114TH CONGRESS
1ST SESSION

S. 1027

To require notification of information security breaches and to enhance penalties for cyber criminals, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 21, 2015

Mr. KIRK (for himself and Mrs. GILLIBRAND) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To require notification of information security breaches and to enhance penalties for cyber criminals, 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 Breach Notification and Punishing Cyber Criminals Act of 2015''.

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—

(A) whose personal information was, or that the covered entity reasonably believes to have been, accessed and acquired by an unauthorized person; or

(B) who the covered entity reasonably believes may be at risk of identity theft, fraud, actual financial harm, or other unlawful conduct.

(2) LAW ENFORCEMENT.—

(A) DESIGNATION OF A GOVERNMENT ENTITY TO RECEIVE NOTICE.—

(i) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Attorney General, shall designate a Federal Government entity to receive the information required to be

submitted under this section, and any other reports and information about information security incidents, threats, and vulnerabilities.

(ii) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall—

(I) be responsible for promptly providing the information it receives to the United States Secret Service and the Federal Bureau of Investigation, and to the Federal Trade Commission for civil law enforcement purposes; and

(II) provide the information described in subclause (I) as appropriate to other Federal agencies for law enforcement, national security, or data security purposes.

(B) NOTICE.—Not later than 30 days after the date on which a security breach is discovered, a covered entity shall notify the designated entity of the fact that the breach of security has occurred if—

(i) the number of individuals whose personal information was, or is reasonably believed to be to have been accessed and acquired by an unauthorized person is more than 1,000;

(ii) the security breach involves a database, networked or integrated databases, or other data system containing the personal information of more than 250,000 individuals;

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

(iv) the security breach involves personal information of primarily individuals known to the covered entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(C) FTC REVIEW OF THRESHOLDS.—

(i) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Federal Trade Commission, in consultation with the Attorney General and the Secretary of Homeland Security, shall promul-

gate regulations regarding the reports required under subparagraph (A).

(ii) RULEMAKING.—The Federal Trade Commission, in consultation with the Attorney General and the Secretary of Homeland Security, after notice and the opportunity for public comment, and in a manner consistent with this section, shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subparagraph (A) and to facilitate the purposes of this section.

(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, the third-party entity shall notify the 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.—For purposes of this paragraph, a service provider shall not be considered a third-party agent.

(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, the service provider shall notify the covered entity who initiated such connection, transmission, routing, or storage if the 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) NOTIFICATION TO AFFECTED INDIVIDUALS.—

(A) IN GENERAL.—Unless subject to a delay authorized under subparagraph (B) or paragraph (2), a notification required under subsection (a)(1) with respect to a security breach shall be made not later than 30 days after the date on which the security breach was discovered, 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.

(B) FOLLOW-UP NOTIFICATION.—Not later than 60 days after the date on which notice is provided under subsection (a)(1), if a covered entity has discovered additional information relating to how a breach of security occurred (as required under subsection (d)(1)(B)(iii) to be included in a notification) the covered entity may provide a follow-up notification to affected individuals that contains the additional information.

(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 rea-

sonably 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 any 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;

(iii) a general description of how the breach of security occurred; and

(iv) 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.—Substitute notification described in subparagraph (A) shall include—

(i) a conspicuous notice on the Internet Web site of the covered entity (if such covered entity maintains such a Web site); and

(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.

(3) COST OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) shall provide such notification at no cost to the individual.

(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) any covered entity 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 sub-

section, the maximum civil penalty for which any covered entity may be liable under this subsection for all actions shall not exceed—

(A) $1,000,000 for all violations of section 2 resulting from the same related act or omission; and

(B) $1,000,000 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. CRIMINAL PENALTIES FOR CYBER CRIMES.

Part I of title 18, United States Code, is amended—

(1) in chapter 47—

(A) in section 1028(b)—

(i) in paragraph (1)—

(I) in subparagraph (B), by inserting ''or'' after the semicolon;

(II) in subparagraph (C), by striking ''or'' after the semicolon; and

(III) by striking subparagraph (D);

(ii) by redesignating paragraphs (5) and (6), as paragraphs (6) and (7), respectively; and

(iii) by inserting after paragraph (4), the following:

''(5) for an offense under paragraph (7) of such subsection, a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 30 years, or both;'';

(B) in section 1028A(a)(1), by striking ''2 years'' and inserting ''4 years'';

(C) in section 1029(c)(1)—

(i) in subparagraph (A)—

(I) in clause (i), by striking ''a fine under this title or imprisonment for not more than 10 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 20 years''; and

(II) in clause (ii), by striking ''a fine under this title or imprisonment for not more than 15 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 30 years''; and

(ii) in subparagraph (B), by striking ''a fine under this title or imprisonment for not more than 20 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 40 years''; and

(D) in section 1030(c)—

(i) in paragraph (2)—

(I) in subparagraph (A), by striking ''subsection (a)(2), (a)(3),'' and inserting ''subsection (a)(3)'';

(II) in subparagraph (B)—

(aa) in the matter preceding clause (i), by striking ''a fine under this title or imprisonment for not more than 5 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 10 years''; and

(bb) in clause (iii), by striking ''and'' at the end;

(III) in subparagraph (C), by striking ''(a)(2),''; and

(IV) by adding at the end the following:

''(D) a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 2 years, or both, in the case of an offense under subsection (a)(2) which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

''(E) a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(2) which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;'';

(ii) in paragraph (3)—

(I) in subparagraph (A), by striking ''(a)(4) or''; and

(II) in subparagraph (B), by striking ''(a)(4), or'';

(iii) in paragraph (4)—

(I) in subparagraph (A), in the matter preceding clause (i), by striking ''a fine under this title, imprisonment for not more than 5 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 10 years'';

(II) in subparagraph (B), in the matter preceding clause (i), by striking ''a fine under this title, imprisonment for not more than 10 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 20 years'';

(III) in subparagraph (C), in the matter preceding clause (i), by striking ''a fine under this title, imprisonment for not more than 20 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 40 years'';

(IV) in subparagraph (D), in the matter preceding clause (i), by striking ''a fine under this title, imprisonment for not more than 10 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 20 years'';

(V) in subparagraph (E), by striking ''a fine under this title, imprisonment for not more than 20 years'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 40 years'';

(VI) in subparagraph (F)—

(aa) by striking ''a fine under this title'' and inserting ''a fine of not more than $500,000 ($1,000,000 if the person is an organization)''; and

(bb) by striking ''or'' at the end; and

(VII) in subparagraph (G)—

(aa) in the matter preceding clause (i), by striking ''under this title, imprisonment for not more than 1 year'' and inserting ''of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 2 years''; and

(bb) in clause (ii), by striking the period at the end and inserting ''; and''; and

(iv) by adding at the end the following:

''(5)(A) a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(4) which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

''(B) a fine of not more than $500,000 ($1,000,000 if the person is an organization), imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(4) which occurs after a conviction for another offense under

this section, or an attempt to commit an offense punishable under this subparagraph.'';

(2) in chapter 63—

(A) in section 1343—

(i) in the first sentence, by striking ''fined under this title or imprisoned not more than 20 years'' and inserting ''fined not more than $500,000 ($1,000,000 if the person is an organization), imprisoned not more than 40 years''; and

(ii) in the second sentence, by striking ''$1,000,000 or imprisoned not more than 30 years'' and inserting ''$2,000,000, imprisoned for any term of years or for life''; and

(B) in section 1344, by striking ''$1,000,000 or imprisoned not more than 30 years'' and inserting ''$2,000,000 or imprisoned for any term of years or for life''; and

(3) in section 1519, by striking ''fined under this title, imprisoned not more than 20 years'' and inserting ''fined not more than $500,000 ($1,000,000 if the person is an organization), imprisoned not more than 40 years''.

SEC. 6. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is physically present within a country with which the United States does not have a mutual legal assistance treaty or an extradition treaty;

(2) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or its citizens; and

(3) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) BILATERAL CONSULTATIONS.—The Secretary of State, or designee, shall consult with the appropriate government official of each country in which one or more international cyber criminals are physically present to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that identifies—

(A) the number of international cyber criminals who are located in countries that do not have an extradition treaty or mutual legal assistance treaty with the United States, broken down by country;

(B) the dates on which an official of the Department of State, as a result of this Act, discussed ways to thwart or prosecute international cyber criminals in a bilateral conversation with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited into the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

(D) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(E) the Committee on Foreign Affairs of the House of Representatives;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives; and

(H) the Committee on Financial Services of the House of Representatives.

SEC. 7. 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) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated under section 3(a)(2)(A).

(6) 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 one 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.

(iv) Federal or State government issued identification card.

(v) A username or email address, in combination with a password or security question and answer that would allow access to an online account.

(vi) Medical information, including the medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional of the individual.

(vii) Health insurance information, including a health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or any information in a health insurance application or claim history filed by the individual.

(viii) An individual taxpayer identification number.

(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 gov-

ernment 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.

(7) 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. 8. 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. 9. EFFECTIVE DATE.

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

○