

115TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

To create an Office of Cybersecurity at the Federal Trade Commission for supervision of data security at consumer reporting agencies, to require the promulgation of regulations establishing standards for effective cybersecurity at consumer reporting agencies, to impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

---

Ms. WARREN (for herself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on

---

---

**A BILL**

To create an Office of Cybersecurity at the Federal Trade Commission for supervision of data security at consumer reporting agencies, to require the promulgation of regulations establishing standards for effective cybersecurity at consumer reporting agencies, to impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk, and for other purposes.

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

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Data Breach Preven-  
3 tion and Compensation Act of 2018”.

4 **SEC. 2. DEFINITIONS.**

5 In this Act:

6 (1) CAREER APPOINTEE.—The term “career  
7 appointee” has the meaning given the term in sec-  
8 tion 3132(a) of title 5, United States Code.

9 (2) COMMISSION.—The term “Commission”  
10 means the Federal Trade Commission.

11 (3) COVERED BREACH.—The term “covered  
12 breach” means any instance in which at least 1 piece  
13 of personally identifying information is exposed or is  
14 reasonably likely to have been exposed to an unau-  
15 thORIZED party.

16 (4) COVERED CONSUMER REPORTING AGEN-  
17 CY.—The term “covered consumer reporting agency”  
18 means—

19 (A) a consumer reporting agency described  
20 in section 603(p) of the Fair Credit Reporting  
21 Act (15 U.S.C. 1681a(p)); or

22 (B) a consumer reporting agency that  
23 earns not less than \$7,000,000 in annual rev-  
24 enue from the sales of consumer reports.

25 (5) DIRECTOR.—The term “Director” means  
26 the Director of the Office of Cybersecurity.

1           (6) **DETAIL.**—The term “detail” means a tem-  
2           porary assignment of an employee to a different po-  
3           sition for a specified period, with the employee re-  
4           turning to his or her regular duties at the end of the  
5           detail.

6           (7) **PERSONALLY IDENTIFYING INFORMA-**  
7           **TION.**—The term “personally identifying informa-  
8           tion” means—

9                   (A) a social security number;

10                   (B) a driver’s license number;

11                   (C) a passport number;

12                   (D) an alien registration number or other  
13           government-issued unique identification num-  
14           ber;

15                   (E) unique biometric data, such as  
16           faceprint, fingerprint, voice print, iris image, or  
17           other unique physical representations;

18                   (F) an individual’s first and last name or  
19           first initial and last name in combination with  
20           any information that relates to the individual’s  
21           past, present, or future physical or mental  
22           health or condition, or to the provision of health  
23           care to or diagnosis of the individual;

1 (G)(i) a financial account number, debit  
2 card number, or credit card number of the con-  
3 sumer; or

4 (ii) any passcode required to access an ac-  
5 count described in clause (i); and

6 (H) such additional information, as deter-  
7 mined by the Director.

8 **SEC. 3. CYBERSECURITY STANDARDS AND FTC AUTHORITY.**

9 (a) **ESTABLISHMENT.**—There is established in the  
10 Commission an Office of Cybersecurity, which shall be  
11 headed by a Director, who shall be a career appointee.

12 (b) **DUTIES.**—The Office of Cybersecurity—

13 (1) shall—

14 (A) supervise covered consumer reporting  
15 agencies with respect to data security;

16 (B) promulgate regulations for effective  
17 data security for covered consumer reporting  
18 agencies, including regulations that require cov-  
19 ered consumer reporting agencies to—

20 (i) provide the Commission with de-  
21 scriptions of technical and organizational  
22 security measures, including—

23 (I) system and network security  
24 measures, including—

1 (aa) asset management, in-  
2 cluding—

3 (AA) an inventory of  
4 authorized and unauthorized  
5 devices;

6 (BB) an inventory of  
7 authorized and unauthorized  
8 software, including applica-  
9 tion whitelisting; and

10 (CC) secure configura-  
11 tions for hardware and soft-  
12 ware;

13 (bb) network management  
14 and monitoring, including—

15 (AA) mapped data  
16 flows, including functional  
17 mission mapping;

18 (BB) maintenance,  
19 monitoring, and analysis of  
20 audit logs;

21 (CC) network seg-  
22 mentation; and

23 (DD) local and remote  
24 access privileges, defined  
25 and managed; and

## 6

- 1 (cc) application manage-  
2 ment, including—
- 3 (AA) continuous vulner-  
4 ability assessment and reme-  
5 diation;
- 6 (BB) server application  
7 hardening;
- 8 (CC) vulnerability han-  
9 dling such as coordinated  
10 vulnerability disclosure pol-  
11 icy; and
- 12 (DD) patch manage-  
13 ment, including at, or near,  
14 real-time dashboards of  
15 patch implementation across  
16 network hosts; and
- 17 (II) data security, including—
- 18 (aa) data-centric security  
19 mechanisms such as format-pre-  
20 serving encryption, cryptographic  
21 data-splitting, and data-tagging  
22 and lineage;
- 23 (bb) encryption for data at  
24 rest;

1 (cc) encryption for data in  
2 transit;

3 (dd) system-wide data mini-  
4 mization evaluations and policies;  
5 and

6 (ee) data recovery capability;  
7 and

8 (ii) create and maintain documenta-  
9 tion demonstrating that the covered con-  
10 sumer reporting agency is employing rea-  
11 sonable technical measures and corporate  
12 governance processes for continuous moni-  
13 toring of data, intrusion detection, and  
14 continuous evaluation and timely patching  
15 of vulnerabilities;

16 (C) annually examine the data security  
17 measures of covered consumer reporting agen-  
18 cies for compliance with the standards promul-  
19 gated under subparagraph (B);

20 (D) investigate any covered consumer re-  
21 porting agency if the Office has reason to sus-  
22 pect a potential covered breach or noncompli-  
23 ance with the standards promulgated under  
24 subparagraph (B);

1           (E) after consultation with members of the  
2           technical and academic communities, develop a  
3           rigorous, repeatable methodology for evaluating,  
4           testing, and measuring effective data security  
5           practices of covered consumer reporting agen-  
6           cies, that employs forms of static and dynamic  
7           software analysis and penetration testing;

8           (F) submit to Congress an annual report  
9           on the findings on any investigation under sub-  
10          paragraph (C);

11          (G) determine whether covered consumer  
12          reporting agencies are complying with the regu-  
13          lations promulgated under subparagraph (B);  
14          and

15          (H) coordinate with the National Institute  
16          of Standards and Technology and the National  
17          Cybersecurity and Communications Integration  
18          Center of the Department of Homeland Secu-  
19          rity; and

20          (2) may—

21                (A) investigate any breach to determine if  
22                the covered consumer reporting agency was in  
23                compliance with the regulations promulgated  
24                under paragraph (1)(B); and



1 (B) if the Commission has reason to be-  
2 lieve that any covered consumer reporting agen-  
3 cy is violating, or is about to violate, a regula-  
4 tion promulgated under paragraph (1)(B),  
5 bring a suit in a district court of the United  
6 States to enjoin any such act or practice.

7 (c) STAFF.—

8 (1) IN GENERAL.—The Director shall, without  
9 regard to the civil service laws and regulations, ap-  
10 point such personnel, including computer security re-  
11 searchers and practitioners with technical expertise  
12 in computer science, engineering, and cybersecurity,  
13 as the Director determines are necessary to carry  
14 out the duties of the Office.

15 (2) DETAILS.—An employee of the National In-  
16 stitute of Standards and Technology, the Bureau of  
17 Consumer Financial Protection, or the National Cy-  
18 bersecurity and Communications Integration Center  
19 of the Department of Homeland Security may be de-  
20 tailed to the Office, without reimbursement, and  
21 such detail shall be without interruption or loss of  
22 civil service status or privilege.

23 **SEC. 4. NOTIFICATION AND ENFORCEMENT.**

24 (a) NOTIFICATION.—Not later than 10 days after a  
25 covered breach, the covered consumer reporting agency

1 that was subject to the covered breach shall notify the  
2 Commission of the covered breach.

3 (b) PENALTY.—

4 (1) IN GENERAL.—In the event of a covered  
5 breach, the Commission shall, not later than 30 days  
6 after the date on which the Commission receives no-  
7 tification of the covered breach, commence a civil ac-  
8 tion to recover a civil penalty in a district court of  
9 the United States against the covered consumer re-  
10 porting agency that was subject to the covered  
11 breach.

12 (2) DETERMINING PENALTY AMOUNT.—

13 (A) IN GENERAL.—Except as provided in  
14 subparagraph (B), in determining the amount  
15 of a civil penalty under paragraph (1), the  
16 court shall impose a civil penalty on a covered  
17 consumer reporting agency of—

18 (i) \$100 for each consumer whose  
19 first and last name, or first initial and last  
20 name, and at least 1 item of personally  
21 identifying information was compromised;  
22 and

23 (ii) an additional \$50 for each addi-  
24 tional item of personally identifying infor-  
25 mation compromised for each consumer.

1 (B) EXCEPTION.—

2 (i) IN GENERAL.—Except as provided  
3 in clause (ii), a court may not impose a  
4 civil penalty under this subsection in an  
5 amount greater than 50 percent of the  
6 gross revenue of the covered consumer re-  
7 porting agency for the previous fiscal year  
8 before the date on which the covered con-  
9 sumer reporting agency became aware of  
10 the covered breach.

11 (ii) PENALTY DOUBLED.—A court  
12 shall impose a civil penalty on a covered  
13 consumer reporting agency double the pen-  
14 alty described in subparagraph (A), but  
15 not greater than 75 percent of the gross  
16 revenue of the covered consumer reporting  
17 agency for the previous fiscal year before  
18 the date on which the covered consumer  
19 reporting agency became aware of the cov-  
20 ered breach if—

21 (I) the covered consumer report-  
22 ing agency fails to notify the Commis-  
23 sion of a covered breach before the  
24 deadline established under subsection  
25 (a); or

1 (II) the covered consumer report-  
2 ing agency violates any regulation  
3 promulgated under section 3(b)(1)(C).

4 (3) PROCEEDS OF THE PENALTIES.—Of the  
5 penalties assessed under this subsection—

6 (A) 50 percent shall be used for cybersecu-  
7 rity research and inspections by the Office of  
8 Cybersecurity; and

9 (B) 50 percent shall be used by the Com-  
10 mission to be divided fairly among consumers  
11 affected by the covered breach.

12 (4) NO PREEMPTION.—Nothing in this sub-  
13 section shall preclude an action by a consumer under  
14 State or other Federal law.

15 (c) INJUNCTIVE RELIEF.—The Commission may  
16 bring suit in a district court of the United States or in  
17 the United States court of any Territory to enjoin a cov-  
18 ered consumer reporting agency to implement or correct  
19 a particular security measure in order to promote effective  
20 security.

21 **SEC. 5. AUTHORIZATION OF APPROPRIATIONS.**

22 There are authorized to be appropriated  
23 \$100,000,000 to carry out this Act, to remain available  
24 until expended.