

S.1535, The Personal Data Protection and Breach Accountability Act of 2011

Sec. 1. Short Title; Table of Contents. This section provides that the legislation may be cited as the “Personal Data Protection and Breach Accountability Act of 2011.”

Sec. 2. Findings. Section 2 provides Congressional findings on the threats to consumers posed by data breaches.

Sec. 3. Definitions. Section 3 contains the definitions used in the bill.

TITLE I: ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

Sec. 101. Concealment of Security Breaches Involving Sensitive Personally Identifiable Information. Amends title 18 to allow for the prosecution of a person who intentionally and willfully conceals the fact of a security breach of sensitive personally identifiable information that must be reported to individuals under this Act. Punishment may include a fine and up to 5 years in prison.

Sec. 102. Unauthorized Manipulation of Internet Traffic on a User’s Computer. Establishes civil penalties for knowingly and intentionally redirecting web searches or monitoring, manipulating, aggregating, or marketing data collected from search results without the user’s consent.

TITLE II: PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A: A Data Privacy and Security Program

Sec. 201. Purpose and Applicability of Data Privacy and Security Program. Requires covered entities to create a data privacy and security program to deter and avoid preventable breaches of sensitive personally identifiable information A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons. Exempts from such requirements public records, certain financial institutions subject to and compliant with the Gramm-Leach-Bliley Act, covered entities subject

to the data security requirements of the Health Insurance Portability and Accountability Act (HIPAA), and service providers exclusively engaged in the transmission of data.

Sec 202. Requirements for a Personal Data Privacy and Security Program. Requires a business entity that is subject to data privacy and security requirements to implement a comprehensive personal data privacy and security program that (i) ensures the privacy, security, and confidentiality of sensitive personally identifying information; (ii) protects against anticipated vulnerabilities to the privacy, security, or integrity of such information; and (iii) protects against unauthorized access to such information that could create a significant risk of harm or fraud. Compliance required within one year of enactment.

- Requires covered entities to assess risks of future breaches and design a security program to mitigate those risks. Such programs must include efforts to track access to personal information, ensure it is only accessed for a valid legal reason, and minimize the amount of unnecessary personal information retained.
- Ensures employee training and supervision for implementation of data security programs.
- Requires regular vulnerability testing of key controls, systems, and procedures of each security program to detect, prevent, and respond to attacks.
- Requires regular updating of each security program to respond to new developments.

Sec. 203. Federal Enforcement. Imposes civil penalties of \$5,000 per violation per day while a violation exists, up to \$20 million, on business entities that violate the data privacy and security requirements of this subtitle. Allows for additional penalties of \$5,000 per violation per day for intentional or willful violations. Allows DOJ to seek injunctions to prevent practices or to compel compliance with the data privacy and security requirements.

Sec. 204. Enforcement by State Attorneys General. Allows state Attorneys General or authorized state agencies to pursue civil penalties of \$5,000 per violation per day while a violation exists, up to \$20 million, against business entities that violate the data privacy and security requirements of this subtitle and whose violations harm or threaten to harm state residents.

Sec. 205. Supplemental Enforcement by Individuals. Allows individual consumers harmed by the failure of a business entity to comply with the data privacy and security requirements of this subtitle to bring a civil action seeking \$10,000 per violation per day while such a violation exists, up to \$20 million, and injunctive relief.

Subtitle B: Security Breach Notification

Sec. 211. Notice to Individuals. Requires any agency or business entity engaged in interstate commerce that uses, accesses, transmits, stores disposes of or collects sensitive personally

identifiable information to notify any U.S. resident of a security breach in which such resident's information has been, or is reasonably believed to have been, accessed or acquired, without unreasonable delay.

- Any agency business entity agency that does not own or license information compromised in a security breach must notify the owner or licensee of the data, and the owner or licensee must provide required notice to individuals, subject to any agreements between owners, licensees, and third parties regarding assignment of the notification requirements of this subtitle.
- Allows a federal law enforcement or intelligence agency to delay notification under this subtitle if it determines such notification would impede a criminal investigation or authorized intelligence activity. This time can be extended if the agency provides the company with written notification.

Sec. 212. Exemptions from Notice to Individuals.

- Exempts agencies or business entities from security breach notification requirements if the Secret Service and the FBI notifies the agency or business entity that providing such notification would impede a criminal investigation or damage national security. Agencies or business entities will be exempt from the security breach notification requirements if they conduct a risk assessment in consultation with the FTC and conclude that no significant risk of harm exists to any individual and the FTC does not express disapproval of the risk assessment.
 - Creates a rebuttable presumption of no significant risk if the agency or business entity has rendered the information indecipherable through best practices as described by the FTC and National Institute of Standards and Technology.
 - Alternatively creates a presumption of significant risk if the agency or business entity failed to render the information indecipherable through the best practices as described by the FTC and NIST.
- Creates a narrow financial fraud prevention exemption if a business entity has a program to block the fraudulent use of information to initiate unauthorized transactions that includes notice to consumers, but only where the breach involves only a credit card number or security code.
- Creates a narrow exemption for a business entity subject to HIPAA/HITECH/ARRA, but only where the breach involves only health information.

Sec. 213. Methods of Notice to Individuals. Requires an agency or business entity to give notice under this subtitle by: (1) written notice to the last known home mailing address or e-mail notice to individuals whose sensitive personally identifiable information was subject of the security breach; (2) telephone notice to each individual personally; (3) notice to the public via all reasonable means of electronic contact between the individual and the business entity when the number of affected individuals is believed to exceed 5,000; and (4) notice to major media outlets

serving states or jurisdictions where the affected individuals within that state or jurisdiction is believed to include more than 5,000 residents.

Section 214. Content of Notice to Individuals. Establishes requirements for the content of written or email notification to individuals, telephone notice, and public (electronic and mass media) notice, including notice regarding the remedies provided under Section 215. Preserves the rights of states to require notification of additional victim protection assistance provided by those states.

Sec. 215. Remedies for Security Breach. Requires an agency or business entity, following a breach, to provide (at no cost to victims) the following upon request by individuals whose sensitive personally identifiable information was, or is reasonably believed to be, subject to the breach:

- Credit monitoring or consumer credit reports for up to two years after the security breach;
- A security freeze requirement that prohibits any credit reporting agency from releasing all or any part of a victim's credit report or any information derived from it without the express authorization of the consumer; and
- Compensation in the form of (i) insurance; or (ii) compensation without unreasonable delay for any actual costs or damages incurred by an individual as a result of the security breach.

Sec. 216. Notice to Credit Reporting Agencies. Requires any agency or business entity required to notify more than 5,000 consumers of a security breach under this subtitle to also notify consumer credit reporting agencies without unreasonable delay.

Sec. 217. Notice to Law Enforcement. Requires business entities and agencies to notify a designated entity of particularly significant security breaches within 10 days of the discovery of a breach, and allows the FTC to adjust the threshold requirements for providing notice to law enforcement. Requires the Secret Service and the FBI to notify other governmental entities as appropriate.

Sec. 218. Federal Enforcement. Authorizes the Attorney General to bring a civil action, including an injunction, in federal court for violations of the requirements of this subtitle by a business entity. Allows the FTC to enforce violations of this subtitle in conjunction with the Attorney General. Civil penalties may not exceed \$500 per day per individual whose sensitive personally identifiable information was or is reasonably believed to have subject to the breach, and are capped at \$20 million per violation, unless the violation was willful or intentional.

Sec. 219. Enforcement by State Attorneys General. Allows state Attorneys General or authorized state agencies to pursue equitable relief as well as civil penalties of \$500 per day per individual whose sensitive personally identifiable information was or is reasonably believed to

have subject to the breach, capped at \$20 million per violation unless the violation was willful or intentional.

Sec. 220. Supplemental Enforcement by Individuals. Allows individual consumers harmed by the failure of a business entity to comply with this subtitle to seek damages up to \$500 per day per individual whose sensitive personally identifiable information was or is reasonably believed to have subject to the breach, capped at \$20 million per violation. Consumers may also seek equitable relief and punitive damages for willful and intentional violations.

Sec. 221. Relation to Other Laws. Supersedes other provisions of state or federal law relating to notification, but does not exempt any entity from liability under common law arising from a failure to notify.

Sec. 222. Authorization of Appropriations. Authorizes appropriations to the Secret Service to carry out investigations and risk assessments of security breaches.

Sec. 223. Reporting on Risk Assessment Exemptions. Requires the Secret Service to report to Congress on the number and nature of security breaches described in notices filed by businesses invoking risk assessment and law enforcement exemptions within 18 months of the enactment of this Act.

Subtitle C: Post-Breach Technical Information Clearinghouse

Sec. 230. Clearinghouse Information Collection, Maintenance, and Access. Directs the designated entity to maintain a clearinghouse of technical information concerning system vulnerabilities identified in the wake of security breaches reported to the designated entity. Allows certified entities to review the information in the clearinghouse to help defend against future breaches. Certification can only be granted if a company agrees to use such information only to improve network security and not for any commercial purpose, and agrees not to share such information with any third party without express written consent from the designated entity.

Sec. 231. Protections for Clearinghouse Participants. Directs the designated entity to protect proprietary business information from inadvertent disclosure, to render the source company of such data anonymous, to limit liability for any company as a sole consequence of reporting technical information to the clearinghouse, and to protect such information from public disclosure.

Sec. 232. Effective Date. Establishes an effective date for the provisions of this subtitle at 90 days from the date of enactment.

TITLE III: ACCESS TO AND USE OF COMMERCIAL DATA

Sec. 301. General Services Administration Review of Contracts. Requires the Administrator of the General Services Administration (GSA), in awarding contracts totaling more than \$500,000 to data brokers, to evaluate whether they are compliant with the requirements of this Act. Requires the GSA to impose monetary penalties on brokers for violations of the Act or for providing inaccurate sensitive personally identifiable information, and imposes other requirements on data brokers to protect sensitive personally identifiable information from security breaches.

Sec. 302. Requirement to Audit Information Security Practices of Contractors and Third Party Business Entities. Requires federal agencies to audit and evaluate the information security practices of government contractors and third parties that support the information technology systems of such agencies.

Sec. 303. Privacy Impact Assessment of Government Use of Commercial Information Services Containing Sensitive Personally Identifiable Information. Requires federal agencies that purchase or subscribe to sensitive personally identifiable information from a commercial entity to conduct privacy impact assessments on the use of those services. Requires the Comptroller General to conduct a study and audit and prepare a report for submission to Congress on federal agency adherence to privacy principles in using data brokers or commercial databases containing sensitive personally identifiable information.

Sec. 304. FBI Report on Reported Breaches and Compliance. Requires the FBI, in coordination with the Secret Service, to report to Congress regarding breaches at agencies and business entities during the preceding year.

Sec. 305. Department Of Justice Report on Enforcement Actions. Requires the Attorney General to report to Congress regarding federal, state, and private enforcement of this Act, and any recommendations for increasing the effectiveness of this act..

Sec. 306. Report on Notification Effectiveness. Requires the FBI, in coordination with the Attorney General and the FTC, to report to Congress regarding the effectiveness of post-breach notification practices by agencies and business entities.

TITLE IV: COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

Sec. 401. Budget Compliance. Provides language to comply with the Statutory Pay-As-You-Go Act of 2010.