[DISCUSSION DRAFT]

116TH CONGRESS
1ST SESSION

H. R. _____

To amend the Gramm-Leach-Bliley Act to provide for financial data protection requirements for non-financial institutions, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Gramm-Leach-Bliley Act to provide for financial data protection requirements for non-financial institutions, 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 ''Financial Information Data Modernization Act''.

SEC. 2. PROTECTION OF CONSUMER FINANCIAL DATA.

(a) IN GENERAL.—Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) is amended by adding at the end the following:

"Subtitle C—Protection of Consumer Financial Data

"SEC. 531. FINANCIAL DATA PROTECTION REQUIREMENTS.

''(a) IN GENERAL.—Any non-financial institution shall keep financial data secure by establishing, implementing, and maintaining reasonable data security practices to protect the confidentiality, integrity, and availability of financial data consistent with industry best practices for safety and security, including administrative, technical, and physical safeguards.

''(b) MINIMUM REQUIREMENTS.—The data security practices required under subsection (a) shall include, at a minimum—

''(1) using encryption standards for data at rest;

''(2) using transport security controls for data in transit;

''(3) using encryption for data in use;

''(4) tokenizing all information related to account information;

''(5) ensuring any cloud storage of financial data has advanced protections, and configurations;

''(6) maintaining an internal guide that designates and defines data based on the risk if the data were to ever be public;

''(7) requiring the chief information security officer (or the equivalent in responsibilities) to report at least every 6 months to the institution's board of directors on issues related to the information security program;

''(8) developing procedures for the secure disposal of customer information in any format that is no longer necessary for the institution's business operations or other legitimate business purposes;

''(9) providing information security personnel and other relevant staff as necessary with security training and certifications sufficient to address relevant security risks;

''(10) developing a process for taking action designed to mitigate against vulnerabilities and for internal and public response in the event of a breach or incident of data abuse; and

''(11) conducting regular assessments of—

''(A) access controls;

''(B) vulnerability assessments;

''(C) data incident response plans; and

''(D) data designations, definitions, and retention of data.

''(c) EXCEPTION.—Subsection (a) shall not apply to a non-financial institution if the Director of the Bureau of Consumer Financial Protection determines that financial data protection requirements applicable to such non-financial institution under Federal law other than this subtitle provide greater protections to consumers than the requirements under subsection (a).

''SEC. 532. CIVIL PENALTY.

''(a) CIVIL FINE.—A person who violates any provision of this subtitle shall be fined in amount equal to—

''(1) for the first violation, 1 percent of the most recent quarterly gross revenue of the person;

''(2) for the second violation, 2 percent of such revenue; and

''(3) for the third violation and any subsequent violation, 3 percent of such revenue.

''(b) LIABILITY TO HARMED INDIVIDUALS.—A person who violates any provision of this subtitle with respect to the financial data of an individual shall be liable to such individual in an amount equal to the sum of—

''(1) any actual damage sustained by such individual by reason of such violation; and

''(2) reasonable punitive damages, as determined by a court of competent jurisdiction.

"SEC. 533. DEFINITIONS.

''In this subtitle:

''(1) FINANCIAL DATA.—The term 'financial data' means personal information associated with money or digital representations of value, including personal information and aggregated data that is associated with transactional information, the ability to repay, cash flow analysis, payment information, and credit and debit card and savings information.

''(2) FINANCIAL INSTITUTION.—The term 'financial institution' has the meaning given under section 509.

''(3) NON-FINANCIAL INSTITUTION.—

''(A) IN GENERAL.—The term 'non-financial institution' means an institution—

''(i) that is not a financial institution;

''(ii) significantly engaged in using online financial data for core business purposes; and

''(iii) that derives more than 50 percent of the institution's total revenue from online financial data or financial data combined with online data.

''(B) EXCEPTION FOR SMALLER INSTITUTIONS.—The term 'non-financial institution' does not include an institution that grosses less than $5,000,000 in annual revenue, as reported to the Bureau of Consumer Financial Protection.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Gramm-Leach-Bliley Act is amended by inserting after the item relating to section 527 the following:

''Subtitle C—Protection of Consumer Financial Data

''Sec. 531. Financial data protection requirements.
''Sec. 532. Civil penalty.
''Sec. 533. Definitions.''.

(c) RULEMAKING.—The Director of the Consumer Financial Protection Bureau, in consultation with the Secretary of Homeland Security, the Chairman of the Federal Trade Commission, the Director of the National Institute of Standards and Technology, the Secretary of the Treasury, the Comptroller of the Currency, the Chairperson of the Federal Deposit Insurance Corporation, the Chairman of the National Credit Union Administration Board, State attorneys general, and public interest group, shall issue rules to carry out the requirements of this Act.