I

115TH CONGRESS
1ST SESSION

H. R. 135

To protect cyber privacy, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 3, 2017

Mr. CONYERS (for himself and Mr. JOHNSON of Georgia) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To protect cyber privacy, 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 ''Cyber Privacy Fortification Act of 2017''.

TITLE I—DATA BREACH NOTIFICATION

SEC. 101. FAILURE TO PROVIDE NOTICE OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1041. Failure to provide notice of security breaches involving sensitive personally identifiable information

''(a) Whoever, having a covered obligation to provide notice of a security breach involving sensitive personally identifiable information, knowingly fails to do so, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) As used in this section—

''(1) the term 'covered obligation', with respect to providing notice of a security breach, means an obligation under Federal law or, if the breach is in or affects interstate or foreign commerce, under State law;

''(2) the term 'sensitive personally identifiable information' means any electronic or digital information that includes—

''(A) an individual's first and last name, or first initial and last name, or address or phone number in combination with any one of the following data elements where the data elements are not protected by a technology protection measure that renders the data element indecipherable—

''(i) a nontruncated social security number, driver's license number, state resident identification number, passport number, or alien registration number;

''(ii) both—

''(I) mother's maiden name, if identified as such; and

''(II) month, day, and year of birth; and

''(iii) unique biometric data such as a fingerprint, voice print, a retina or iris image; or

''(B) a financial account number or credit or debit card number in combination with any security code, access code or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction by means of such number;

''(3) the term 'security breach' means a compromise of the security, confidentiality, or integrity of computerized data that there is reason to believe has resulted in improper access to sensitive personally identifiable information; and

''(4) the term 'improper access' means access without authorization or in excess of authorization.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of security breaches involving personally identifiable information.''.

(c) OBLIGATION TO REPORT.—

(1) IN GENERAL.—A person who owns or possesses data in electronic form containing a means of identification and has knowledge of a major security breach of the system containing such data maintained by such person, must provide prompt notice of such breach to the United States Secret Service or Federal Bureau of Investigation.

(2) PUBLICATION OF LIST OF NOTIFICATIONS.—The Secret Service and the Federal Bureau of Investigation shall annually publish in the Federal Register a list of all notifications submitted the previous calendar year and the identity of each entity

with respect to which the major security breach occurred.

(3) DEFINITION.—In this subsection—

(A) the term ''major security breach'' means any security breach involving—

(i) means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired;

(ii) databases owned by the Federal Government; or

(iii) means of identification of Federal Government employees or contractors involved in national security matters or law enforcement; and

(B) the term ''means of identification'' has the meaning given that term in section 1028 of title 18, United States Code.

TITLE II—NON-CRIMINAL PRIVACY ENFORCEMENT AND PRIVACY IMPACT STATEMENTS

SEC. 201. ENFORCEMENT BY ATTORNEY GENERAL AND STATE AUTHORITIES.

(a) DEFINITION OF ''AUTHORIZED ENTITY''.—As used in this section, the term ''authorized entity'' means

the Attorney General, with respect to any conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security and engaged in by a business entity, and a State Attorney General with respect to that conduct to the extent the conduct adversely affects an interest of the residents of a State.

(b) CIVIL PENALTY.—

(1) GENERALLY.—An authorized entity may in a civil action obtain a civil penalty of not more than $500,000 from any business entity that engages in conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security.

(2) SPECIAL RULE FOR INTENTIONAL VIOLATION.—If the violation described in subsection (a) is intentional, the maximum civil penalty is $1,000,000.

(c) INJUNCTIVE RELIEF.—An authorized entity may, in a civil action against a business entity that has engaged, or is engaged, in any conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security, obtain an order—

(1) enjoining such act or practice; or

(2) enforcing compliance with that law.

(d) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section do not affect any other rights and remedies available under Federal or State law.

SEC. 202. COORDINATION OF STATE AND FEDERAL EFFORTS.

(a) NOTICE.—

(1) IN GENERAL.—A State consumer protection attorney may not bring an action under section 201, until the attorney general of the State involved provides to the Attorney General of the United States—

(A) written notice of the action; and

(B) a copy of the complaint for the action.

(2) EXCEPTION.—Paragraph (1) does not apply with respect to the filing of an action by an attorney general of a State under this section if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action, in such a case the State attorney general shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—The Attorney General may—

(1) move to stay any non-Federal action under section 201, pending the final disposition of a pending Federal action under that section;

(2) initiate an action in an appropriate United States district court and move to consolidate all pending actions under section 201, including State actions, in that court; and

(3) intervene in a State action under section 201.

(c) PENDING PROCEEDINGS.—If the Attorney General institutes a proceeding or action for a violation of a Federal law enacted after the date of the enactment of this Act relating to data security, no authority of a State may, during the pendency of such proceeding or action, bring an action under this section against any defendant named in such criminal proceeding or a civil action against any defendant for any violation that is alleged in that proceeding or action.

(d) DEFINITION.—As used in this section, the term ''State consumer protection attorney'' means the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law.

SEC. 203. REQUIREMENT THAT AGENCY RULEMAKING TAKE INTO CONSIDERATION IMPACTS ON INDIVIDUAL PRIVACY.

(a) IN GENERAL.—Title 5, United States Code, is amended by adding after section 553 the following new section:

"§ 553a. Privacy impact assessment in rulemaking

''(a) INITIAL PRIVACY IMPACT ASSESSMENT.—

''(1) IN GENERAL.—Whenever an agency is required by section 553 of this title, or any other law, to publish a general notice of proposed rulemaking for a proposed rule, or publishes a notice of proposed rulemaking for an interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government, the agency shall prepare and make available for public comment an initial privacy impact assessment that describes the impact of the proposed rule on the privacy of individuals. Such assessment or a summary thereof shall be signed by the senior agency official with primary responsibility for privacy policy and be published in the Federal Register at the time of the

publication of a general notice of proposed rulemaking for the rule.

''(2) CONTENTS.—Each initial privacy impact assessment required under this subsection shall contain the following:

''(A) A description and analysis of the extent to which the proposed rule will impact the privacy interests of individuals, including the extent to which the proposed rule—

''(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

''(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

''(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

''(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of

the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

''(B) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant privacy impact of the proposed rule on individuals.

''(b) FINAL PRIVACY IMPACT ASSESSMENT.—

''(1) IN GENERAL.—Whenever an agency promulgates a final rule under section 553 of this title, after being required by that section or any other law to publish a general notice of proposed rulemaking, or promulgates a final interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government, the agency shall prepare a final privacy impact assessment, signed by the senior agency official with primary responsibility for privacy policy.

''(2) CONTENTS.—Each final privacy impact assessment required under this subsection shall contain the following:

''(A) A description and analysis of the extent to which the final rule will impact the privacy interests of individuals, including the extent to which such rule—

''(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

''(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

''(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

''(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthor-

ized release of personally identifiable information as a result of a breach of security at or by the agency.

''(B) A summary of any significant issues raised by the public comments in response to the initial privacy impact assessment, a summary of the analysis of the agency of such issues, and a statement of any changes made in such rule as a result of such issues.

''(C) A description of the steps the agency has taken to minimize the significant privacy impact on individuals consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the privacy interests of individuals was rejected.

''(3) AVAILABILITY TO PUBLIC.—The agency shall make copies of the final privacy impact assessment available to members of the public and shall publish in the Federal Register such assessment or a summary thereof.

''(c) WAIVERS.—

''(1) EMERGENCIES.—An agency head may waive or delay the completion of some or all of the requirements of subsections (a) and (b) to the same extent as the agency head may, under section 608, waive or delay the completion of some or all of the requirements of sections 603 and 604, respectively.

''(2) NATIONAL SECURITY.—An agency head may, for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort, waive or delay the completion of some or all of the following requirements:

''(A) The requirement of subsection (a)(1) to make an assessment available for public comment, provided that such assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public.

''(B) The requirement of subsection (a)(1) to have an assessment or summary thereof published in the Federal Register, provided that such assessment or summary is made available, in classified form, to the Committees on the Ju-

diciary of the House of Representatives and the Senate, in lieu of publishing such assessment or summary in the Federal Register.

''(C) The requirements of subsection (b)(3), provided that the final privacy impact assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public and publishing such assessment in the Federal Register.

''(d) PROCEDURES FOR GATHERING COMMENTS.—When any rule is promulgated which may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals, the head of the agency promulgating the rule or the official of the agency with statutory responsibility for the promulgation of the rule shall assure that individuals have been given an opportunity to participate in the rulemaking for the rule through techniques such as—

''(1) the inclusion in an advance notice of proposed rulemaking, if issued, of a statement that the proposed rule may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals;

''(2) the publication of a general notice of proposed rulemaking in publications of national circulation likely to be obtained by individuals;

''(3) the direct notification of interested individuals;

''(4) the conduct of open conferences or public hearings concerning the rule for individuals, including soliciting and receiving comments over computer networks; and

''(5) the adoption or modification of agency procedural rules to reduce the cost or complexity of participation in the rulemaking by individuals.

''(e) PERIODIC REVIEW OF RULES.—

''(1) IN GENERAL.—Each agency shall carry out a periodic review of the rules promulgated by the agency that have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals. Under such periodic review, the agency shall determine, for each such rule, whether the rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes. For each such determination, the agency shall consider the following factors:

''(A) The continued need for the rule.

''(B) The nature of complaints or comments received from the public concerning the rule.

''(C) The complexity of the rule.

''(D) The extent to which the rule overlaps, duplicates, or conflicts with other Federal rules, and, to the extent feasible, with State and local governmental rules.

''(E) The length of time since the rule was last reviewed under this subsection.

''(F) The degree to which technology, economic conditions, or other factors have changed in the area affected by the rule since the rule was last reviewed under this subsection.

''(2) PLAN REQUIRED.—Each agency shall carry out the periodic review required by paragraph (1) in accordance with a plan published by such agency in the Federal Register. Each such plan shall provide for the review under this subsection of each rule promulgated by the agency not later than 10 years after the date on which such rule was published as the final rule and, thereafter, not later than 10 years after the date on which such rule was last reviewed under this subsection. The agency may

amend such plan at any time by publishing the revision in the Federal Register.

''(3) ANNUAL PUBLICATION.—Each year, each agency shall publish in the Federal Register a list of the rules to be reviewed by such agency under this subsection during the following year. The list shall include a brief description of each such rule and the need for and legal basis of such rule and shall invite public comment upon the determination to be made under this subsection with respect to such rule.

''(f) JUDICIAL REVIEW.—

''(1) IN GENERAL.—For any rule subject to this section, an individual who is adversely affected or aggrieved by final agency action is entitled to judicial review of agency compliance with the requirements of subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

''(2) JURISDICTION.—Each court having jurisdiction to review such rule for compliance with section 553, or under any other provision of law, shall have jurisdiction to review any claims of noncompliance with subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d)

shall be judicially reviewable in connection with judicial review of subsection (b).

''(3) LIMITATIONS.—

''(A) An individual may seek such review during the period beginning on the date of final agency action and ending 1 year later, except that where a provision of law requires that an action challenging a final agency action be commenced before the expiration of 1 year, such lesser period shall apply to an action for judicial review under this subsection.

''(B) In the case where an agency delays the issuance of a final privacy impact assessment pursuant to subsection (c), an action for judicial review under this section shall be filed not later than—

''(i) 1 year after the date the assessment is made available to the public; or

''(ii) where a provision of law requires that an action challenging a final agency regulation be commenced before the expiration of the 1-year period, the number of days specified in such provision of law that is after the date the assessment is made available to the public.

''(4) RELIEF.—In granting any relief in an action under this subsection, the court shall order the agency to take corrective action consistent with this section and chapter 7, and may—

''(A) remand the rule to the agency; and

''(B) defer the enforcement of the rule against individuals, unless the court finds that continued enforcement of the rule is in the public interest.

''(5) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of any court to stay the effective date of any rule or provision thereof under any other provision of law or to grant any other relief in addition to the requirements of this subsection.

''(6) RECORD OF AGENCY ACTION.—In an action for the judicial review of a rule, the privacy impact assessment for such rule, including an assessment prepared or corrected pursuant to paragraph (4), shall constitute part of the entire record of agency action in connection with such review.

''(7) EXCLUSIVITY.—Compliance or noncompliance by an agency with the provisions of this section shall be subject to judicial review only in accordance with this subsection.

''(8) SAVINGS CLAUSE.—Nothing in this subsection bars judicial review of any other impact statement or similar assessment required by any other law if judicial review of such statement or assessment is otherwise permitted by law.

''(g) DEFINITION.—For purposes of this section, the term 'personally identifiable information' means information that can be used to identify an individual, including such individual's name, address, telephone number, photograph, social security number or other identifying information. It includes information about such individual's medical or financial condition.''.

(b) PERIODIC REVIEW TRANSITION PROVISIONS.—

(1) INITIAL PLAN.—For each agency, the plan required by subsection (e) of section 553a of title 5, United States Code (as added by subsection (a)), shall be published not later than 180 days after the date of the enactment of this Act.

(2) REVIEW PERIOD.—In the case of a rule promulgated by an agency before the date of the enactment of this Act, such plan shall provide for the periodic review of such rule before the expiration of the 10-year period beginning on the date of the enactment of this Act. For any such rule, the head of the agency may provide for a 1-year extension of

such period if the head of the agency, before the expiration of the period, certifies in a statement published in the Federal Register that reviewing such rule before the expiration of the period is not feasible. The head of the agency may provide for additional 1-year extensions of the period pursuant to the preceding sentence, but in no event may the period exceed 15 years.

(c) CONGRESSIONAL REVIEW.—Section 801(a)(1)(B) of title 5, United States Code, is amended—

(1) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively; and

(2) by inserting after clause (ii) the following new clause:

''(iii) the agency's actions relevant to section 553a;''.

(d) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 5 of title 5, United States Code, is amended by adding after the item relating to section 553 the following new item:

''553a. Privacy impact assessment in rulemaking.''.

○