about $61 billion more than their stock options expenses on their books. Similar data for July 1, 2006 to June 30, 2007, showed that the excess stock option tax deductions totaled about $48 billion. In addition, the IRS data shows that nearly 60 percent of the excess tax deductions in 2007 were attributable to only 100 corporations; 75 percent were attributable to only 250 corporations. The IRS also determined that stock options were one of the most important factors why corporations reported different income on their books compared to their tax returns.

Claiming these massive stock option tax deductions enabled U.S. corporations, as a whole, to legally reduce payment of their taxes by billions of dollars, perhaps as much as $10 billion, $15 billion, even $20 billion per year.

There were other surprises in the data as well. One set of issues disclosed by the data involves what happens to unexercised stock options. Under the current mismatched set of accounting and tax rules, stock options which are granted, vested, but never exercised by the option holder turn out to produce a corporate book expense but no tax deduction.

Cisco Systems told the Subcommittee, for example, that in addition to the 19 million exercised stock options previously mentioned, their CEO held about 8 million options that, due to a stock price drop, would likely expire without being exercised. Cisco calculated that, had FAS 123R been in effect a the time those options were granted, the company would have had to show a $139 million book expense, but would never be able to claim a tax deduction for this expense since the options would never be exercised. Apple made a similar point. It told the Subcommittee that, in 2003, it allowed its CEO to trade 17.5 million in underwater stock options for 5 million shares of restricted stock. That trade meant the stock options would never be exercised and, under current rules, would produce a book expense without ever producing a tax deduction.

In both of these cases, under FAS 123R, it is possible that the stock options given to a corporate executive would have produced a reported book expense greater than the company's tax deduction. While the M–3 data indicates that, overall, accounting expenses lag far behind claimed tax deductions, the possible financial impact on an individual company of a large number of unexercised stock options is additional evidence that existing stock option accounting and tax rules are out of kilter and should be brought into alignment. Under our bill, if a company incurred a stock option expense, it would always be able to claim a tax deduction for that expense.

Another set of issues brought to light by theIRS data focuses on the fact that the current stock option tax deduction is typically claimed years later than the initial book expense. Normally, a corporation dispenses compensation to an employee and takes a tax deduction in the same year for the expense. The company controls the timing and amount of the compensation expense and the corresponding tax deduction. With respect to stock options, however, corporations may have to wait years to see if, when, and how much of a deduction can be taken. That is because the corporate tax deduction is wholly dependent upon when an individual corporate executive decides to exercise his or her stock options.

Our bill would require that, when the company gives away something of value, it reflects that expense on its books and claims that same expense on its tax return. The company, and the government, should not have to wait to see whether the stock options given to executives later increased in value and were exercised. As with any other form of compensation, the company should determine the value of what it is giving away, and take the appropriate tax deduction at that time.

UnitedHealth, for example, told the Subcommittee that it gave its former CEO 8 million stock options in 1999, of which, by 2006, only about 730,000 had been exercised. It did not know if or when its former CEO would exercise the remaining 7 million options, and so could not calculate when or how much of a tax deduction it would be able to claim for this compensation expense.

If the rules for stock option tax deductions were changed as suggested in our bill, companies would typically be able to take the deduction years earlier than they do now, without waiting to see if and when particular options are exercised. Companies would also be allowed to deduct stock options that are vested but never exercised. In addition, by requiring stock option expenses to be deducted in the same year they appear on the company books, stock options would become consistent with how other forms of compensation are treated in the tax code.

Right now, U.S. stock option accounting and tax rules are mismatched, misaligned, and out of kilter. They allow companies collectively to deduct billions of dollars in stock option expenses in excess of the expenses that actually appear on the company books. They disallow tax deductions for stock options that are given as compensation but never exercised. They often force companies to wait years to claim a tax deduction for a compensation expense that could and should be claimed in the same year it appears on the company books.

The Levin-McCain bill we are introducing today would cure these problems. It would bring stock option accounting and tax rules into alignment, so that the two sets of rules would apply in a consistent manner. It would accomplish that goal simply by requiring the corporate stock option tax deduction to be no greater than the stock option expenses shown on the corporate books each year.

Specifically, the bill would end use of the current stock option deduction under Section 83 of the tax code, which allows corporations to deduct stock option expenses when exercised in an amount equal to the income declared by the individual exercising the option, replacing it with a new Section 162(q), which would require companies to deduct the stock option expenses shown on their books each year.

The bill would apply only to corporate stock option deductions; it would make no changes to the rules that apply to individuals who have been given stock options as part of their compensation. Individuals would still report their compensation on the day they exercised their stock options. They would still report as income the difference between what they paid to exercise the options and the fair market value of the stock they received upon exercise. The gain would continue to be treated as ordinary income rather than a capital gain, since the option holder did not invest any capital in the stock prior to exercising the stock option and the only reason the person obtained the stock was because of the services they performed for the corporation.

The amount of income declared by the individual after exercising a stock option will likely often be greater than the stock option expense booked and deducted by the corporation who employed that individual. That's in part because the individual's gain often comes years later than the original

stock option grant, and the underlying stock will usually have gained in value. In addition, the individual's gain is typically provided, not by the corporation that supplied the stock options years earlier, but by third parties active in the stock market.

Consider the same example discussed earlier of an executive who exercises options to buy 1 million shares of stock at $10 per share, obtains the shares from the corporation, and then immediately sells them on the open market for $30 per share, making a toal profit of $20 million. The individual's corporation didn't supply the $20 million. Just the opposite. Rather than paying cash to its executive, the corporation received a $10 million payment from the executive in exchange for the 1 million shares. The $20 million profit from selling the shares was paid, not by the corporation, but by third parties in the marketplace who purchased the stock. That is why it makes no sense for the company to declare as an expense the amount of profit that an employee—or former employee—obtained from unrelated parties in the marketplace.

The bill we are introducing today would put an end to the current approach of using the stock option income declared by an individual as the tax deduction claimed by the corporation that supplied the stock options. It would break that old artificial symmetry and replace it with a new symmetry—one in which the corporation's stock option tax deduction would match its book expense.

I describe the current approach to corporate stock option deductions as artificial, because it uses a construct in the tax code that, when first implemented 40 years ago, enabled corporations to calculate their stock option expense on the exercise date, when there was no consensus on how to calculate stock option expenses on the grant date. The artificiality of the approach is demonstrated by the fact that it allows companies to claim a deductible expense for money that comes not from company coffers, but from third parties in the stock market. Now that U.S. accounting rules require the calculation of stock option expenses on the grant date, however, there is no longer any need to rely on an artificial construct that calculated corporate stock option expenses on the exercise date using third party funds.

It is also important to note that the bill would not affect in any way current tax provisions that provide favored tax treatment to so-called Incentive Stock Options under Sections 421 and 422 of the tax code. Under those sections, in certain circumstances, corporations can surrender their stock option deductions in favor of allowing their employees with stock option gains to be taxed at a capital gains rate instead of ordinary income tax rates. Many start-up companies use these types of stock options, because they don't yet have taxable profits and don't need a stock option tax deduction. So they forfeit their stock option corporate deduction in favor of giving their employees more favorable treatment of their stock option income. Incentive Stock Options would not be affected by our legislation and would remain available to any corporation providing stock options to its employees.

The bill would make one other important change to the tax code as it relates to corporate stock option tax deductions. In 1993, Congress enacted a $1 million cap on the compensation that a corporation can deduct from its taxes, so taxpayers would not be forced to subsidize excessive executive pay. However, the cap was not applied to stock options, allowing companies to deduct any amount of stock option compensation, without limit.

By not applying the $1 million cap to stock option compensation, the tax code created a significant incentive for corporations to pay their executives with stock options. Indeed, it is very common for executives to have salaries of $1 million, while simultaneously receiving millions of dollars more in stock options. It is effectively meaningless to cap deductions for executive salary compensation but not also for stock options.

Further, while corporate directors may be comfortable diluting their shareholders' interests and doling out massive amounts of stock options, that does not mean that the taxpayers should subsidize it. This bill would eliminate this favored treatment of executive stock options by making deductions for this type of compensation subject to the same $1 million cap that applies to other forms of compensation covered by Section 162(m).

The bill also contains several technical provisions. First, it would make a conforming change to the research tax credit so that stock option expenses claimed under that credit would match the stock option deductions taken under the new tax code section 162(q). Second, the bill would authorize the Secretary of the Treasury to adopt regulations governing how to calculate the deduction for stock options issued by a parent corporation to the employees of a subsidiary.

Finally, the bill contains a transition rule for applying the new Section 162(q) stock option tax deduction to existing and future stock option grants. This transition rule would make it clear that the new tax deduction would not apply to any stock option exercised prior to the date of enactment of the bill.

The bill would also allow the old Section 83 deduction rules to apply to any option which was vested prior to the effective date of Financial Accounting Standard, FAS, 123R, and exercised after the date of enactment of the bill. The effective date of FAS 123R is June 15, 2005 for most corporations, and December 31, 2005 for most small businesses. Prior to the effective date of FAS 123R, most corporations would have shown a zero expense on their books for the stock options issued to their executives and, thus, would be unable to claim a tax deduction under the new Section 162(q). For that reason, the bill would allow these corporations to continue to use Section 83 to claim stock option deductions on their tax returns.

For stock options that vested after the effective date of FAS 123R and were exercised after the date of enactment, the bill takes another tack. Under FAS 123R, these corporations would have had to show the appropriate stock option expense on their books, but would have been unable to take a tax deduction until the executive actually exercised the option. For these options, the bill would allow corporations to take an immediate tax deduction—in the first year that the bill is in effect—for all of the expenses shown on their books with respect to these options. This ''catch-up deduction'' in the first year after enactment would enable corporations, in the following years, to begin with a clean slate so that their tax returns the next year would reflect their actual stock option book expenses for that same year.

After that catch-up year, all stock option expenses incurred by a company each year would be reflected in their annual tax deductions under the new Section 162(q).

The current differences between accounting and tax rules for stock options make no sense.

The current book-tax difference is the historical product of accounting and tax policies that have not been coordinated or integrated. The resulting mismatch has allowed companies to take tax deductions that are usually many times larger than the actual stock option expenses shown on their books, at the expense of the Treasury (i.e., other taxpayers). Companies are incentivized to dole out excessive options packages, producing outsized executive pay, while being allowed to reflect much smaller ''expenses'' on their books. They get to avoid paying their fair share to Uncle Sam by simply giving their executives the rights to huge sums of money from the financial markets.

Right now, stock options are the only compensation expense where the tax code allows companies to deduct more than their book expenses. In the last year for which the data is available, companies used the existing book-tax disparity to claim $48 billion more in stock option tax deductions than the expenses shown on their books. In these times of financial crisis, we cannot afford this multi-billion dollar loss to the Treasury, not only because of the need to finance the mounting costs of rescuing the economy, but also because this stock option book-tax difference contributes to the anger and social disruption caused by the ever deepening chasm between the pay of executives and the pay of average workers.

The Obama administration has pledged itself to closing unfair corporate tax loopholes and to returning sanity to executive pay. It should start with supporting the ending of excessive stock option corporate deductions. I urge my colleagues to join Senator MCCAIN and me in enacting this bill into law this year.

Mr. President, I ask unanimous consent that the text of the bill and a bill summary be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1491

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Ending Excessive Corporate Deductions for Stock Options Act''.

SEC. 2. CONSISTENT TREATMENT OF STOCK OPTIONS BY CORPORATIONS.

(a) CONSISTENT TREATMENT FOR WAGE DEDUCTION.—

(1) IN GENERAL.—Section 83(h) of the Internal Revenue Code of 1986 (relating to deduction of employer) is amended—

(A) by striking ''In the case of'' and inserting:

''(1) IN GENERAL.—In the case of'', and

(B) by adding at the end the following new paragraph:

''(2) STOCK OPTIONS.—In the case of property transferred to a person in connection with the exercise of a stock option, any deduction by the employer related to such stock option shall be allowed only under section 162(q) and paragraph (1) shall not apply.''.

(2) TREATMENT OF COMPENSATION PAID WITH STOCK OPTIONS.—Section 162 of such Code (relating to trade or business expenses) is amended by redesignating subsection (q) as subsection (r) and by inserting after subsection (p) the following new subsection:

''(q) TREATMENT OF COMPENSATION PAID WITH STOCK OPTIONS.—

''(1) IN GENERAL.—In the case of compensation for personal services that is paid with stock options, the deduction under subsection (a)(1) shall not exceed the amount the taxpayer has treated as an expense with respect to such stock options for the purpose of ascertaining income, profit, or loss in a report or statement to shareholders, partners, or other proprietors (or to beneficiaries), and shall be allowed in the same period that the accounting expense is recognized.

''(2) SPECIAL RULES FOR CONTROLLED GROUPS.—The Secretary shall prescribe rules for the application of paragraph (1) in cases where the stock option is granted by a parent or subsidiary corporation (within the meaning of section 424) of the employer corporation.''.

(b) CONSISTENT TREATMENT FOR RESEARCH TAX CREDIT.—Section 41(b)(2)(D) of the Internal Revenue Code of 1986 (defining wages for purposes of credit for increasing research expenses) is amended by inserting at the end the following new clause:

''(iv) SPECIAL RULE FOR STOCK OPTIONS.—The amount which may be treated as wages for any taxable year in connection with the issuance of a stock option shall not exceed the amount allowed for such taxable year as a compensation deduction under section 162(q) with respect to such stock option.''.

(c) APPLICATION OF AMENDMENTS.—The amendments made by this section shall apply to stock options exercised after the date of the enactment of this Act, except that—

(1) such amendments shall not apply to stock options that were granted before such date and that vested in taxable periods beginning on or before June 15, 2005,

(2) for stock options that were granted before such date of enactment and vested during taxable periods beginning after June 15, 2005, and ending before such date of enactment, a deduction under section 162(q) of the Internal Revenue Code of 1986 (as added by subsection (a)(2)) shall be allowed in the first taxable period of the taxpayer that ends after such date of enactment,

(3) for public entities reporting as small business issuers and for non-public entities required to file public reports of financial condition, paragraphs (1) and (2) shall be applied by substituting ''December 15, 2005'' for ''June 15, 2005'', and

(4) no deduction shall be allowed under section 83(h) or section 162(q) of such Code with respect to any stock option the vesting date of which is changed to accelerate the time at which the option may be exercised in order to avoid the applicability of such amendments.

SEC. 3. APPLICATION OF EXECUTIVE PAY DEDUCTION LIMIT.

(a) IN GENERAL.—Subparagraph (D) of section 162(m)(4) of the Internal Revenue Code of 1986 (defining applicable employee remuneration) is amended to read as follows:

''(D) STOCK OPTION COMPENSATION.—The term 'applicable employee remuneration' shall include any compensation deducted under subsection (q), and such compensation shall not qualify as performance-based compensation under subparagraph (C).''.

(b) EFFECTIVE DATE.—The amendment made by this section shall apply to stock options exercised or granted after the date of the enactment of this Act.

SUMMARY OF THE ENDING EXCESSIVE CORPORATE DEDUCTIONS FOR STOCK OPTIONS ACT

SECTION 1—SHORT TITLE

''Ending Excessive Corporate Deductions for Stock Options Act''

SECTION 2—CONSISTENT TREATMENT OF STOCK OPTIONS BY CORPORATIONS

Eliminates favored tax treatment of corporate stock option deductions, in which corporations are currently allowed to deduct a higher stock option compensation expense on their tax returns than shown on their financial books—(1) creates a new corporate stock option deduction under a new tax code section 162(q) requiring the tax deduction to be consistent with the book expense, and (2) eliminates the existing corporate stock option deduction under tax code section 83(h) allowing excess deductions.

Allows corporations to deduct stock option compensation in the same year it is recorded on the company books, without waiting for the options to be exercised.

Makes a conforming change to the research tax credit so that stock option expenses under that credit will match the deductions taken under the new tax code section 162(q).

Authorizes Treasury to issue regulations applying the new deduction to stock options issued by a parent corporation to a subsidiary's employees.

Establishes a transition rule applying the new deduction to stock options exercised after enactment, permitting deductions under the old rule for options vested prior to adoption of Financial Accounting Standard (FAS) 123R (on expensing stock options) on June 15, 2005, and allowing a catch-up deduction in the first year after enactment for options that vested between adoption of FAS 123R and the date of enactment.

Makes no change to stock option compensation rules for individuals, or for incentive stock options that qualify under section 422 of the tax code.

SECTION 3—APPLICATION OF EXECUTIVE PAY DEDUCTION LIMIT

Eliminates favored treatment of corporate executive stock options under tax code section 162(m) by making executive stock option compensation deductions subject to the same $1 million cap on corporate deductions that applies to other types of compensation paid to the top executives of publicly held corporations. This approach mirrors that taken in the Economic Emergency Stabilization Act to address the financial crisis.

By Mr. REID (for Ms. MIKULSKI (for herself, Mr. BOND, Mrs. GILLIBRAND, Mr. MENENDEZ, Mr. BURR, and Ms. COLLINS)):

S. 1492. A bill to amend the Public Health Service Act to fund breakthroughs in Alzheimer's disease research while providing more help to caregivers and increasing public education about prevention; to the Committee on Health, Education, Labor, and Pensions.

Ms. MIKULSKI. Mr. President, today, I rise to introduce the Alzheimer's Breakthrough Act of 2009. This critical bipartisan legislation passed the HELP Committee in 2007, but it has yet to pass the Senate. My hope is that we can finish the job this year and finally get this legislation signed into law.

Alzheimer's' disease is an alarming and mounting crisis that we must address. Today there are over five million Americans living with Alzheimer's disease. That number is expected to triple by 2050 in a nation where ten million Americans care for a sick family member.

We know a lot about Alzheimer's disease but it's been 100 years since it was first diagnosed, and we still have no cure or proven ways to prevent the disease. Urgency is needed in developing better treatments and better assistance for families impacted by the disease as the baby boom generation ages. If nothing is done, Alzheimer's will cost Medicare and Medicaid $19.89 trillion between 2010 and 2050.

The Alzheimer's Breakthrough Act of 2009 responds to this crisis in four ways.

First, it doubles funding for Alzheimer's research at NIH to $2 billion for fiscal year 2010, making Alzheimer's research a priority. Through this commitment, the bill gives researchers adequate resources to make breakthroughs in diagnosis, prevention and intervention, bringing us closer to a cure.

Second, the bill creates the National Summit on Alzheimer's. This Summit will bring together the Nation's best researchers, policymakers and public health professionals to discuss the most promising breakthroughs for saving lives and livelihood, and to generate priorities in moving forward in the fight against Alzheimer's.

Third, the act enhances public health activities related to Alzheimer's through the CDC's ''Roadmap to Maintaining Cognitive Health.''

Finally, the Alzheimer's Breakthrough Act provides family and caregiver support by expanding the Alzheimer's 24/7 call center, which provides crisis assistance and referrals to local community programs. The bill also expands the multilingual capacity of the call center.

America needs this legislation. Alzheimer's takes a toll on many victims. The disease is awful for the person living with it, emotionally and financially draining for caregivers and it is now costing the nation $175 billion annually, a number that could rise to $1 trillion annually by 2050.

We know the family of an Alzheimer's patient suffers gravely. The out-of-pocket cost of caring for an aging parent or spouse averages about $5,500 a year for necessities like groceries, household goods and drugs and medical copayments. If the care is long-distance, the cost could be up to $8,700 a year. Caregivers spend ten percent of their household income caring for a sick loved one who is suffering from this terrible disease.

Experts have told us ''we will lose opportunities if we don't move quickly'' and that ''we are at a crucial point where NIH funding can make a difference.'' We know about the long goodbye. Alzheimer's is a disease that affects millions of Americans including our All-American President Ronald Reagan and his beloved caregiver, First Lady Nancy Reagan. Now we need a response supported by millions that will lead to breakthroughs and ensure we are assisting patients and their families dealing with this disease on a daily basis.

Passage of the Alzheimer's Breakthrough Act of 2009 will help us advance the study and treatment of Alzheimer's to make a difference in the lives of millions of Americans and to equip caregivers with the resources and support services they need to care for their loved ones. This legislation is critical to the American public and America's future. We must act now.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1492

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Alzheimer's Breakthrough Act of 2009''.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Alzheimer's disease is a disorder that destroys cells in the brain. The disease is the leading cause of dementia, a condition that involves gradual memory loss, decline in the ability to perform routine tasks, disorientation, difficulty in learning, loss of language skills, impairment of judgment, and personality changes. As the disease progresses, people with Alzheimer's disease become unable to care for themselves. The loss of brain cells eventually leads to the failure of other systems in the body.

(2) An estimated 5,300,000 Americans have Alzheimer's disease and 1 in 10 individuals has a family member with the disease. By 2050, the number of individuals with the disease could reach 16,000,000 unless science finds a way to prevent or cure the disease.

(3) One in 8 people over the age of 65, and nearly half of those over the age of 85 have Alzheimer's disease. Younger people also get the disease.

(4) The Alzheimer's disease process may begin in the brain as many as 20 years before the symptoms of Alzheimer's disease appear. An individual will live an average of 4 to 6 years, and as many as 20 years, once the symptoms of Alzheimer's disease appear.

(5) In 2005, Medicare alone spent $91,000,000,000 for the care of individuals with Alzheimer's disease and this amount is projected to increase to $160,000,000,000 in 2010.

(6) Ninety-five percent of Medicare beneficiaries with Alzheimer's disease have one or more other chronic conditions that are common in the elderly, such as coronary heart disease (26 percent), congestive heart failure (16 percent), diabetes (23 percent), and chronic obstructive pulmonary disease (15 percent).

(7) Seven in 10 individuals with Alzheimer's disease live at home. Cost for care at home is higher for people with Alzheimer's disease than other individuals. Almost all families pay some out-of-pocket costs.

(8) Half of all nursing home residents have Alzheimer's disease or a related disorder. The average annual cost of Alzheimer's disease nursing home care is more than $77,000. Medicaid pays half of the total nursing home bill and helps 2 out of 3 residents pay for their care. Medicaid expenditures for nursing home care for people with Alzheimer's disease are estimated to increase from $21,000,000,000 in 2005 to $24,000,000,000 in 2010.

(9) In fiscal year 2007, the Federal Government spent an estimated $411,000,000 on Alzheimer's disease research. Over the next 40 years, Alzheimer's disease-related costs to Medicare and Medicaid alone are projected to total $20,000,000,000,000 in constant dollars, rising to over $1,000,000,000,000 per year by 2050. This amounts to less than a penny spent on Alzheimer's disease research for each dollar that the Federal Government spends on Alzheimer's disease-related costs each year.

(10) It is estimated that the annual value of the informal care system is $94,000,000,000. Family caregiving comes at enormous physical, emotional, and financial sacrifice, putting the whole system at risk.

(11) Almost 60 percent of caregivers of individuals with Alzheimer's disease are women, and over one-fourth have children or grandchildren under the age of 18 living at home. Caregiving leaves them less time for other family members and they are much more likely to report family conflicts because of their caregiving role.

(12) Most Alzheimer's disease caregivers work outside the home before beginning their caregiving careers, but caregiving forces them to miss work, cut back to part-time, take less demanding jobs, choose early retirement, or give up work altogether. As a result, in 2002, Alzheimer's disease cost American business an estimated $36,500,000,000 in lost productivity, as well as an additional $24,600,000,000 in business contributions to the total cost of care.

TITLE I—INCREASING THE FEDERAL COMMITMENT TO ALZHEIMER'S RESEARCH

SEC. 101. DOUBLING NIH FUNDING FOR ALZHEIMER'S DISEASE RESEARCH.

For the purpose of conducting and supporting research on Alzheimer's disease (including related activities under subpart 5 of part C of title IV of the Public Health Service Act (42 U.S.C. 285e et seq.)), there are authorized to be appropriated $2,000,000,000 for fiscal year 2010, and such sums as may be necessary for each of fiscal years 2011 through 2014.

SEC. 102. PRIORITY TO ALZHEIMER'S DISEASE RESEARCH.

Section 443 of the Public Health Service Act (42 U.S.C. 285e) is amended—

(1) by striking ''The general'' and inserting the following:

''(a) IN GENERAL.—The general;'' and

(2) by adding at the end the following:

''(b) PRIORITIES.—The Director of the Institute shall, in expending amounts appropriated to carry out this subpart, give priority to conducting and supporting Alzheimer's disease research.''.

SEC. 103. ALZHEIMER'S DISEASE PREVENTION INITIATIVE.

Section 443 of the Public Health Service Act (42 U.S.C. 285e), as amended by section 102, is further amended by adding at the end the following:

''(c) PREVENTION TRIALS.—The Director of the Institute shall increase the emphasis on the need to conduct Alzheimer's disease prevention trials within the National Institutes of Health.

''(d) NEUROSCIENCE INITIATIVE.—The Director of the Institute shall ensure that Alzheimer's disease is maintained as a high priority for the neuroscience initiative of the National Institutes of Health.''.

SEC. 104. ALZHEIMER'S DISEASE CLINICAL RESEARCH.

(a) CLINICAL RESEARCH.—Subpart 5 of part C of title IV of the Public Health Service Act (42 U.S.C. 285e et seq.) is amended by adding at the end the following:

''SEC. 445J. ALZHEIMER'S DISEASE CLINICAL RESEARCH.

''(a) IN GENERAL.—The Director of the Institute, pursuant to section 444(d), shall conduct and support cooperative clinical research regarding Alzheimer's disease. Such research shall include—

''(1) investigating therapies, interventions, and agents to detect, treat, slow the progression of, or prevent Alzheimer's disease;

''(2) enhancing the national infrastructure for the conduct of clinical trials on Alzheimer's disease;

''(3) developing and testing novel approaches to the design and analysis of such trials;

''(4) facilitating the enrollment of patients for such trials, including patients from diverse populations;

''(5) developing improved diagnostics and means of patient assessment for Alzheimer's disease;

''(6) the conduct of clinical trials on potential therapies, including readily available compounds such as herbal remedies and other alternative treatments;

''(7) research to develop better methods of early diagnosis, including the use of current imaging techniques; and

''(8) other research, as determined appropriate by the Director of the Institute after consultation with the Alzheimer's disease centers and Alzheimer's disease research centers established under section 445.

''(b) EARLY DIAGNOSIS AND DETECTION RESEARCH.—

''(1) IN GENERAL.—The Director of the Institute, in consultation with the directors of other relevant institutes and centers of the National Institutes of Health, shall conduct, or make grants for the conduct of, research related to the early detection, diagnosis, and prevention of Alzheimer's disease and of mild cognitive impairment or other potential precursors to Alzheimer's disease.

''(2) EVALUATION.—The research described in paragraph (1) may include the evaluation of diagnostic tests and imaging techniques.

''(3) STUDY.—Not later than 1 year after the date of enactment of this section, the Director of the Institute, in cooperation with the heads of other relevant Federal agencies, shall conduct a study, and submit to Congress a report, to estimate the number of individuals with early-onset Alzheimer's disease (those diagnosed before the age of 65) and related dementias in the United States, the causes of early-onset dementia, and the unique problems faced by such individuals, including problems accessing government services.

''(c) VASCULAR DISEASE.—The Director of the Institute, in consultation with the directors of other relevant institutes and centers of the National Institutes of Health, shall conduct, or make grants for the conduct of, research related to the relationship of vascular disease and Alzheimer's disease, including clinical trials to determine whether drugs developed to prevent cerebrovascular disease can prevent the onset or progression of Alzheimer's disease.

''(d) TREATMENTS AND PREVENTION.—The Director of the Institute shall place special emphasis on expediting the translation of research findings under this section into effective treatments and prevention strategies for individuals at risk of Alzheimer's disease and other dementias.

''(e) NATIONAL ALZHEIMER'S COORDINATING CENTER.—The Director of the Institute may establish a National Alzheimer's Coordinating Center to facilitate collaborative research among the Alzheimer's Disease Centers and Alzheimer's Disease Research Centers established under section 445.''.

(b) ALZHEIMER'S DISEASE CENTERS.—Section 445(a)(1) of the Public Health Service Act (42 U.S.C. 285e–2(a)(1)) is amended by inserting '', outcome measures, and disease management,'' after ''treatment methods''.

SEC. 105. RESEARCH ON ALZHEIMER'S DISEASE CAREGIVING.

Section 445C of the Public Health Service Act (42 U.S.C. 285e–5) is amended—

(1) by striking ''SEC. 445C. RESEARCH PROGRAM AND PLAN (a)'' and inserting the following:

''SEC. 445C. RESEARCH ON ALZHEIMER'S DISEASE SERVICES AND CAREGIVING.

''(a) SERVICES RESEARCH.—'';

(2) by striking subsections (b), (c), and (e);

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

''(b) INTERVENTIONS RESEARCH.—The Director of the Institute shall, in collaboration with the directors of the other relevant institutes and centers of the National Institutes of Health, conduct, or make grants for the conduct of, clinical, social, and behavioral research related to interventions designed to help caregivers of patients with Alzheimer's disease and other dementias and improve patient outcomes.'';

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

(5) in subsection (c) (as redesignated by paragraph (4)), by striking ''the Director'' and inserting ''MODEL CURRICULA AND TECHNIQUES.—The Director''.

SEC. 106. NATIONAL SUMMIT ON ALZHEIMER'S DISEASE.

(a) IN GENERAL.—Not later than 3 years after the date of enactment of this Act, and every 3 years thereafter, the Secretary of Health and Human Services (referred to in this section as the ''Secretary'') shall convene a National Summit on Alzheimer's Disease to—

(1) provide a detailed overview of current research activities relating to Alzheimer's disease at the National Institutes of Health; and

(2) discuss and solicit input related to potential areas of collaboration between the National Institutes of Health and other Federal health agencies, including the Centers for Disease Control and Prevention, the Administration on Aging, the Agency for Healthcare Research and Quality, and the Health Resources and Services Administration, related to research, prevention, and treatment of Alzheimer's disease.

(b) PARTICIPANTS.—The summit convened under subsection (a) shall include researchers, representatives of academic institutions, Federal and State policymakers, public health professionals, and representatives of voluntary health agencies as participants.

(c) FOCUS AREAS.—The summit convened under subsection (a) shall focus on—

(1) a broad range of Alzheimer's disease research activities relating to biomedical research, prevention research, and caregiving issues;

(2) clinical research for the development and evaluation of new treatments for Alzheimer's disease;

(3) translational research on evidence-based and cost-effective best practices in the treatment and prevention of Alzheimer's disease;

(4) information and education programs for health care professionals and the public relating to Alzheimer's disease;

(5) priorities among the programs and activities of the various Federal agencies regarding Alzheimer's disease and other dementias; and

(6) challenges and opportunities for scientists, clinicians, patients, and voluntary organizations relating to Alzheimer's disease.

(d) REPORT.—Not later than 180 days after the date on which the summit is convened under subsection (a), the Director of the National Institutes of Health shall prepare and submit to the appropriate committees of Congress a report that includes a summary of the proceedings of the summit and a description of Alzheimer's disease research, education, and other activities that are conducted or supported through the National Institutes of Health.

(e) PUBLIC INFORMATION.—The Secretary shall make readily available to the public information about the research, education, and other activities relating to Alzheimer's disease and other related dementias, that are conducted or supported by the National Institutes of Health.

TITLE II—PUBLIC HEALTH PROMOTION AND PREVENTION OF ALZHEIMER'S DISEASE

SEC. 201. ENHANCING PUBLIC HEALTH ACTIVITIES RELATED TO COGNITIVE HEALTH, ALZHEIMER'S DISEASE, AND OTHER DEMENTIAS.

Part P of title III of the Public Health Service Act (42 U.S.C. 280g et seq.) is amended—

(1) by redesignating the second and third sections 399R as sections 399S and 399T, respectively; and

(2) by adding at the end the following:

''SEC. 399U. ALZHEIMER'S DISEASE PUBLIC EDUCATION CAMPAIGN.

''(a) IN GENERAL.—The Secretary, acting through the Director of the Centers for Disease Control and Prevention, shall directly or through grants, cooperative agreements, or contracts to eligible entities—

''(1) conduct, support, and promote the coordination of research, investigations, demonstrations, training, and studies relating to the control, prevention, and surveillance of the risk factors associated with cognitive health, Alzheimer's disease, and other dementias; and

''(2) seek early recognition of, and early intervention in the course of, Alzheimer's disease and other dementias.

''(b) CERTAIN ACTIVITIES.—Activities under subsection (a) shall include—

''(1) providing support for the dissemination and implementation of the Roadmap to Maintaining Cognitive Health of the Centers for Disease Control and Prevention to effectively mobilize the public health community into action;

''(2) the development of coordinated public education programs, services, and demonstrations which are designed to increase general awareness of cognitive function and promote a brain healthy lifestyle;

''(3) the development of targeted communication strategies and tools to educate health professionals and service providers about the early recognition, diagnosis, care, and management of Alzheimer's disease and other dementias, and to provide consumers with information about interventions, products, and services that promote cognitive health and assist consumers in maintaining current understanding about cognitive health based on the best science available; and

''(4) providing support for the collection, publication, and analysis of data and the prevalence and incidence of cognitive health, Alzheimer's disease, and other dementias, and the evaluation of existing population-based surveillance systems (such as the Behavioral Risk Factors Surveillance Survey (BRFSS) and the National Health Interview Survey (NHIS)) to identify limitations that exist in the area of cognitive health, and if necessary, the development of a surveillance system for cognitive decline, including Alzheimer's disease and other dementias.

''(c) GRANTS.—The Secretary may award grants under this section—

''(1) to State and local health agencies for the purpose of—

''(A) coordinating activities related to cognitive health, Alzheimer's disease, and other dementias with existing State-based health programs and community-based organizations;

''(B) providing Alzheimer's disease education and training opportunities and programs for health professionals; and

''(C) developing, testing, evaluating, and replicating effective Alzheimer's disease intervention programs to maintain or improve cognitive health; and

''(2) to nonprofit private health organizations with expertise in providing care and services to individuals with Alzheimer's disease for the purpose of—

''(A) disseminating information to the public;

''(B) testing model intervention programs to improve cognitive health; and

''(C) coordinating existing services related to cognitive health, Alzheimer's disease, and other dementias with State-based health programs.

''(d) AUTHORIZATION OF APPROPRIATIONS.—For the purpose of carrying out this section, there are authorized to be appropriated $15,000,000 for fiscal year 2010, and such sums as may be necessary for each of fiscal years 2011 through 2014.''.

TITLE III—ASSISTANCE FOR CAREGIVERS

SEC. 301. ALZHEIMER'S CALL CENTER.

Part P of title III of the Public Health Service Act (42 U.S.C. 280g et seq.), as amended by section 201, is further amended by adding at the end the following:

''SEC. 399V. ALZHEIMER'S CALL CENTER.

''(a) IN GENERAL.—The Secretary, acting through the Administration on Aging, shall award a cooperative grant to a non-profit or community-based organization to support the establishment and operation of an Alzheimer's Call Center that is accessible 24 hours a day, 7 days a week, at the national and local levels, to provide expert advice,

care consultation, information, and referrals regarding Alzheimer's disease.

''(b) ACTIVITIES.—The Alzheimer's Call Center established under subsection (a) shall—

''(1) collaborate with the Administration on Aging in the development, modification, and execution of the Call Center's work plan;

''(2) assist the Administration on Aging in developing and sustaining collaborations between the Call Center, the Eldercare Locator of the Administration of Aging, and the grantees under the Alzheimer's disease demonstration program under subpart II of part K;

''(3) provide a 24 hours a day, 7 days a week toll-free call center with trained professional staff who are available to provide care consultation and crisis intervention to individuals with Alzheimer's disease and other dementias, their family and informal caregivers, and others as appropriate;

''(4) be accessible by telephone through a single toll-free telephone number, website, and e-mail address; and

''(5) evaluate the impact of the Call Center's activities and services.

''(c) MULTILINGUAL CAPACITY.—The Call Center established under this section shall have a multilingual capacity and shall respond to inquiries in at least 140 languages through its own bilingual staff and with the use of a language translation service.

''(d) RESPONSE TO EMERGENCY AND ONGOING NEEDS.—The Call Center established under this section shall collaborate with community-based organizations, including non-profit agencies and organizations, to ensure local, on-the-ground capacity to respond to emergency and on-going needs of individuals with Alzheimer's disease and other dementias, their families, and informal caregivers.

''(e) AUTHORIZATION OF APPROPRIATIONS.—For the purpose of carrying out this section, there are authorized to be appropriated $1,000,000 for fiscal year 2010, and such sums as may be necessary for each of fiscal years 2011 through 2014.''.

SEC. 302. INNOVATIVE ALZHEIMER'S CARE STATE MATCHING GRANT PROGRAM.

(a) AUTHORIZATION OF APPROPRIATIONS.—Section 398B(e) of the Public Health Service Act (42 U.S.C. 280c–5(e)) is amended—

(1) by striking ''and such'' and inserting ''such''; and

(2) by inserting before the period the following: '', $25,000,000 for fiscal year 2010, and such sums as may be necessary for each of fiscal years 2011 through 2014''.

(b) PROGRAM EXPANSION.—Section 398(a) of the Public Health Service Act (42 U.S.C. 280c–3(a)) is amended—

(1) in paragraph (2), by inserting after ''other respite care'' the following: ''and care consultation, including assessment of needs, assistance with planning and problem solving, and providing supportive listening,'';

(2) in paragraph (3), by striking ''; and'' and inserting the following: '', and individuals in frontier areas (in this subsection, defined as areas with 6 or fewer people per square mile or areas in which residents must travel at least 60 minutes or 60 miles to receive health care services);'';

(3) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(4) by adding at the end the following:

''(5) to encourage grantees under this section to coordinate activities with other State officials administering efforts to promote long-term care options that enable older individuals to receive long-term care in home- and community-based settings, in a manner responsive to the needs and preferences of older individuals and their family caregivers;

''(6) to encourage grantees under this section to—

''(A) engage in activities that support early detection and diagnosis of Alzheimer's disease and other dementias;

''(B) provide training about how Alzheimer's disease can affect behavior and impede communication in medical and community settings to—

''(i) medical personnel, including hospital staff, emergency room personnel, home health care workers and physician office staff;

''(ii) rehabilitation services providers; and

''(iii) caregivers of individuals with Alzheimer's disease;

''(C) develop guidelines to provide the medical community with up-to-date information about the best methods of care for individuals with Alzheimer's disease;

''(D) inform community physicians about available resources to assist the physician in detecting and managing Alzheimer's disease; and

''(E) raise awareness among community physicians about the availability of community-based organizations which can assist individuals with Alzheimer's disease and their caregivers;

''(7) to encourage grantees under this section to engage in activities that use findings from evidence-based research on service models and techniques to support individuals with Alzheimer's disease and their caregivers; and

''(8) to encourage grantees under this section to incorporate best practices for effectively serving individuals with Alzheimer's disease in community-based settings into systems initiatives and long-term care activities.''.

By Mr. MCCONNELL:

S. 1493. A bill to designate the current and future Department of Veterans Affairs Medical Center in Louisville, Kentucky, as the ''Robley Rex Department of Veterans Affairs Medical Center''; to the Committee on Veterans' Affairs.

Mr. MCCONNELL. Mr. President, I rise today to introduce legislation to honor a Kentuckian who is a true American hero: Robley Henry Rex.

When Robley passed away in April of this year just a few days shy of his 108th birthday, he was recognized across my State as Kentucky's last World War I-era veteran and hailed as a champion of his fellow service members.

Ninety years ago, Robley bravely put on his country's uniform and left Christian County, KY, where he was born and raised, to patrol the hills of France in the immediate aftermath of what was then called The Great War. After leaving the Army in 1922, he returned to the Commonwealth.

In the years following his Army service, Robley began volunteering at the Louisville Veterans Affairs Medical Center, VAMC. He would go on to devote over 14,000 hours of service, right up until the last years of his long and productive life.

My legislation would name the current VA hospital in Louisville after Robley Rex. It also ensures that when a new VAMC is built, that future facility will also bear his name.

The idea to name this facility after Kentucky's pre-eminent volunteer on behalf of veterans came from a constituent of mine, himself also a veteran. Moreover, the Kentucky Department of Veterans of Foreign Wars had the very same idea and endorsed the proposal during its recent state convention. I'm just pleased that as a Kentucky Senator, I am in a position to make it happen.

I can't think of a more appropriate person to name the facility after than Robley Rex. And I can't think of a more appropriate source for the idea than the Kentucky veterans community.

The new VAMC will be vital to Kentucky's veterans, as well as to Louisville's economy. Once complete, the VA hospital will ensure that the men and women who served our country will receive the quality health care they deserve.

That devotion to ensuring quality care to our veterans is exemplified in the life and service of Robley Rex. How fitting that his fellow veterans—so many of whom knew Robley personally from his countless hours of volunteer service—will see his name above the door.

Finally, I note that this is bipartisan legislation. It enjoys the support of Representatives JOHN YARMUTH and BEN CHANDLER in the other chamber. I ask my colleagues to support this legislation.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1493

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. DESIGNATION OF ROBLEY REX DEPARTMENT OF VETERANS AFFAIRS MEDICAL CENTER.

(a) DESIGNATION.—The Department of Veterans Affairs Medical Center in Louisville, Kentucky, and any successor to such medical center, shall after the date of the enactment of this Act be known and designated as the ''Robley Rex Department of Veterans Affairs Medical Center''.

(b) REFERENCES.—Any reference in any law, regulation, map, document, record, or other paper of the United States to the medical center referred to in subsection (a) shall be considered to be a reference to the Robley Rex Department of Veterans Affairs Medical Center.

By Ms. CANTWELL (for herself and Mrs. MURRAY):

S. 1497. A bill to amend the Internal Revenue Code of 1986 to allow tax-exempt bond financing for fixed-wing emergency medical aircraft; to the Committee on Finance.

Ms. CANTWELL. Mr. President, I rise to introduce legislation that will remove an unintended obstacle in the tax-exempt bond rules so that states can use these bonds to finance the purchase of fixed-wing air ambulances in the same way they can now use them to finance the purchase of medical helicopters.

The difference between a medical helicopter and a fixed wing air ambulance

may seem minor to some, but if you live in a remote area the difference can be as big as life or death.

Air medical services, AMS, are an essential component of the health care system. When appropriately used, air critical care transport saves lives and reduces the cost of health care by minimizing the time the critically injured and ill spend out of a hospital, by bringing more medical capabilities to the patient than are normally provided by ground emergency medical services, and by quickly getting the patient to the right specialty care. Dedicated medical helicopters and fixed wing aircraft are mobile flying emergency intensive care units deployed at a moment's notice to patients whose lives depend on rapid care and transport.

In remote rural areas, the use of helicopters often is impractical and unsafe because of the long distances that patients must be transported, sometimes during poor weather conditions. In these situations, the better alternative is a fixed-wing aircraft.

Both helicopters and fixed wing aircraft cost millions of dollars to purchase or lease, operate, house and maintain. But under the way that the tax-exempt bond rules currently work, states are prohibited from using these bonds to finance air ambulance services in rural areas, even though they can use these bonds for helicopters. This result was not what Congress intended, and our bill would make that clear.

Under current law, tax-exempt bonds can not be issued for the purchase of any ''airplane, skybox or other privacy luxury box, health club facility, facility primarily used for gambling, or store the principal business of which is the sale of alcoholic beverages for consumption off premises.'' The restrictions were enacted in order to prevent tax-exmpt bonds to be used for frivolous or extravagant purposes. Unfortunately, the law has been interpreted to exclude the purchase of new fixed-wing planes to provide air ambulance services, but the purchase of helicopters—which are not airplanes—is permitted.

This result is not what was intended by the restrictions and our bill would simply make it clear that the general restriction against the use of tax-exempt bonds for purchasing an airplane does not apply in the case of planes that are equipped for and exclusively dedicated to emergency medical services.

There is supporting precedent in distinguishing planes for air ambulance services different than other airplanes. The air transportation excise tax provides an exemption for air transportation that is used to provide ''emergency medical services . . . by a fixed-wing aircraft equipped for and exclusively dedicated on that flight to acute care emergency medical services.''

This issue hits close to home for me and my colleagues who are joining me on this legislation, but we are certainly not alone with respect to the need to ensure that folks in our rural and remote areas have access to needed medical services.

Inland Northwest Health Services, INHS, is a non-profit organization that provides critical health care support services in the Inland Northwest, including air ambulance services through Northwest MedStar. INHS is based in Spokane, Washington, and provides health care services in Eastern Washington, Eastern Oregon, Northern Idaho, and Western Montana. Unfortunately, this unintended restriction in the tax code is preventing INHS from asking the appropriate state authorities to issue tax-exempt bonds to finance the purchase of new fixed-wing planes for air ambulance service.

The legislation that I am introducing with Senator MURRAY is a commonsense fix to this problem, and I hope we can address it quickly.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1497

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TAX-EXEMPT BOND FINANCING FOR FIXED-WING EMERGENCY MEDICAL AIRCRAFT.

(a) IN GENERAL.—Subsection (e) of section 147 of the Internal Revenue Code of 1986 (relating to no portion of bonds may be issued for skyboxes, airplanes, gambling establishments, etc.) is amended by adding at the end the following new sentence: ''The preceding sentence shall not apply to any fixed-wing aircraft equipped for, and exclusively dedicated to providing, acute care emergency medical services (within the meaning of 4261(g)(2)).''

(b) EFFECTIVE DATE.—The amendment made by this section shall apply to obligations issued after the date of the enactment of this Act.

By Mr. CASEY (for himself and Mr. ENZI):

S. 1502. A bill to establish a program to be managed by the Department of Energy to ensure prompt and orderly compensation for potential damages relating to the storage of carbon dioxide in geological storage units; to the Committee on Energy and Natural Resources.

Mr. CASEY. Mr. President, I rise today on behalf of myself and my colleague Senator ENZI of Wyoming to introduce the Carbon Storage Stewardship Trust Fund Act of 2009. This bill will encourage the commercial deployment of technology that will allow for the continued use of our Nation's vast coal resources to produce economical and reliable power while at the same time mitigating the impact of climate change.

The capture and storage of carbon dioxide from power generation facilities and large industrial sources is a critical component of both U.S. and international policy to reduce global emissions of greenhouse gases. The criticality of this technology has been driven home by the Pew Center on Global Climate Change which has pointed out that ''carbon capture and storage, CCS, is the key enabling technology for a future in which we can continue to use our vast coal resources and protect the climate.'' And former British Prime Minister Tony Blair stated in November, 2008, that ''the vast majority of new power stations in China and India will be coal fired; not ''may be coal fired''- will be. So developing carbon capture and storage technology is not optional, it is literally the essence.''

The commercial deployment of CCS will require further large-scale development and demonstration of the technology. Just as important, however, it will also require a well thought out approach to address the risk and liability of injecting large volumes of CO_2 into geological formations, such as saline aquifers, depleted oil and gas fields, and unminable coal seams, where it will be permanently stored.

The risk of geological CO_2 storage, also commonly known as carbon sequestration, is considered small. In fact, CO_2 has been safely injected into oil and gas fields to enhance the recovery of these hydrocarbons for decades without incident. While the potential for CO_2 to leak to the surface and cause human or ecological harm in a well designed and operated carbon sequestration project is minimal, the financial liability associated with this risk is uncertain given the huge disparity between the typical lifetime of a firm operating a storage facility and the need to ensure the safe storage of CO_2 in perpetuity. This uncertainty can cause a chilling effect on private sector investment in CCS.

The purpose of this act is to create a program for managing the financial risk, or liability, of the long-term storage of CO_2 . This program will offer the private sector with a framework for how legal and financial responsibilities for commercial carbon storage operations will be addressed. Moreover, it will provide a strong incentive to industry to manage and reduce risk by deploying carbon sequestration in the safest possible manner.

Specifically, the act will require the owner or operator of a commercial CO_2 storage facility to self insure or obtain private insurance or other types of financial assurance to cover liability claims during the CO_2 injection phase of the project and for an extended period of time after injection has stopped. After the operator has received a site closure certificate from the appropriate regulatory agency, the act would then convey stewardship for the long-term management of the site to the U.S. Department of Energy. The State where the storage facility is located may request to take on stewardship for the site from the Department of Energy. The act will also create a trust fund from fees paid by storage facility operators on a per ton of CO_2 injected basis that will be used to pay for

claims for damages made after storage facility stewardship is transferred to the Federal government.

In summary, this act will give the private sector the certainty they need regarding the longterm stewardship of CO_2 storage facilities. Just as important, it will strongly encourage the safe and responsible operation of these facilities while ensuring the prompt and orderly compensation for damages or harm to humans, to the environment, and to natural resources, should they occur, from the injection and storage of CO_2 in geological formations.

I urge all of my colleagues to join Senator ENZI and me in support of this act so that a clear signal is given about our commitment to the development, demonstration, and ultimately, the widespread commercial deployment of CCS technology as a key component of the Nation's strategy to reduce emissions of CO_2.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1502

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Carbon Storage Stewardship Trust Fund Act of 2009''.

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to promote the commercial deployment of carbon capture and storage as an essential component of a national climate mitigation strategy;

(2) to require private liability assurance during the active project period of a carbon dioxide storage facility;

(3) to establish a Federal trust fund consisting of amounts received as fees from operators of carbon dioxide storage facilities;

(4) to establish a limit on liability for damages caused by injection of carbon dioxide by carbon dioxide storage facilities subject to certificates of closure;

(5) to establish a program—

(A) to certify the closure of commercial carbon dioxide storage facilities; and

(B) to provide for the transfer of long-term stewardship to the Federal Government for carbon dioxide storage facilities on the issuance of certificates of closure for the facilities;

(6) to provide for the prompt and orderly compensation for damages relating to the storage of carbon dioxide; and

(7) to protect the environment and public by providing long-term stewardship of geological storage units.

SEC. 3. DEFINITIONS.

In this Act:

(1) ACTIVE PROJECT PERIOD.—The term ''active project period'' means the phases of the carbon dioxide storage facility through receipt of a certificate of closure, including—

(A) the siting and construction of the facility;

(B) carbon dioxide injection;

(C) well capping;

(D) facility decommissioning; and

(E) geological storage unit monitoring, measurement, verification, and remediation.

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Environmental Protection Agency.

(3) CARBON DIOXIDE STORAGE FACILITY.—The term ''carbon dioxide storage facility'' means a facility that receives and permanently stores or sequesters carbon dioxide within a geological storage unit, including carbon dioxide permanently stored as a result of enhanced hydrocarbon recovery.

(4) CERTIFICATE OF CLOSURE.—The term ''certificate of closure'' means a determination issued by the Administrator or other Federal or State regulatory authority with respect to a carbon dioxide storage facility that certifies that the operator of the carbon dioxide storage facility has completed injection operations, well closure, and any required monitoring and remediation to ensure that any carbon dioxide injected into a geological storage unit would not harm or present a risk to human health, safety, and the environment, including drinking water supplies.

(5) CIVIL CLAIM.—The term ''civil claim'' means a claim, cause of action, lawsuit, judgment, court order, administrative order, government or agency order, fine, penalty, or notice of violation, for civil relief with respect to damages or harm to persons, property, or natural resources from the injection of carbon dioxide by a carbon dioxide storage facility.

(6) DAMAGE.—

(A) IN GENERAL.—The term ''damage'' means any direct or indirect damage or harm to persons, property, or natural resources from the injection of carbon dioxide into geological storage units.

(B) INCLUSIONS.—The term ''damage'' includes personal injury, sickness, real or personal property damage, natural resource damage, trespass, subsidence losses, revenue losses, and loss of profits.

(7) ENHANCED HYDROCARBON RECOVERY.—The term ''enhanced hydrocarbon recovery'' means the use of carbon dioxide to improve or enhance the recovery of oil or natural gas from oil or natural gas fields.

(8) FUND.—The term ''Fund'' means the Carbon Storage Trust Fund established by section 5(d)(1).

(9) GEOLOGICAL STORAGE UNIT.—The term ''geological storage unit'' includes saline formations, hydrocarbon formations, basalt formations, salt caverns, unmineable coal seams, or any other geological formation capable of permanently storing carbon dioxide.

(10) LIABILITY ASSURANCE.—The term ''liability assurance'' means privately funded financial mechanisms, including third-party insurance, self-insurance, performance bonds, trust funds, letters of credit, and surety bonds.

(11) LONG-TERM STEWARDSHIP.—The term ''long-term stewardship'' means the monitoring, measurement, verification, and remediation and related activities associated with a carbon dioxide storage facility after issuance of a certificate of closure.

(12) PROGRAM.—The term ''Program'' means the Carbon Storage Stewardship and Trust Fund Program established by section 5(a).

(13) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

SEC. 4. LONG-TERM STEWARDSHIP RESPONSIBILITY.

(a) IN GENERAL.—Subject to subsection (b), the Secretary shall be responsible for the long-term stewardship of a carbon dioxide storage facility on the issuance of a certificate of closure for the carbon dioxide storage facility.

(b) TRANSFER TO STATE.—

(1) IN GENERAL.—A State may request that the management responsibilities associated with long-term stewardship of a carbon dioxide storage facility located in the State be transferred to the State in accordance with regulations established by the Secretary.

(2) APPROVAL OF REQUEST.—If the Secretary approves a request under paragraph (1), the State shall be responsible for the long-term stewardship of the applicable carbon dioxide storage facility beginning on the date of the approval in accordance with applicable Federal and State laws (including regulations).

(3) FAILURE TO ACT BY STATE.—In accordance with any regulations established under paragraph (1), if the Secretary determines that a State that has accepted management responsibilities under paragraph (1) has failed to carry out the responsibilities of the State with respect to the carbon dioxide storage facility, the Secretary shall assume long-term stewardship of the carbon dioxide storage facility as soon as practicable after the date of the determination.

(c) STANDARDS.—The Secretary, in coordination with the Administrator, shall establish standards for any monitoring, measurement, verification, and site remediation activities necessary to protect health, safety, and the environment during long-term stewardship performed by a State or the Federal Government.

(d) COORDINATION WITH ADMINISTRATOR.—If long-term stewardship is vested with the Secretary, the Secretary may coordinate responsibility for site monitoring, measurement, verification, and remediation and related activities with the Administrator.

SEC. 5. CARBON STORAGE STEWARDSHIP AND TRUST FUND PROGRAM.

(a) IN GENERAL.—There is established in the Department of Energy the Carbon Storage Stewardship and Trust Fund Program.

(b) LIABILITY ASSURANCE REQUIRED FOR OPERATORS OF COMMERCIAL CARBON DIOXIDE STORAGE FACILITIES.—Notwithstanding any other provision of Federal or State law, in carrying out the Program, the Secretary shall require operators of carbon dioxide storage facilities to maintain adequate liability assurance during the active project period.

(c) FEES.—

(1) IN GENERAL.—In carrying out the Program, the Secretary shall require operators of carbon dioxide storage facilities to pay a risk-based fee, in an amount to be established in accordance with paragraph (2), for each ton of carbon dioxide injected by the carbon dioxide storage facility into geological storage units during the operation phase of the facility.

(2) AMOUNT.—

(A) IN GENERAL.—As soon as practicable after the date of enactment of this Act and after taking into account the criteria described in subparagraph (B), the Secretary shall establish—

(i) the minimum and maximum balance for the Fund; and

(ii) the amount of the fee required under paragraph (1).

(B) CRITERIA.—The criteria referred to in subparagraph (A) are—

(i) the estimated quantity of carbon dioxide to be injected annually into geological storage units by all operating commercial carbon dioxide storage facilities;

(ii) the likelihood or risk of an incident resulting in liability;

(iii) the likely dollar value of any damages relating to an incident;

(iv) other factors relating to the risk of the carbon dioxide storage facility and associated geological storage unit; and

(v) impact on commercial and economic viability of carbon dioxide storage facilities.

(C) CONSIDERATIONS.—In establishing the amount of the fee under subparagraph (A)(ii), the Secretary may consider using a fee system that is based on the level of risk associated with a specific geological storage unit to provide an incentive for the selection and

operation of the best carbon dioxide storage facilities.

(D) ENHANCED HYDROCARBON RECOVERY.—The Secretary shall determine the most appropriate approach for charging a fee on the quantity of carbon dioxide injected into oil and gas fields, after taking into consideration—

(i) the quantity of carbon dioxide that is permanently stored;

(ii) whether or not the enhanced hydrocarbon recovery operation is also being operated as a carbon dioxide storage facility; and

(iii) any other factors that the Secretary determines to be appropriate.

(E) REVIEW AND ADJUSTMENT.—The Secretary shall, on at least an annual basis, review the Fund balance—

(i) to ensure that there are sufficient amounts in the Fund to make the payments required under subsection (d)(3)(A); and

(ii) to determine whether or not to increase or decrease the amount, or discontinue collection, of the fee, after taking into consideration—

(I) the annual quantity of carbon dioxide injected by carbon dioxide storage facilities;

(II) the number and estimated value of claims against the Fund; and

(III) any other relevant factors, as determined by the Secretary.

(3) DEPOSIT.—Notwithstanding section 3302 of section 31, United States Code, the fees collected under paragraph (1) shall be deposited in the Fund.

(d) CARBON STORAGE TRUST FUND.—

(1) ESTABLISHMENT.—There is established in the Treasury of the United States a revolving fund, to be known as the ''Carbon Storage Trust Fund'', consisting of such amounts as are deposited under subsection (c)(3).

(2) USE OF FUND.—

(A) IN GENERAL.—Amounts in the Fund shall be made available, without further appropriation or fiscal year limitation—

(i) to the Secretary for the payment of civil claims from a carbon dioxide storage facility that are brought after a certificate of closure for the carbon dioxide storage facility has been issued;

(ii) to the Secretary for long-term stewardship after the date of issuance of a certificate for closure; and

(iii) to the Secretary or other appropriate regulatory authority to pay any reasonable and verified administrative costs incurred by the Secretary or regulatory authority in carrying out the Program.

(B) LIMITATION.—Amounts in the Fund shall only be used for the purposes described in clause (i), (ii), or (iii) of subparagraph (A).

(C) LIMITATION ON PAYMENTS.—

(i) IN GENERAL.—Subject to clause (ii), an aggregate claim for damages brought under subparagraph (A)(i) shall be limited to an amount to be established by the Secretary as soon as practicable after the date of enactment of this Act, based on mechanisms such as—

(I) actuarial modeling of probable damage; and

(II) net present value analysis.

(ii) CONGRESSIONAL ACTION.—If estimated or actual aggregate damages exceed the amount established under clause (i)—

(I) the Secretary shall notify Congress; and

(II) on receipt of notice under subclause (I), Congress may provide for payments in excess of that amount, in accordance with guidelines established by Congress by law.

(D) EXCEPTION FOR GROSS NEGLIGENCE AND INTENTIONAL MISCONDUCT.—Notwithstanding subparagraph (A), no amounts in the Fund shall be used to pay a claim for liability arising out of conduct of an operator of a carbon dioxide storage facility that is grossly negligent or that constitutes intentional misconduct, as determined by the Secretary.

(E) PROCEDURES FOR ADJUDICATION OF CLAIMS.—Claims of damage brought under subparagraph (A)(i) relating to carbon dioxide in a carbon dioxide storage facility subject to a certificate of closure shall be—

(i) filed in the United States Court of Federal Claims; and

(ii) adjudicated in accordance with procedures established by the United States Court of Federal Claims.

(3) INITIAL FUNDING.—

(A) IN GENERAL.—If sufficient amounts are not available in the Fund to cover potential claims during the first years of the Program, the Secretary may request from the Secretary of the Treasury an interest-bearing advance in funding from the Treasury to carry out the Program, subject to subparagraph (B).

(B) TERMS AND CONDITIONS.—The terms and conditions for the repayment of an advance under subparagraph (A) shall be specified by the Secretary of the Treasury.

SEC. 6. LIMITATION ON CIVIL CLAIMS.

(a) IN GENERAL.—Except as provided in subsection (b), on issuance of a certificate of closure, a civil claim or claim for the performance of long-term stewardship responsibilities under applicable Federal and State law, may not be brought against—

(1) the operator or owner of the carbon dioxide storage facility subject to the certificate of closure;

(2) the generator of the carbon dioxide stored in the applicable geological storage unit; or

(3) the owner or operator of the pipeline used to transport the carbon dioxide to the carbon dioxide storage facility subject to the certificate of closure.

(b) EXCEPTION.—Subsection (a) shall not apply in the case of a civil claim involving the gross negligence or intentional misconduct of an owner, operator, or generator.

Mr. ENZI. Mr. President, we need clean energy. We need cheap energy. We need abundant energy from right here at home. Why not concentrate some of our efforts on hitting a triple play?

Coal is our Nation's most abundant energy source. It provides more than 50 percent of our Nation's electricity today and makes electricity more affordable for millions of Americans. It provides for thousands of well paying American jobs and is an essential part of my home State's economy.

Unfortunately, in the discussions surrounding climate change, some have suggested that we should end our Nation's use of coal. Because of the abundant, cost-effective nature of this resource, that doesn't make sense. Instead of talking about eliminating one of our country's most important energy sources, we should be talking about how we can make coal cleaner.

An essential element of the effort to make coal cleaner will be the development of carbon capture and storage, CCS, technology. There are many pieces to that effort, and today, Senator CASEY and I have introduced The Carbon Storage Stewardship Trust Fund Act of 2009 to address one issue with CCS liability for the stored CO_2.

Our legislation sets up a framework that answers the question of who is responsible for the CO_2 once it is placed underground. The Carbon Storage Stewardship Trust Fund Act of 2009 requires companies injecting CO_2 into the ground to obtain private liability insurance for a period of time. After the CO_2 is injected and the injection site is certified as closed by the Federal Government, liability for the CO_2 is transferred to the Federal Government.

To cover any claims that may arise from damages caused by the injected CO_2, the bill sets up a Federal trust fund that is paid for through a small fee charged for each ton of CO_2 that is injected. Additionally, it provides a method for compensation for those damages.

While this legislation is far from everything we need to make commercial CCS a reality, it is an important step and answers an important question about long-term liability of CO_2. I appreciate Senator CASEY's leadership on this issue and look forward to working with him and other Members of the Senate to move this legislation forward.

Mr. SPECTER:

S. 1504. A bill to provide that Federal courts shall not dismiss complaints under rule 12(b)(6) or (e) of the Federal Rules of Civil Procedure, except under the standards set forth by the Supreme Court of the United States in *Conley* v. *Gibson*, 355 U.S. 41 (1957); to the Committee on the Judiciary.

Mr. SPECTER. Mr. President, I seek recognition to speak on legislation I am introducing that will restore the system of notice pleading that has served our Federal judicial system well since 1938, the year the Federal Rules of Civil Procedure were adopted.

Civil litigation in our Federal system is commenced by the filing a complaint that puts the defendant on notice of the plaintiffs claims. Rule 8(a)(2) of the Federal Rules of Civil Procedure provides that a complaint need only contain a ''short and plain statement of the claim showing the pleader'', usually the plaintiff, ''is entitled to relief.'' This is not a demanding standard. An appendix to the Rules includes a form complaint for negligence that the drafters of Rule 8 obviously thought would satisfy Rule 8's standard. That complaint, in relevant part, alleges only that ''[o]n June 1, 1936, in a public highway called Boylston Street in Boston Massachusetts, defendant negligently drove a motor vehicle against plaintiff who was crossing the highway.''

The Federal Rules require the court to await the submission of the plaintiff's evidence—first at the summary-judgment stage and, if summary judgment is not granted, then at trial—before evaluating or passing on the truth of the complaint's allegations. It's only sensible that courts do so: Not until a plaintiff has had access to relevant information in the defendant's possession during the discovery process that follows the filing of a complaint as a matter of right can the plaintiff normally offer evidence to support the complaint's allegations.

For over 70 years following the adoption of the Federal Rules, the Supreme Court of the U.S. consistently and faithfully implemented Rule 8's notice-pleading language. Its leading decision on the subject, *Conley* v. *Gibson*, 355 U.S. 41, 1957, prohibited federal courts from dismissing a complaint ''for failure to state a claim unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim that would entitle him to relief.''

Two years ago in *Bell Atlantic Corporation* v. *Twombly*, 550 U.S. 544, 2007, the Court jettisoned the standard set forth in Conley and announced that henceforth it would require not only factual specificity in complaints not previously required of plaintiffs, but also that a complaint's allegation of wrongdoing appear ''plausible'' to the court. This year in *Ashcroft* v. *Iqbal*, 129 S. Ct. 1937, 2009, the Supreme Court significantly expanded upon Twombly by, to quote Professor Stephen Burbank of the University of Pennsylvania Law School, effectively authorizing federal judges to indulge their ''subject judgments'' in evaluating an allegation's plausibility. According to an article that just appeared in The York Times, Justice Ruth Bader Ginsburg recently told a group of Federal judges that, as a result of these two cases, the Supreme Court has ''messed up the federal rules'' governing pleading.

When it passed the Rules Enabling Act, Congress established a carefully designed process for amending the Federal Rules of Civil Procedure. The process ends with the Supreme Court's presentation of a proposed rule change to Congress for approval. In Twombly and Ashcroft the Court effectively end ran that process.

The effect of the Court's actions will no doubt be to deny many plaintiffs with meritorious claims access to the Federal courts and, with it, any legal redress for their injuries. I think that is an especially unwelcome development at a time when, with the litigating resources of our executive-branch and administrative agencies stretched thin, the enforcement of Federal antitrust, consumer protection, civil rights and other laws that benefit the public will fall increasingly to private litigants.

The Notice Pleading Restoration Act will require the Federal courts to test the sufficiency of a complaint's allegations under the well-established standards that prevailed in the Federal courts until Twombly. I urge its passage.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 220—SUPPORTING THE DESIGNATION OF SEPTEMBER AND ''NATIONAL ATRIAL FIBRILLATION AWARENESS MONTH'' AND ENCOURAGING EFFORTS TO EDUCATE THE PUBLIC ABOUT ATRIAL FIBRILLATION

Mr. FEINGOLD (for himself, Ms. COLLINS, Mr. DORGAN, and Mr. CRAPO) submitted the following resolution; which was referred to the Committee on Health, Education, Labor, and Pensions:

S. RES. 220

Whereas atrial fibrillation is a cardiac condition in which electrical pulses disrupt the regular beating of the atria in the heart, hampering the ability of the atria to fill the ventricles with blood, and subsequently causing blood to pool in the atria and form clots;

Whereas atrial fibrillation is the most common cardiac malfunction and affects at least 2,200,000 people in the United States, with increased prevalence anticipated as the population of the United States ages;

Whereas atrial fibrillation is associated with an increased, long-term risk of stroke, heart failure, and mortality from all causes, especially among women;

Whereas atrial fibrillation accounts for approximately ⅓ of hospitalizations for cardiac rhythm disturbances;

Whereas, according to the American Heart Association, 3 to 5 percent of people in the United States aged 65 and older are estimated to have atrial fibrillation;

Whereas atrial fibrillation is recognized as a major contributor to strokes, with an estimated 15 to 20 percent of strokes occurring in people afflicted with atrial fibrillation;

Whereas it is estimated that treating atrial fibrillation costs approximately $3,600 per patient annually for a total cost burden in the United States of approximately $15,700,000,000;

Whereas obesity is a significant risk factor for atrial fibrillation;

Whereas better education for patients and health care providers is needed in order to ensure timely recognition of atrial fibrillation symptoms;

Whereas more research into effective treatments for atrial fibrillation is needed; and

Whereas September is an appropriate month to observe as National Atrial Fibrillation Awareness Month: Now, therefore, be it

Resolved, That the Senate—

(1) supports the designation of September as ''National Atrial Fibrillation Awareness Month'';

(2) supports efforts to educate people about atrial fibrillation;

(3) recognizes the need for additional research into treatment for atrial fibrillation; and

(4) encourages the people of the United States and interested groups to observe and support National Atrial Fibrillation Awareness Month through appropriate programs and activities that promote public awareness of atrial fibrillation and potential treatments for atrial fibrillation.

SENATE RESOLUTION 221—EXPRESSING SUPPORT FOR THE GOALS AND IDEALS OF THE FIRST ANNUAL NATIONAL WILD HORSE AND BURRO ADOPTION DAY TAKING PLACE ON SEPTEMBER 26, 2009

Mr. REID (for himself, Mrs. FEINSTEIN, and Mr. ENSIGN) submitted the following resolution; which was referred to the Committee on Energy and Natural Resources:

S. RES. 221

Whereas, in 1971, in Public Law 92–195 (commonly known as the ''Wild Free-Roaming Horses and Burros Act'') (16 U.S.C. 1331 et seq.), Congress declared that wild free-roaming horses and burros are living symbols of the historic and pioneer spirit of the West;

Whereas, under that Act, the Secretary of the Interior and the Secretary of Agriculture have responsibility for the humane capture, removal, and adoption of wild horses and burros;

Whereas the Bureau of Land Management and the Forest Service are the Federal agencies responsible for carrying out the provisions of the Act;

Whereas a number of private organizations will assist with the adoption of excess wild horses and burros, in conjunction with the first National Wild Horse and Burro Adoption Day; and

Whereas there are approximately 31,000 wild horses in short-term and long-term holding facilities, with 18,000 young horses awaiting adoption: Now, therefore, be it

Resolved, That the Senate—

(1) supports the goals of a National Wild Horse and Burro Adoption Day to be held annually in coordination with the Secretary of Interior and the Secretary of Agriculture;

(2) recognizes that creating a successful adoption model for wild horses and burros is consistent with Public Law 92-195 (commonly known as the ''Wild Free-Roaming Horses and Burros Act'') (16 U.S.C. 1331 et seq.) and beneficial to the long-term interests of the people of the United States in protecting wild horses and burros; and

(3) encourages citizens of the United States to adopt a wild horse or burro so as to own a living symbol of the historic and pioneer spirit of the West.

SENATE CONCURRENT RESOLUTION 34—EXPRESSING THE SENSE OF CONGRESS THAT A COMMEMORATIVE POSTAGE STAMP SHOULD BE ISSUED TO HONOR THE CREW OF THE USS MASON DE–529 WHO FOUGHT AND SERVED DURING WORLD WAR II

Mr. BURRIS submitted the following concurrent resolution; which was referred to the Committee on Homeland Security and Governmental Affairs:

S. CON. RES. 34

Whereas the USS Mason DE–529 was the only United States Navy destroyer with a predominantly black enlisted crew during World War II;

Whereas the integration of the crew of the USS Mason DE–529 was the role model for racial integration on Navy vessels and served as a beacon for desegregation in the Navy;

Whereas the integration of the crew signified the first time that black citizens of the United States were trained to serve in ranks other than cooks and stewards;

Whereas the USS Mason DE–529 served as a convoy escort in the Atlantic and Mediterranean Theatres during World War II;