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.

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 Breach Prevention and Compensation Act of 2019''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFECTED CONSUMER.—The term ''affected consumer'' means any individual to whom personally identifying information pertains that was, or that may have been, affected by a covered breach.

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

(3) CAREER APPOINTEE.—The term ''career appointee'' has the meaning given the term in section 3132(a) of title 5, United States Code.

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

(5) CONSUMER REPORT; CONSUMER REPORTING AGENCY.—The terms ''consumer report'' and ''consumer reporting agency'' have the meanings given the terms in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

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

is reasonably likely to have been exposed, to an unauthorized party.

(7) COVERED CONSUMER REPORTING AGENCY.—The term ''covered consumer reporting agency'' means—

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

(B) a consumer reporting agency that earns not less than $7,000,000 in annual revenue from the sale of consumer reports.

(8) DETAIL.—The term ''detail'' means a temporary assignment of an employee to a different position for a specified period, with the employee returning to the regular duties of the employee at the end of the specified period.

(9) DIRECTOR.—The term ''Director'' means the Director of the Office.

(10) OFFICE.—The term ''Office'' means the Office of Cybersecurity established under section 3(a).

(11) PERSONALLY IDENTIFYING INFORMATION.—The term ''personally identifying information'' means, with respect to an individual—

(A) the social security number of the individual;

(B) a driver's license number of the individual;

(C) a passport number of the individual;

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

(E) unique biometric data, such as a faceprint, a fingerprint, a voice print, an iris image, or any other unique physical representation of the individual;

(F) the first and last name of the individual, or the first initial of the first name and the last name of the individual, in combination with any information that relates to—

(i) the past, present, or future physical or mental health or condition of the individual; or

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

(G)(i) a financial account number, debit card number, or credit card number of the individual; or

(ii) any passcode required to access an account described in clause (i); and

(H) such additional information, as determined by the Director.

SEC. 3. CYBERSECURITY STANDARDS AND FTC AUTHORITY.

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

(b) DUTIES.—The Office—

(1) shall—

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

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

(i) provide the Commission with descriptions of technical and organizational security measures of the consumer reporting agency, including—

(I) system and network security measures, including—

(aa) asset management, including—

(AA) an inventory of devices of the covered consumer reporting agency that are authorized to access data maintained by the covered consumer reporting agency;

(BB) an inventory of software that is authorized by the covered consumer reporting agency to access data maintained by the covered consumer reporting agency, including application whitelisting; and

(CC) secure configurations for hardware and software of the covered consumer reporting agency;

(bb) network management and monitoring, including—

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

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

(CC) network segmentation; and

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

(cc) application management, including—

(AA) continuous vulnerability assessment and remediation;

(BB) server application hardening;

(CC) vulnerability handling, such as coordinated vulnerability disclosure policy; and

(DD) patch management, including at, or near, real-time dashboards of

patch implementation across network hosts; and

(II) data security measures, including—

(aa) data-centric security mechanisms such as format-preserving encryption, cryptographic data-splitting, and data-tagging and lineage;

(bb) encryption for data at rest;

(cc) encryption for data in transit;

(dd) systemwide data minimization evaluations and policies; and

(ee) data recovery capability;

(ii) employ reasonable technical measures and corporate governance processes for continuous monitoring of data, intrusion detection, and continuous evaluation and timely patching of vulnerabilities;

(iii) employ reasonable technical measures and corporate governance processes that satisfy and exceed all relevant data se-

curity policy recommendations contained in the framework of the National Institute of Standards and Technology entitled ''Framework for Improving Critical Infrastructure Cybersecurity'', dated February 12, 2014, or any successor thereto, as determined appropriate by the Office; and

(iv) create and maintain documentation demonstrating that the covered consumer reporting agency is employing the technical measures and corporate governance processes described in clauses (ii) and (iii);

(C) annually examine the data security measures of covered consumer reporting agencies for compliance with the requirements described in clauses (ii) and (iii) of subparagraph (B);

(D) investigate any covered consumer reporting agency if the Office has reason to suspect—

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

(ii) the covered consumer reporting agency is not in compliance with the requirements described in clauses (ii) and (iii) of subparagraph (B);

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

(i) for evaluating, testing, and measuring effective data security practices of covered consumer reporting agencies; and

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

(F) submit to Congress an annual report on the findings of each investigation carried out under subparagraph (D) during the year covered by the report that includes a statement of how Congress could enhance the authorities of the Office in order to assist the Office in carrying out the duties of the Office under this Act;

(G) determine whether covered consumer reporting agencies are complying with the requirements described in clauses (ii) and (iii) of subparagraph (B); and

(H) coordinate with the National Institute of Standards and Technology and the National Cybersecurity and Communications Integration Center of the Department of Homeland Security; and

(2) may—

(A) investigate any covered breach to determine if the covered consumer reporting agency that was subject to the covered breach was in compliance with the requirements described in clauses (ii) and (iii) of paragraph (1)(B) as of the date on which the covered breach occurred; and

(B) if the Director has reason to believe that any covered consumer reporting agency is violating, or in the immediate future will violate, a requirement described in clause (ii) or (iii) of paragraph (1), bring a suit in an appropriate district court of the United States to enjoin any such act or practice.

(c) STAFF.—

(1) IN GENERAL.—The Director shall, without regard to the civil service laws and regulations, appoint such personnel, including computer security researchers and practitioners with technical expertise

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

(2) DETAILS.—

(A) IN GENERAL.—An employee of the National Institute of Standards and Technology, the Bureau of Consumer Financial Protection, or the National Cybersecurity and Communications Integration Center of the Department of Homeland Security may be detailed to the Office, without reimbursement.

(B) CIVIL SERVICE STATUS AND PRIVILEGE.—Detail under subparagraph (A) shall be without interruption or loss of the civil service status or privilege of the employee who is detailed to the Office.

SEC. 4. NOTIFICATION AND ENFORCEMENT.

(a) NOTIFICATION.—

(1) NOTIFICATION TO THE COMMISSION AND RELEVANT FEDERAL LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.—

(A) NOTIFICATION TO THE COMMISSION.—Except as provided in paragraph (3), not later than 10 days after the date on which a covered breach occurs, any covered consumer reporting

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

(B) NOTIFICATION TO RELEVANT FEDERAL LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.—Not later than 10 days after the date on which the Commission receives a notification under subparagraph (A) that a covered breach has occurred, the Commission shall—

(i) notify the relevant Federal law enforcement agencies and intelligence agencies that the covered breach has occurred; and

(ii) with respect to the covered breach, consult with the relevant Federal law enforcement agencies and intelligence agencies, as appropriate.

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

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

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

(iii) with respect to the covered breach—

(I) the number of affected consumers;

(II) the measures that the covered consumer reporting agency is taking to remedy the covered breach; and

(III) the potential risks created by the covered breach, a list of which the covered consumer reporting agency shall develop in consultation with the Office.

(3) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) NOTIFICATION BY LAW ENFORCEMENT AGENCY OR INTELLIGENCE AGENCY.—If a Federal law enforcement agency or intelligence agency to which the Commission has provided notice under paragraph (1)(B)(i) determines that the notification required under paragraph

(2) may impede a criminal investigation or national security activity—

(i) the Federal law enforcement agency or intelligence agency shall provide written notice to the Commission and the covered consumer reporting agency that was subject to the covered breach that is the subject of the notification that states—

(I) that the notification required under paragraph (2) shall be delayed for law enforcement or national security purposes; and

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

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

(B) EXTENDED DELAY OF NOTIFICATION.—If the notification required under paragraph (2) is delayed under subparagraph (A) of this paragraph, a covered consumer reporting

agency that is required to provide notice under paragraph (2) shall provide that notice on an expeditious and practical timeline, as determined appropriate by the Commission, after the date on which the law enforcement or national security delay under subparagraph (A) of this paragraph ends, unless a Federal law enforcement or intelligence agency to which the Commission has provided notice under paragraph (1)(B)(i) provides written notification to the Commission and the covered consumer reporting agency that states—

(i) that further delay is necessary; and

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

(C) LAW ENFORCEMENT IMMUNITY.—No nonconstitutional cause of action shall lie in any court against any agency for acts relating to the delay of notification under subparagraph (A), or the extended delay of notification under subparagraph (B), for law enforcement or national security purposes.

(b) PENALTY.—

(1) IN GENERAL.—In the event of a covered breach, the Commission shall, not later than 30 days after the date on which the Commission receives notification of the covered breach under subsection (a)(1)(A), commence a civil action to recover a civil penalty in an appropriate district court of the United States against the covered consumer reporting agency that was subject to the covered breach.

(2) DETERMINING PENALTY AMOUNT.—

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

(i) $100 for each consumer for whom the first and last name, or the first initial of the first name and last name, and 1 other item of personally identifying information were exposed to an unauthorized party; and

(ii) in addition to the penalty imposed under clause (i), an additional $50 for each item of personally identifying information of the consumer, other than an

item described in that clause, that was exposed to an unauthorized party.

(B) EXCEPTION.—

(i) IN GENERAL.—Except as provided in clause (ii), in an action commenced under this subsection, a court may not impose a civil penalty in an amount that is more than 50 percent of the gross revenue of the covered consumer reporting agency against which the action is brought for the fiscal year before the fiscal year in which the covered consumer reporting agency became aware of the covered breach that is the subject of the action.

(ii) PENALTY DOUBLED.—In an action commenced under this subsection, the court shall impose a civil penalty on a covered consumer reporting agency in an amount that is 2 times the amount of the penalty described in subparagraph (A), but not greater than 75 percent of the gross revenue of the covered consumer reporting agency for the fiscal year before the fiscal 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-

porting agency to implement or correct a particular security measure in order to promote effective security in accordance with the requirements described in clauses (ii) and (iii) of section 3(b)(1)(B).

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

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

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

"(E) CONSUMER REPORTING AGENCIES SPECIFICALLY INCLUDED.—The term 'financial institution' includes any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p))).".

SEC. 6. AUTHORIZATION OF APPROPRIATIONS.

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

○