115TH CONGRESS
2D SESSION

S. 2289

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

JANUARY 10, 2018

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 2018''.

SEC. 2. DEFINITIONS.

In this Act:

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

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

(3) COVERED BREACH.—The term ''covered breach'' means any instance in which at least 1 piece of personally identifying information is exposed or is reasonably likely to have been exposed to an unauthorized party.

(4) 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 sales of consumer reports.

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

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

(7) PERSONALLY IDENTIFYING INFORMATION.—The term ''personally identifying information'' means—

(A) a Social Security number;

(B) a driver's license number;

(C) a passport number;

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

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

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

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

(1) shall—

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

(B) promulgate regulations for effective data security for covered consumer reporting agencies, including regulations that require covered consumer reporting agencies to—

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

(I) system and network security measures, including—

(aa) asset management, including—

(AA) an inventory of authorized and unauthorized devices;

(BB) an inventory of authorized and unauthorized software, including application whitelisting; and

(CC) secure configurations for hardware and software;

(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, 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; and

(ii) create and maintain documentation demonstrating that the covered consumer reporting agency is employing reasonable technical measures and corporate governance processes for continuous monitoring of data, intrusion detection, and continuous evaluation and timely patching of vulnerabilities;

(C) annually examine the data security measures of covered consumer reporting agencies for compliance with the standards promulgated under subparagraph (B);

(D) investigate any covered consumer reporting agency if the Office has reason to suspect a potential covered breach or noncompliance with the standards promulgated under subparagraph (B);

(E) after consultation with members of the technical and academic communities, develop a rigorous, repeatable methodology for evaluating, testing, and measuring effective data security practices of covered consumer reporting agencies, that employs forms of static and dynamic software analysis and penetration testing;

(F) submit to Congress an annual report on the findings on any investigation under subparagraph (C);

(G) determine whether covered consumer reporting agencies are complying with the regulations promulgated under 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 breach to determine if the covered consumer reporting agency was in compliance with the regulations promulgated under paragraph (1)(B); and

(B) if the Commission has reason to believe that any covered consumer reporting agency is violating, or is about to violate, a regulation promulgated under paragraph (1)(B), bring a suit in a 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.—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, and such detail shall be without interruption or loss of civil service status or privilege.

SEC. 4. NOTIFICATION AND ENFORCEMENT.

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

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

(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, commence a civil action to recover a civil penalty in a 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 whose first and last name, or first initial and last name, and at least 1 item of personally identifying information was compromised; and

(ii) an additional $50 for each additional item of personally identifying information compromised for each consumer.

(B) EXCEPTION.—

(i) IN GENERAL.—Except as provided in clause (ii), a court may not impose a civil penalty under this subsection in an amount greater than 50 percent of the gross revenue of the covered consumer reporting agency for the previous fiscal year before the date on which the covered consumer reporting agency became aware of the covered breach.

(ii) PENALTY DOUBLED.—A court shall impose a civil penalty on a covered consumer reporting agency double the penalty described in subparagraph (A), but not greater than 75 percent of the gross revenue of the covered consumer reporting agency for the previous fiscal year before the date on which the covered consumer reporting agency became aware of the covered breach if—

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

(II) the covered consumer reporting agency violates any regulation promulgated under section 3(b)(1)(C).

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

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

(B) 50 percent shall be used by the Commission 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 may bring suit in a district court of the United States or in the United States court of any Territory to enjoin a covered consumer reporting agency to implement or correct a particular security measure in order to promote effective security.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

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

○