I

115TH CONGRESS
1ST SESSION

H. R. 3904

To direct the Federal Trade Commission to prescribe rules that require covered entities to secure sensitive personally identifiable information against a security breach.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 2, 2017

Mrs. DINGELL introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To direct the Federal Trade Commission to prescribe rules that require covered entities to secure sensitive personally identifiable information against a security breach.

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 Protection Act of 2017''.

SEC. 2. REASONABLE MEASURES TO SECURE SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) RULES REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Commission

shall prescribe rules in accordance with section 553 of title 5, United States Code, that require a covered entity to employ reasonable measures to secure sensitive personally identifiable information maintained by such entity against a security breach.

(b) FACTORS FOR CONSIDERATION IN DETERMINING REASONABLENESS.—The rules prescribed under subsection (a) shall provide for the consideration, in determining whether measures employed by a covered entity are reasonable, of factors that include the following:

(1) Whether the covered entity follows any applicable best practices issued by the National Institute of Standards and Technology.

(2) Whether the covered entity takes reasonable steps to keep software up-to-date in order to mitigate security vulnerabilities, especially critical security vulnerabilities, in any database or other computer system in which sensitive personally identifiable information is maintained by such entity.

(c) CONSIDERATION OF BINDING ARBITRATION CLAUSES IN DETERMINING CIVIL PENALTY AMOUNT.—If a violation of the rules prescribed under subsection (a) results in a security breach and the covered entity experiencing such breach offers any credit, identity theft, fraud, or similar monitoring or protection service to consumers

as a result of such breach, in determining the amount of a civil penalty under section 5(m) of the Federal Trade Commission Act (15 U.S.C. 45(m)) for such violation, the court shall consider, in addition to the factors required to be considered under such section, imposing a higher penalty if the terms and conditions applicable to such service include a requirement that any disputes be resolved by binding arbitration (or a requirement that consumers take action to opt out of binding arbitration) than if such terms and conditions did not include any such requirement.

SEC. 3. ENFORCEMENT BY FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of a rule prescribed under section 2(a) shall be treated 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)) regarding unfair or deceptive acts or practices.

(b) POWERS OF COMMISSION.—The Commission shall enforce the rules prescribed under section 2(a) 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. Any person who violates such

a rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

SEC. 4. DEFINITIONS.

In this Act:

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

(2) COVERED ENTITY.—The term ''covered entity'' means any person, partnership, or corporation—

(A) over which the Commission has jurisdiction under section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(B) that maintains sensitive personally identifiable information of more than 100,000 individuals.

(3) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; or

(ii) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term ''security breach'' does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an element of the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))).

(4) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—

(A) IN GENERAL.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form, that includes one or more of the following:

(i) An individual's first and last name or first initial and last name in combina-

tion with any two of the following data elements:

(I) Home address or telephone number.

(II) Mother's maiden name.

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

(ii) A Social Security number (but not including only the last four digits of a Social Security number), driver's license number, passport number, or alien registration number or other Government-issued unique identification number.

(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, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(v) A user name or electronic mail address, in combination with a password or

security question and answer that would permit access to an online account.

(vi) Any combination of the following data elements:

(I) An individual's first and last name or first initial and last name.

(II) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(III) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule prescribed in accordance with section 553 of title 5, United States Code, amend the definition of ''sensitive personally identifiable information'' to the extent that such amendment will accomplish the purposes of this Act. In amending the definition, the Commission may determine—

(i) that any particular combinations of information are sensitive personally identifiable information; or

(ii) that any particular piece of information, on its own, is sensitive personally identifiable information.

○