

116TH CONGRESS  
1ST SESSION

# S. 1336

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

MAY 7, 2019

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

---

## 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 2019”.

4 **SEC. 2. DEFINITIONS.**

5 In this Act:

6 (1) **AFFECTED CONSUMER.**—The term “af-  
7 fected consumer” means any individual to whom  
8 personally identifying information pertains that was,  
9 or that may have been, affected by a covered breach.

10 (2) **AGENCY.**—The term “agency” has the  
11 meaning given the term in section 551 of title 5,  
12 United States Code.

13 (3) **CAREER APPOINTEE.**—The term “career  
14 appointee” has the meaning given the term in sec-  
15 tion 3132(a) of title 5, United States Code.

16 (4) **COMMISSION.**—The term “Commission”  
17 means the Federal Trade Commission.

18 (5) **CONSUMER REPORT; CONSUMER REPORTING**  
19 **AGENCY.**—The terms “consumer report” and “con-  
20 sumer reporting agency” have the meanings given  
21 the terms in section 603 of the Fair Credit Report-  
22 ing Act (15 U.S.C. 1681a).

23 (6) **COVERED BREACH.**—The term “covered  
24 breach” means any instance in which not less than  
25 1 piece of personally identifying information held by  
26 a covered consumer reporting agency is exposed, or

1 is reasonably likely to have been exposed, to an un-  
2 authorized party.

3 (7) COVERED CONSUMER REPORTING AGEN-  
4 CY.—The term “covered consumer reporting agency”  
5 means—

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

9 (B) a consumer reporting agency that  
10 earns not less than \$7,000,000 in annual rev-  
11 enue from the sale of consumer reports.

12 (8) DETAIL.—The term “detail” means a tem-  
13 porary assignment of an employee to a different po-  
14 sition for a specified period, with the employee re-  
15 turning to the regular duties of the employee at the  
16 end of the specified period.

17 (9) DIRECTOR.—The term “Director” means  
18 the Director of the Office.

19 (10) OFFICE.—The term “Office” means the  
20 Office of Cybersecurity established under section  
21 3(a).

22 (11) PERSONALLY IDENTIFYING INFORMA-  
23 TION.—The term “personally identifying informa-  
24 tion” means, with respect to an individual—

1 (A) the social security number of the indi-  
2 vidual;

3 (B) a driver's license number of the indi-  
4 vidual;

5 (C) a passport number of the individual;

6 (D) an alien registration number or other  
7 government-issued unique identification number  
8 of the individual;

9 (E) unique biometric data, such as a  
10 faceprint, a fingerprint, a voice print, an iris  
11 image, or any other unique physical representa-  
12 tion of the individual;

13 (F) the first and last name of the indi-  
14 vidual, or the first initial of the first name and  
15 the last name of the individual, in combination  
16 with any information that relates to—

17 (i) the past, present, or future phys-  
18 ical or mental health or condition of the in-  
19 dividual; or

20 (ii) the provision of health care to, or  
21 a diagnosis of, the individual;

22 (G)(i) a financial account number, debit  
23 card number, or credit card number of the indi-  
24 vidual; or

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

3 (H) such additional information, as deter-  
 4 mined by the Director.

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

6 (a) ESTABLISHMENT.—There is established in the  
 7 Commission an Office of Cybersecurity, which shall be  
 8 headed by a Director, who shall be a career appointee.

9 (b) DUTIES.—The Office—

10 (1) shall—

11 (A) supervise covered consumer reporting  
 12 agencies with respect to data security;

13 (B) promulgate regulations, through notice  
 14 and comment rulemaking that complies with  
 15 section 553 of title 5, United States Code, for  
 16 effective data security for covered consumer re-  
 17 porting agencies, including requirements for a  
 18 covered consumer reporting agency to—

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

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

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

3 (AA) an inventory of  
4 devices of the covered con-  
5 sumer reporting agency that  
6 are authorized to access  
7 data maintained by the cov-  
8 ered consumer reporting  
9 agency;

10 (BB) an inventory of  
11 software that is authorized  
12 by the covered consumer re-  
13 porting agency to access  
14 data maintained by the cov-  
15 ered consumer reporting  
16 agency, including application  
17 whitelisting; and

18 (CC) secure configura-  
19 tions for hardware and soft-  
20 ware of the covered con-  
21 sumer reporting agency;

22 (bb) network management  
23 and monitoring, including—

1 (AA) mapped data  
2 flows, including functional  
3 mission mapping;

4 (BB) maintenance,  
5 monitoring, and analysis of  
6 audit logs;

7 (CC) network seg-  
8 mentation; and

9 (DD) local and remote  
10 access privileges, defined  
11 and managed; and

12 (cc) application manage-  
13 ment, including—

14 (AA) continuous vulner-  
15 ability assessment and reme-  
16 diation;

17 (BB) server application  
18 hardening;

19 (CC) vulnerability han-  
20 dling, such as coordinated  
21 vulnerability disclosure pol-  
22 icy; and

23 (DD) patch manage-  
24 ment, including at, or near,  
25 real-time dashboards of

1 patch implementation across  
2 network hosts; and

3 (II) data security measures, in-  
4 cluding—

5 (aa) data-centric security  
6 mechanisms such as format-pre-  
7 serving encryption, cryptographic  
8 data-splitting, and data-tagging  
9 and lineage;

10 (bb) encryption for data at  
11 rest;

12 (cc) encryption for data in  
13 transit;

14 (dd) systemwide data mini-  
15 mization evaluations and policies;  
16 and

17 (ee) data recovery capability;

18 (ii) employ reasonable technical meas-  
19 ures and corporate governance processes  
20 for continuous monitoring of data, intru-  
21 sion detection, and continuous evaluation  
22 and timely patching of vulnerabilities;

23 (iii) employ reasonable technical meas-  
24 ures and corporate governance processes  
25 that satisfy and exceed all relevant data se-



1 security policy recommendations contained in  
2 the framework of the National Institute of  
3 Standards and Technology entitled  
4 “Framework for Improving Critical Infra-  
5 structure Cybersecurity”, dated February  
6 12, 2014, or any successor thereto, as de-  
7 termined appropriate by the Office; and

8 (iv) create and maintain documenta-  
9 tion demonstrating that the covered con-  
10 sumer reporting agency is employing the  
11 technical measures and corporate govern-  
12 ance processes described in clauses (ii) and  
13 (iii);

14 (C) annually examine the data security  
15 measures of covered consumer reporting agen-  
16 cies for compliance with the requirements de-  
17 scribed in clauses (ii) and (iii) of subparagraph  
18 (B);

19 (D) investigate any covered consumer re-  
20 porting agency if the Office has reason to sus-  
21 pect—

22 (i) a covered breach has occurred and  
23 the covered consumer reporting agency was  
24 subject to the covered breach; or

1                   (ii) the covered consumer reporting  
2                   agency is not in compliance with the re-  
3                   quirements described in clauses (ii) and  
4                   (iii) of subparagraph (B);

5                   (E) after consultation with members of the  
6                   technical and academic communities, develop a  
7                   rigorous, repeatable methodology—

8                   (i) for evaluating, testing, and meas-  
9                   uring effective data security practices of  
10                  covered consumer reporting agencies; and

11                  (ii) that employs forms of static and  
12                  dynamic software analysis and penetration  
13                  testing;

14                  (F) submit to Congress an annual report  
15                  on the findings of each investigation carried out  
16                  under subparagraph (D) during the year cov-  
17                  ered by the report that includes a statement of  
18                  how Congress could enhance the authorities of  
19                  the Office in order to assist the Office in car-  
20                  rying out the duties of the Office under this  
21                  Act;

22                  (G) determine whether covered consumer  
23                  reporting agencies are complying with the re-  
24                  quirements described in clauses (ii) and (iii) of  
25                  subparagraph (B); and

1 (H) coordinate with the National Institute  
2 of Standards and Technology and the National  
3 Cybersecurity and Communications Integration  
4 Center of the Department of Homeland Secu-  
5 rity; and

6 (2) may—

7 (A) investigate any covered breach to de-  
8 termine if the covered consumer reporting agen-  
9 cy that was subject to the covered breach was  
10 in compliance with the requirements described  
11 in clauses (ii) and (iii) of paragraph (1)(B) as  
12 of the date on which the covered breach oc-  
13 curred; and

14 (B) if the Director has reason to believe  
15 that any covered consumer reporting agency is  
16 violating, or in the immediate future will vio-  
17 late, a requirement described in clause (ii) or  
18 (iii) of paragraph (1), bring a suit in an appro-  
19 priate district court of the United States to en-  
20 join any such act or practice.

21 (c) STAFF.—

22 (1) IN GENERAL.—The Director shall, without  
23 regard to the civil service laws and regulations, ap-  
24 point such personnel, including computer security re-  
25 searchers and practitioners with technical expertise

1 in computer science, engineering, and cybersecurity,  
2 as the Director determines are necessary to carry  
3 out the duties of the Office.

4 (2) DETAILS.—

5 (A) IN GENERAL.—An employee of the Na-  
6 tional Institute of Standards and Technology,  
7 the Bureau of Consumer Financial Protection,  
8 or the National Cybersecurity and Communica-  
9 tions Integration Center of the Department of  
10 Homeland Security may be detailed to the Of-  
11 fice, without reimbursement.

12 (B) CIVIL SERVICE STATUS AND PRIVI-  
13 LEGE.—Detail under subparagraph (A) shall be  
14 without interruption or loss of the civil service  
15 status or privilege of the employee who is de-  
16 tailed to the Office.

17 **SEC. 4. NOTIFICATION AND ENFORCEMENT.**

18 (a) NOTIFICATION.—

19 (1) NOTIFICATION TO THE COMMISSION AND  
20 RELEVANT FEDERAL LAW ENFORCEMENT AND IN-  
21 TELLIGENCE AGENCIES.—

22 (A) NOTIFICATION TO THE COMMISSION.—

23 Except as provided in paragraph (3), not later  
24 than 10 days after the date on which a covered  
25 breach occurs, any covered consumer reporting

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

4 (B) NOTIFICATION TO RELEVANT FED-  
5 ERAL LAW ENFORCEMENT AND INTELLIGENCE  
6 AGENCIES.—Not later than 10 days after the  
7 date on which the Commission receives a notifi-  
8 cation under subparagraph (A) that a covered  
9 breach has occurred, the Commission shall—

10 (i) notify the relevant Federal law en-  
11 forcement agencies and intelligence agen-  
12 cies that the covered breach has occurred;  
13 and

14 (ii) with respect to the covered breach,  
15 consult with the relevant Federal law en-  
16 forcement agencies and intelligence agen-  
17 cies, as appropriate.

18 (2) NOTIFICATION TO AFFECTED CONSUMERS  
19 AND THE PUBLIC.—

20 (A) IN GENERAL.—Except as provided in  
21 paragraph (3), on an expeditious and practical  
22 timeline, as determined appropriate by the  
23 Commission, a covered consumer reporting  
24 agency that is subject to a covered breach  
25 shall—

(i) submit to each affected consumer with respect to whom the covered consumer reporting agency holds a piece of personally identifying information a notification regarding the covered breach that complies with subparagraph (B); and

(ii) publish on the internet website of the covered consumer reporting agency a notice that contains a statement of—

(I) the information described in clauses (i) and (ii) of subparagraph (B) and subclauses (I) and (II) of clause (iii) of that subparagraph; and

(II) the steps that the covered consumer reporting agency is taking to notify the affected consumers described in clause (i) regarding the covered breach.

(B) NOTIFICATION TO AFFECTED CONSUMERS.—In a notification to affected consumers under subparagraph (A)(i), the covered consumer reporting agency submitting the notification shall include a statement of—

(i) the fact that the covered breach occurred;

1 (ii) the approximate date on which the  
2 covered breach occurred; and

3 (iii) with respect to the covered  
4 breach—

5 (I) the number of affected con-  
6 sumers;

7 (II) the measures that the cov-  
8 ered consumer reporting agency is  
9 taking to remedy the covered breach;  
10 and

11 (III) the potential risks created  
12 by the covered breach, a list of which  
13 the covered consumer reporting agen-  
14 cy shall develop in consultation with  
15 the Office.

16 (3) DELAY OF NOTIFICATION AUTHORIZED FOR  
17 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-  
18 POSES.—

19 (A) NOTIFICATION BY LAW ENFORCEMENT  
20 AGENCY OR INTELLIGENCE AGENCY.—If a Fed-  
21 eral law enforcement agency or intelligence  
22 agency to which the Commission has provided  
23 notice under paragraph (1)(B)(i) determines  
24 that the notification required under paragraph

1           (2) may impede a criminal investigation or na-  
2           tional security activity—

3                   (i) the Federal law enforcement agen-  
4                   cy or intelligence agency shall provide writ-  
5                   ten notice to the Commission and the cov-  
6                   ered consumer reporting agency that was  
7                   subject to the covered breach that is the  
8                   subject of the notification that states—

9                           (I) that the notification required  
10                           under paragraph (2) shall be delayed  
11                           for law enforcement or national secu-  
12                           rity purposes; and

13                           (II) the date on which the delay  
14                           imposed under subclause (I) shall end;  
15                           and

16                   (ii) subject to subparagraph (B), the  
17                   covered consumer reporting agency that  
18                   was subject to the covered breach shall  
19                   delay notification under paragraph (2)  
20                   until the date described in clause (i)(II) of  
21                   this subparagraph.

22           (B) EXTENDED DELAY OF NOTIFICA-  
23           TION.—If the notification required under para-  
24           graph (2) is delayed under subparagraph (A) of  
25           this paragraph, a covered consumer reporting



1 agency that is required to provide notice under  
2 paragraph (2) shall provide that notice on an  
3 expeditious and practical timeline, as deter-  
4 mined appropriate by the Commission, after the  
5 date on which the law enforcement or national  
6 security delay under subparagraph (A) of this  
7 paragraph ends, unless a Federal law enforce-  
8 ment or intelligence agency to which the Com-  
9 mission has provided notice under paragraph  
10 (1)(B)(i) provides written notification to the  
11 Commission and the covered consumer report-  
12 ing agency that states—

13 (i) that further delay is necessary;

14 and

15 (ii) the date on which the further  
16 delay shall end.

17 (C) LAW ENFORCEMENT IMMUNITY.—No  
18 nonconstitutional cause of action shall lie in any  
19 court against any agency for acts relating to  
20 the delay of notification under subparagraph  
21 (A), or the extended delay of notification under  
22 subparagraph (B), for law enforcement or na-  
23 tional security purposes.

24 (b) PENALTY.—

1           (1) IN GENERAL.—In the event of a covered  
 2       breach, the Commission shall, not later than 30 days  
 3       after the date on which the Commission receives no-  
 4       tification of the covered breach under subsection  
 5       (a)(1)(A), commence a civil action to recover a civil  
 6       penalty in an appropriate district court of the  
 7       United States against the covered consumer report-  
 8       ing agency that was subject to the covered breach.

9           (2) DETERMINING PENALTY AMOUNT.—

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

15           (i) \$100 for each consumer for whom  
 16       the first and last name, or the first initial  
 17       of the first name and last name, and 1  
 18       other item of personally identifying infor-  
 19       mation were exposed to an unauthorized  
 20       party; and

21           (ii) in addition to the penalty imposed  
 22       under clause (i), an additional \$50 for  
 23       each item of personally identifying infor-  
 24       mation of the consumer, other than an

1 item described in that clause, that was ex-  
2 posed to an unauthorized party.

3 (B) EXCEPTION.—

4 (i) IN GENERAL.—Except as provided  
5 in clause (ii), in an action commenced  
6 under this subsection, a court may not im-  
7 pose a civil penalty in an amount that is  
8 more than 50 percent of the gross revenue  
9 of the covered consumer reporting agency  
10 against which the action is brought for the  
11 fiscal year before the fiscal year in which  
12 the covered consumer reporting agency be-  
13 came aware of the covered breach that is  
14 the subject of the action.

15 (ii) PENALTY DOUBLED.—In an ac-  
16 tion commenced under this subsection, the  
17 court shall impose a civil penalty on a cov-  
18 ered consumer reporting agency in an  
19 amount that is 2 times the amount of the  
20 penalty described in subparagraph (A), but  
21 not greater than 75 percent of the gross  
22 revenue of the covered consumer reporting  
23 agency for the fiscal year before the fiscal  
24 year in which the covered consumer report-

ing agency became aware of the covered breach that is subject to the action, if—

(I) the covered consumer reporting agency fails to notify the Commission of the covered breach before the deadline established under subsection (a)(1)(A); or

(II) the covered consumer reporting agency violates any requirement described in clause (ii) or (iii) of section 3(b)(1)(B).

(3) PROCEEDS OF THE PENALTIES.—Of the penalties imposed under this subsection—

(A) 50 percent shall be used for cybersecurity research and inspections by the Office; and

(B) 50 percent shall be used by the Office to be divided fairly among consumers affected by the covered breach.

(4) NO PREEMPTION.—Nothing in this subsection shall preclude an action by a consumer under State or other Federal law.

(c) INJUNCTIVE RELIEF.—The Commission, acting through the Office, may bring suit in an appropriate district court of the United States or in the United States court of any territory to require a covered consumer re-

1 porting agency to implement or correct a particular secu-  
 2 rity measure in order to promote effective security in ac-  
 3 cordance with the requirements described in clauses (ii)  
 4 and (iii) of section 3(b)(1)(B).

5 **SEC. 5. AMENDMENTS TO THE GRAMM-LEACH-BLILEY ACT.**

6 (a) ENFORCEMENT RELATING TO DISCLOSURE OF  
 7 NONPUBLIC PERSONAL INFORMATION.—Section  
 8 505(a)(7) of the Gramm-Leach-Bliley Act (15 U.S.C.  
 9 6805(a)(7)) is amended by inserting “, including any con-  
 10 sumer reporting agency that compiles and maintains files  
 11 on consumers on a nationwide basis (as defined in section  
 12 603(p) of the Fair Credit Reporting Act (15 U.S.C.  
 13 1681a(p)))” before the period at the end.

14 (b) DEFINITIONS RELATING TO DISCLOSURE OF  
 15 NONPUBLIC PERSONAL INFORMATION.—Section 509(3)  
 16 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)) is  
 17 amended by adding at the end the following:

18 “(E) CONSUMER REPORTING AGENCIES  
 19 SPECIFICALLY INCLUDED.—The term ‘financial  
 20 institution’ includes any consumer reporting  
 21 agency that compiles and maintains files on  
 22 consumers on a nationwide basis (as defined in  
 23 section 603(p) of the Fair Credit Reporting Act  
 24 (15 U.S.C. 1681a(p))).”.

1 **SEC. 6. AUTHORIZATION OF APPROPRIATIONS.**

2       There    are    authorized    to    be    appropriated  
3 \$100,000,000 to carry out this Act, to remain available  
4 until expended.

○