[DISCUSSION DRAFT]

FEBRUARY 16, 2018

115TH CONGRESS
2D SESSION

H. R. _____

To [be provided]

IN THE HOUSE OF REPRESENTATIVES

Mr. LUETKEMEYER (for himself and Mrs. CAROLYN B. MALONEY of New York) introduced the following bill; which was referred to the Committee on _____

A BILL

To [be provided]

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 Acquisition and Technology Accountability and Security Act''.

SEC. 2. DEFINITIONS.

For purposes of this Act, the following definitions apply:

(1) AFFILIATE.—The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company

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

(3) BREACH OF DATA SECURITY.—The term ''breach of data security'' means the unauthorized acquisition of personal information from a covered entity, but does not include the good faith acquisition of personal information by an employee or agent of the entity, if the personal information is not used or subject to further unauthorized acquisition.

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

(5) CONSUMER.—The term ''consumer'' means an individual.

(6) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(7) COVERED ENTITY.—The term ''covered entity'' means any person, partnership, corporation, trust, estate, cooperative, association, or other entity that accesses, maintains, or stores personal, or handles personal information. For purposes of section 3, a covered entity includes a Federal agency.

(8) FINANCIAL INSTITUTION.—The term ''financial institution'' has the same meaning as in section 509(3) of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)).

(9) NON-PROFIT ORGANIZATION.—The term ''non-profit organization'' means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code. Such term shall not include a credit union as defined in section 101 of the Federal Credit Union Act. (12 U.S.C. 1752).

(10) PERSONAL INFORMATION.—

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

(i) A non-truncated Social Security number, driver's license number, passport number, alien registration number, or

other government-issued unique identification number.

(ii) A financial account number, alone or in combination with its security code, access code, or password that enables an individual to obtain credit, withdraw funds, or engage in a financial transaction.

(iii) Automatic measurements of biometric data unique to an individual that is required to authenticate an individual's identity to complete a financial transaction.

(iv) A user name in combination with any associated security code, access code, or password that is required for an individual to obtain money, or purchase goods, services, or any other thing of value.

(B) EXCEPTIONS.—The term ''personal information'' does not include—

(i) information that is rendered unusable, unreadable, or indecipherable; or

(ii) information available from a publicly available source, including information obtained from a news report, periodical, or other widely distributed media, or from

Federal, State, or local government records.

(11) THIRD PARTY.—

(A) IN GENERAL.—The term ''third party'' means any entity that processes, maintains, stores, or handles, or otherwise is permitted access to personal information in connection with providing services to a covered entity.

(B) EXCEPTION.—The term ''third party'' does not include a service provider.

(12) SERVICE PROVIDER.—The term ''service provider'' means any entity subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where such entity providing such service does not select or modify the content of the electronic data, is not the sender of 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. 3. PROTECTION OF INFORMATION.

(a) SECURITY SAFEGUARDS REQUIRED.—

(1) IN GENERAL.—Each covered entity shall develop, implement, and maintain administrative, technical, and physical safeguards that are reasonably designed to protect the security and confidentiality of personal information from unauthorized acquisition that is reasonably likely to result in identity theft, fraud, or economic loss.

(2) FLEXIBILITY OF SAFEGUARDS.—A covered entity's safeguards under paragraph (1) shall be appropriate to—

(A) the size and complexity of the covered entity;

(B) the nature and scope of the activities of the covered entity;

(C) the cost of available tools to improve security and reduce vulnerabilities; and

(D) the sensitivity of the personal information maintained by the covered entity.

(3) ELEMENTS.—As part of its reasonable safeguards, a covered entity shall—

(A) designate an owner, officer, employee, or employees to maintain safeguards;

(B) identify material internal and external risks to the security and confidentiality of personal information and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the covered entity's operations, such as—

(i) employee training and management;

(ii) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(iii) detecting, preventing and responding to attacks, intrusions, or other systems failures;

(C) implement safeguards designed to control the risks identified in its risk assessment, and regularly assess the effectiveness of those safeguards;

(D) maintain reasonable procedures for the security of personal information by third parties to require that such third parties maintain rea-

sonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such information; and

(E) evaluate the safeguards and make reasonable adjustments to these safeguards in light of any material changes in technology, internal or external threats to personal information, and the covered entity's own changing business arrangements or operations.

(b) ADMINISTRATIVE REQUIREMENT.—If a covered entity has a board of directors, the covered entity shall report to its board or an appropriate committee of the board at least annually, including describing the overall status of the safeguards and the covered entity's compliance with this Act.

SEC. 4. NOTIFICATION OF BREACH OF DATA SECURITY.

(a) PRELIMINARY INVESTIGATION REQUIRED.—If a covered entity believes that a breach of data security containing personal information may have occurred, the covered entity shall conduct an immediate investigation to—

(1) assess the nature and scope of the incident;

(2) identify any personal information that may have been involved in the incident;

(3) determine if the personal information has or is likely to have been acquired without authorization; and

(4) take reasonable measures to restore the security and confidentiality of the systems compromised in the breach of data security.

(b) NOTICE REQUIRED.—

(1) IN GENERAL.—If, after completion of the preliminary investigation under subsection (a), a covered entity determines that there is a reasonable risk that the breach of data security has resulted in or will result in identity theft, fraud, or economic loss to the consumers to whom the personal information involved in the incident relates, the covered entity shall immediately notify without unreasonable delay—

(A) the Secret Service or the Federal Bureau of Investigation, if the breach of data security involves personal information relating to 5,000 or more consumers;

(B) the appropriate agency or authority defined in section 5, if the breach of data security involves personal information relating to 5,000 or more consumers;

(C) if the breach of data security involves payment card numbers, any relevant payment card network, if the breach of data security involves personal information relating to more than 5,000 or more consumers; and

(D) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach of data security involves personal information relating to 5,000 or more consumers.

(2) CONSUMER NOTIFICATION.—If a covered entity determines after completion of the preliminary investigation under subsection (a) that there is a reasonable risk that the breach of data security has resulted in identity theft, fraud, or economic loss to any consumer, the covered entity shall immediately notify such consumer, without unreasonable delay except under circumstances outlined in paragraph (5).

(3) FORM OF NOTIFICATION.—Notification to consumers under paragraph (2) shall be provided by—

(A) written notification;

(B) telephonic notification;

(C) email notification; or

(D) substitute notification made available through a link on the home page of the covered entity's website and broadcast media in the States where the consumers reside, if providing written, telephonic, or email notification is not feasible due to lack of sufficient contact information for the majority of consumers that the entity is required to notify.

(4) CONTENT OF NOTIFICATION.—The information contained in the notification to consumers under paragraph (2) shall be maintained by the covered entity and made available to consumers upon request for not less than six months and shall include—

(A) a description of the type of personal information maintained by the covered entity that was involved in the breach of data security;

(B) a description of the actions taken by the covered entity to restore the security and confidentiality of the personal information involved in the breach of data security; and

(C) a description of steps a consumer can take to protect themselves from identity theft.

(5) DELAY REQUIRED WHEN REQUESTED BY LAW ENFORCEMENT.—A covered entity shall delay

any notification described under paragraph (2) if such delay is requested by the Secret Service, the Federal Bureau of Investigation, or State law enforcement. The covered entity shall notify pursuant to such paragraph when the Secret Service, the Federal Bureau of Investigation, or State law enforcement, as applicable, determines that notification is permitted.

(c) REQUIREMENTS OF THIRD PARTIES.—

(1) REQUIREMENTS.—If a third party becomes aware that a breach of data security involving data in electronic form containing personal information that is maintained or otherwise handled on behalf of a covered entity has or may have occurred, the third party shall—

(A) investigate the nature and scope of the suspected breach of data security;

(B) promptly notify the covered entity whose data has or may have been compromised;

(C) cooperate with the covered entity by providing sufficient information about the suspected breach of data security to allow the covered entity to meet its obligations under this section. That cooperation shall include information , but need not be limited to—

(i) informing the covered entity of the suspected breach of data security, including giving notice of the date or approximate date of the breach of data security and the nature of the breach of data security; and

(ii) informing the covered entity of any steps the third party has taken or plans to take relating to the suspected breach of data security; and

(D) notify any other person as has been previously agreed to in a writing signed by the third party and the covered entity.

(2) RULES OF CONSTRUCTION.—

(A) Nothing in this subsection shall be construed to interfere with the right of a covered entity and third party to agree in writing regarding their respective obligations to provide notice under this section.

(B) Nothing in subparagraph (C) of paragraph (1) shall be interpreted to require a third party to disclose confidential business information or trade secrets to a covered entity.

(d) REQUIREMENTS OF SERVICE PROVIDERS.—

(1) REQUIREMENTS.—If a service provider becomes aware of a breach of data security involving data in electronic form containing personal information that is owned or licensed 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 that initiated such connection, transmission, routing, or storage of the data containing personal information breached if such covered entity can be reasonably identified. If a service provider is acting solely as a service provider for purposes of this subsection, the service provider has no other obligations under this section.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to prohibit a service provider from being considered for purposes of this Act as a covered entity for the purposes of information it collects as a first party.

(e) COMMUNICATIONS WITH FINANCIAL ACCOUNT HOLDERS.—

(1) GENERALLY.—If a covered entity experiences a breach of data security involving personal information, a financial institution that holds an ac-

count to which the personal information relates may communicate with the account holder regarding the breach, including—

(A) an explanation that the financial institution was not breached, and that the breach occurred at a covered entity that had access to the consumer's personal information; and

(B) identify the covered entity that experienced the breach after the covered entity has provided notice required by subsection (b)(2).

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed as creating an obligation on a financial institution to provide notice to consumers.

(f) NOTIFICATION FOR CHANGE OF ONLINE ACCOUNT CREDENTIALS.—In the case of a breach of data security involving personal information for an online account, and no other personal information, the covered entity may comply with this section by providing the notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her security code, access code, or password as applicable to protect the online account with the covered entity.

SEC. 5. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) ENFORCEMENT PRACTICES.—A violation of section 3 or 4 shall be enforced in the same manner as a violation of a rule prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF COMMISSION.—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, and any covered entity subject to the Commission's authority who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(3) JURISDICTION.—

(A) Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), the Commission shall have authority over common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) to enforce this Act.

(B) Notwithstanding any jurisdictional limitation of the Federal Trade Commission Act, the Commission shall have authority over any nonprofit organization to enforce this Act.

(4) PENALTY FACTORS.—In determining the amount of a civil penalty, the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, proactive security measures taken, material harm to consumers, and the overall economics of covered entity such as annual number of customers, revenue or employees, and such other matters as justice may require shall be taken into account.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—With respect to a covered entity that is not a financial institution, in any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity that violates section 3 or 4 of this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin further violation of such section by the defendant;

(B) compel compliance with such section; or

(C) obtain civil penalties in the amount determined in the same manner as subsection (a).

(2) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL.—Whenever a civil action under this subsection is pending and another civil action or actions are commenced pursuant to this subsection in a different Federal district court or courts that involve one or more common questions of fact, such action or actions shall be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia. No such actions shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by a State attorney general.

(3) INTERVENTION BY THE FEDERAL TRADE COMMISSION.—

(A) NOTICE AND INTERVENTION.—In all cases, the attorney general of a State shall provide prior written notice of any action under

paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case which such prior notice is not feasible, in which case such attorney general shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(i) to intervene in the action;

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

(iii) to file for petitions of appeal.

(B) PENDING PROCEEDINGS.—If the Federal Trade Commission initiates a Federal civil action for a violation of this Act, no State attorney general may bring an action for a violation of this Act that resulted from the same or related acts or omissions against a defendant named in the civil action initiated by the Federal Trade Commission. If the Federal Trade Commission has instituted or intervened in a proceeding or a civil action for a violation of this Act, no State attorney general may bring an action under this subsection against any covered entity named as a defendant in such civil

action for any violation of this Act alleged in the complaint.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act 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 or affirmations; or

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

(5) LIMITATION.—An attorney general of a State may not bring an action under this subsection against any covered entity that is a financial institution, or its affiliates.

(c) ENFORCEMENT FOR FINANCIAL INSTITUTIONS.—Subject to subsection (e) and notwithstanding any other provisions of law, sections 3 and 4 shall be enforced exclusively under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) by each agency or authority with authority to enforce section 501(b), with respect to any financial institution or subsidiary of a financial institution

that is subject to the jurisdiction of such agency or authority pursuant to section 501(b).

(d) INSURANCE.—This Act shall not apply to any person engaged in providing insurance.

(e) COMPLIANCE.—

(1) FINANCIAL INSTITUTIONS.—A covered entity that is a financial institution shall be deemed to be in compliance with sections 3 and 4, if the financial institution—

(A) maintains policies and procedures to protect the confidentiality and security of personal information that are consistent with the policies and procedures of the financial institution that are designed to comply with the requirements of section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and any regulations or guidance prescribed under that section that are applicable to the financial institution;

(B) is an affiliate of a bank holding company, bank, or savings and loan holding company that maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of a bank or

savings association that is an affiliate of the financial institution, and the policies and procedures of the bank or savings association are designed to comply with the investigation and notice requirements established by regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to the bank holding company or bank, or savings and loan holding company or savings association; and

(C) provides services that are subject to regulation and examination by a Federal banking agency under the Bank Services Company Act (12 U.S.C. 1861 et seq.) to the extent such services are subject by contract to breach notification obligations imposed by financial institutions in contracts pursuant to Federal banking agency guidance.

(2) OTHER COVERED ENTITIES.—A covered entity shall be deemed to be in compliance with sections 3 and 4—

(A) if the entity is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (41

U.S.C. 1320d-2 note), to the extent that the entity is in compliance with such regulations and to the extent of the personal information is protected by such Act; or

(B) if the entity is in compliance with sections 13402 and 13407 of the HITECH Act (42 U.S.C. 17932; 17937), to the extent the personal information is protected by such Act.

SEC. 6. RELATION TO STATE LAW.

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, with respect to securing information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of data, except as applicable to any person engaged in providing insurance.

SEC. 7. RELATION TO OTHER LAWS.

(a) **[____]**.—Notwithstanding any other provision of law, the Federal Communications Commission shall have no authority to apply any regulations to covered entities with respect to securing information from unauthorized access and acquisition, including notification of unauthorized access and acquisition to data, unless such regulations pertain solely to 9–1–1 calls.

(b) RULE OF CONSTRUCTION.—Nothing in this section otherwise limits the Federal Communication Commission's authority with respect to sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551).

(c) PRESERVATION OF COMMISSION AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 8. EFFECTIVE DATE.

This Act shall take effect 18 months after the date of the enactment of this Act.