

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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Data Protection Act  
5 of 2017”.

6 **SEC. 2. REASONABLE MEASURES TO SECURE SENSITIVE**  
7 **PERSONALLY IDENTIFIABLE INFORMATION.**

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

1 shall prescribe rules in accordance with section 553 of title  
2 5, United States Code, that require a covered entity to  
3 employ reasonable measures to secure sensitive personally  
4 identifiable information maintained by such entity against  
5 a security breach.

6 (b) FACTORS FOR CONSIDERATION IN DETERMINING  
7 REASONABLENESS.—The rules prescribed under sub-  
8 section (a) shall provide for the consideration, in deter-  
9 mining whether measures employed by a covered entity are  
10 reasonable, of factors that include the following:

11 (1) Whether the covered entity follows any ap-  
12 plicable best practices issued by the National Insti-  
13 tute of Standards and Technology.

14 (2) Whether the covered entity takes reasonable  
15 steps to keep software up-to-date in order to miti-  
16 gate security vulnerabilities, especially critical secu-  
17 rity vulnerabilities, in any database or other com-  
18 puter system in which sensitive personally identifi-  
19 able information is maintained by such entity.

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

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

12 **SEC. 3. ENFORCEMENT BY FEDERAL TRADE COMMISSION.**

13 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—  
14 A violation of a rule prescribed under section 2(a) shall  
15 be treated as a violation of a rule prescribed under section  
16 18(a)(1)(B) of the Federal Trade Commission Act (15  
17 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts  
18 or practices.

19 (b) POWERS OF COMMISSION.—The Commission  
20 shall enforce the rules prescribed under section 2(a) in the  
21 same manner, by the same means, and with the same ju-  
22 risdiction, powers, and duties as though all applicable  
23 terms and provisions of the Federal Trade Commission  
24 Act (15 U.S.C. 41 et seq.) were incorporated into and  
25 made a part of this Act. Any person who violates such

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

4 **SEC. 4. DEFINITIONS.**

5 In this Act:

6 (1) COMMISSION.—The term “Commission”  
7 means the Federal Trade Commission.

8 (2) COVERED ENTITY.—The term “covered en-  
9 tity” means any person, partnership, or corpora-  
10 tion—

11 (A) over which the Commission has juris-  
12 diction under section 5(a)(2) of the Federal  
13 Trade Commission Act (15 U.S.C. 45(a)(2));  
14 and

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

18 (3) SECURITY BREACH.—

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

1 (i) the unauthorized acquisition of  
2 sensitive personally identifiable informa-  
3 tion; or

4 (ii) access to sensitive personally iden-  
5 tifiable information that is for an unau-  
6 thorized purpose, or in excess of authoriza-  
7 tion.

8 (B) EXCLUSION.—The term “security  
9 breach” does not include any lawfully author-  
10 ized investigative, protective, or intelligence ac-  
11 tivity of a law enforcement agency of the  
12 United States, a State, or a political subdivision  
13 of a State, or of an element of the intelligence  
14 community (as defined in section 3(4) of the  
15 National Security Act of 1947 (50 U.S.C.  
16 3003(4))).

17 (4) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
18 FORMATION.—

19 (A) IN GENERAL.—The term “sensitive  
20 personally identifiable information” means any  
21 information or compilation of information, in  
22 electronic or digital form, that includes one or  
23 more of the following:

24 (i) An individual’s first and last name  
25 or first initial and last name in combina-

1                   tion with any two of the following data ele-  
2                   ments:

3                   (I) Home address or telephone  
4                   number.

5                   (II) Mother's maiden name.

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

8                   (ii) A Social Security number (but not  
9                   including only the last four digits of a So-  
10                  cial Security number), driver's license  
11                  number, passport number, or alien reg-  
12                  istration number or other Government-  
13                  issued unique identification number.

14                  (iii) Unique biometric data such as a  
15                  finger print, voice print, a retina or iris  
16                  image, or any other unique physical rep-  
17                  resentation.

18                  (iv) A unique account identifier, in-  
19                  cluding a financial account number or  
20                  credit or debit card number, electronic  
21                  identification number, user name, or rout-  
22                  ing code.

23                  (v) A user name or electronic mail ad-  
24                  dress, in combination with a password or

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

3 (vi) Any combination of the following  
4 data elements:

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

7 (II) A unique account identifier,  
8 including a financial account number  
9 or credit or debit card number, elec-  
10 tronic identification number, user  
11 name, or routing code.

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

16 (B) MODIFIED DEFINITION BY RULE-  
17 MAKING.—The Commission may, by rule pre-  
18 scribed in accordance with section 553 of title  
19 5, United States Code, amend the definition of  
20 “sensitive personally identifiable information”  
21 to the extent that such amendment will accom-  
22 plish the purposes of this Act. In amending the  
23 definition, the Commission may determine—

1                   (i) that any particular combinations of  
2 information are sensitive personally identi-  
3 fiable information; or

4                   (ii) that any particular piece of infor-  
5 mation, on its own, is sensitive personally  
6 identifiable information.

○