112TH CONGRESS
2D SESSION

# S. _____

To require certain entities that collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

---

Mr. TOOMEY introduced the following bill; which was read twice and referred to the Committee on _____

---

# A BILL

To require certain entities that collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.

*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 ''Data Security and Breach Notification Act of 2012''.

**SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.**

Each covered entity shall take reasonable measures to protect and secure data in electronic form containing personal information.

**SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.**

(a) NOTIFICATION.—

(1) IN GENERAL.—A covered entity that owns or licenses data in electronic form containing personal information shall give notice of any breach of the security of the system following discovery by the covered entity of the breach of the security of the system to each individual who is a citizen or resident of the United States whose personal information was or that the covered entity reasonably believes to have been accessed and acquired by an unauthorized person and that the covered entity reasonably believes has caused or will cause, identity theft or other financial harm.

(2) LAW ENFORCEMENT.—A covered entity shall notify the Secret Service or the Federal Bureau of Investigation of the fact that a breach of security has occurred if the number of individuals whose personal information the covered entity reasonably believes to have been accessed and acquired by an unauthorized person exceeds 10,000.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY AGENTS.—

(A) IN GENERAL.—In the event of a breach of security of a system maintained by a third-party entity that has been contracted to maintain, store, or process data in electronic form containing personal information on behalf of a covered entity who owns or possesses such data, such third-party entity shall notify such covered entity of the breach of security.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM THIRD PARTIES.—Upon receiving notification from a third party under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(C) EXCEPTION FOR SERVICE PROVIDERS.—A service provider shall not be considered a third-party agent for purposes of this paragraph.

(2) SERVICE PROVIDERS.—

(A) IN GENERAL.—If a service provider becomes aware of a breach of security involving data in electronic form containing personal information that is owned or possessed by a covered entity that connects to or uses a system or

network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM SERVICE PROVIDERS.—Upon receiving notification from a service provider under subparagraph (A), a covered entity shall provide notification as required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) with respect to a security breach shall be made as expeditiously as practicable and without unreasonable delay, consistent with any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the data system that was breached.

(2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) LAW ENFORCEMENT.—If a Federal law enforcement agency determines that the notification required under subsection (a) would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if further delay is necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be delayed upon the written request of the national security agency or homeland security agency for any period which the national security agency or homeland security agency determines is reasonably necessary. A Federal national security agency or homeland security agency may revoke such delay or extend the period set forth in the

original request made under this subparagraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall be in compliance with such requirement if the covered entity provides such notice by one of the following methods:

(i) Written notification, sent to the postal address of the individual in the records of the covered entity.

(ii) Telephone.

(iii) Email or other electronic means.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a security breach, such notification, to the extent practicable, shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the personal information that was accessed and acquired, or

reasonably believed to have been accessed and acquired, by an unauthorized person as a part of the security breach; and

(iii) information that the individual can use to contact the covered entity to inquire about—

(I) the breach of security; or

(II) the information the covered entity maintained about that individual.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) may provide substitute notification in lieu of the direct notification required by paragraph (1) if such direct notification is not feasible due to—

(i) excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity; or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include at least one of the following:

(i) A conspicuous notice on the Internet website of the covered entity (if such covered entity maintains such a website).

(ii) Notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(e) TREATMENT OF PERSONS GOVERNED BY OTHER FEDERAL LAW.—Except as provided in section 4(b), a covered entity who is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a breach of security shall be deemed to be in compliance with this section.

**SEC. 4. APPLICATION AND ENFORCEMENT.**

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

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—Sections 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 222, 338, and 551), and any regulations promulgated thereunder, shall not apply with respect to the information security practices, including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections.

(c) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (a), the Commission shall enforce

this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates section 3 or 4 shall be subject to the penalties and entitled to the privileges and immunities provided in such Act.

(3) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection for all actions shall not exceed—

(A) $500,000 for all violations of section 2 resulting from the same related act or omission; and

(B) $500,000 for all violations of section 3 resulting from a single breach of security.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this Act shall be construed to establish a private cause of action against a person for a violation of this Act.

**SEC. 5. DEFINITIONS.**

In this Act:

(1) BREACH OF SECURITY.—The term ''breach of security'' means unauthorized access and acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or utilizes personal information.

(B) EXEMPTIONS.—The term ''covered entity'' does not include the following:

(i) Financial institutions subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(ii) An entity covered by the regulations issued under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191) to the extent that such entity is subject to

the requirements of such regulations with respect to protected health information.

(4) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(5) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''personal information'' means an individual's first name or first initial and last name in combination with any 1 or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) EXCLUSIONS.—

(i) PUBLIC RECORD INFORMATION.—Personal information does not include information obtained about an individual which has been lawfully made publicly available by a Federal, State, or local government entity or widely distributed by media.

(ii) ENCRYPTED, REDACTED, OR SECURED DATA.—Personal information does not include information that is encrypted, redacted, or secured by any other method or technology that renders the data elements unusable.

(6) SERVICE PROVIDER.—The term ''service provider'' means an entity that provides electronic data transmission, routing, intermediate, and transient storage, or connections to its system or network, where such entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such entity transmits, routes, stores, or for which such entity provides connections. Any such entity shall be treated as a service provider under this Act only to the

extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

**SEC. 6. EFFECT ON OTHER LAWS.**

This Act preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security.

**SEC. 7. EFFECTIVE DATE.**

This Act shall take effect on the date that is 1 year after the date of enactment of this Act.