

[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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Financial Information
5 Data Modernization Act”.

1 **SEC. 2. PROTECTION OF CONSUMER FINANCIAL DATA.**

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

4
5 **“Subtitle C—Protection of**
6 **Consumer Financial Data**

7 **“SEC. 531. FINANCIAL DATA PROTECTION REQUIREMENTS.**

8 “(a) IN GENERAL.—Any non-financial institution
9 shall keep financial data secure by establishing, imple-
10 menting, and maintaining reasonable data security prac-
11 tices to protect the confidentiality, integrity, and avail-
12 ability of financial data consistent with industry best prac-
13 tices for safety and security, including administrative,
14 technical, and physical safeguards.

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

18 “(1) using encryption standards for data at
19 rest;

20 “(2) using transport security controls for data
21 in transit;

22 “(3) using encryption for data in use;

23 “(4) tokenizing all information related to ac-
24 count information;

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

1 “(6) maintaining an internal guide that des-
2 ignates and defines data based on the risk if the
3 data were to ever be public;

4 “(7) requiring the chief information security of-
5 ficer (or the equivalent in responsibilities) to report
6 at least every 6 months to the institution’s board of
7 directors on issues related to the information secu-
8 rity program;

9 “(8) developing procedures for the secure dis-
10 posal of customer information in any format that is
11 no longer necessary for the institution’s business op-
12 erations or other legitimate business purposes;

13 “(9) providing information security personnel
14 and other relevant staff as necessary with security
15 training and certifications sufficient to address rel-
16 evant security risks;

17 “(10) developing a process for taking action de-
18 signed to mitigate against vulnerabilities and for in-
19 ternal and public response in the event of a breach
20 or incident of data abuse; and

21 “(11) conducting regular assessments of—

22 “(A) access controls;

23 “(B) vulnerability assessments;

24 “(C) data incident response plans; and

1 “(D) data designations, definitions, and re-
2 tention of data.

3 “(c) EXCEPTION.—Subsection (a) shall not apply to
4 a non-financial institution if the Director of the Bureau
5 of Consumer Financial Protection determines that finan-
6 cial data protection requirements applicable to such non-
7 financial institution under Federal law other than this
8 subtitle provide greater protections to consumers than the
9 requirements under subsection (a).

10 **“SEC. 532. CIVIL PENALTY.**

11 “(a) CIVIL FINE.—A person who violates any provi-
12 sion of this subtitle shall be fined in amount equal to—

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

15 “(2) for the second violation, 2 percent of such
16 revenue; and

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

19 “(b) LIABILITY TO HARMED INDIVIDUALS.—A per-
20 son who violates any provision of this subtitle with respect
21 to the financial data of an individual shall be liable to such
22 individual in an amount equal to the sum of—

23 “(1) any actual damage sustained by such indi-
24 vidual by reason of such violation; and

1 “(2) reasonable punitive damages, as deter-
2 mined by a court of competent jurisdiction.

3 **“SEC. 533. DEFINITIONS.**

4 “In this subtitle:

5 “(1) FINANCIAL DATA.—The term ‘financial
6 data’ means personal information associated with
7 money or digital representations of value, including
8 personal information and aggregated data that is as-
9 sociated with transactional information, the ability
10 to repay, cash flow analysis, payment information,
11 and credit and debit card and savings information.

12 “(2) FINANCIAL INSTITUTION.—The term ‘fi-
13 nancial institution’ has the meaning given under sec-
14 tion 509.

15 “(3) NON-FINANCIAL INSTITUTION.—

16 “(A) IN GENERAL.—The term ‘non-finan-
17 cial institution’ means an institution—

18 “(i) that is not a financial institution;

19 “(ii) significantly engaged in using
20 online financial data for core business pur-
21 poses; and

22 “(iii) that derives more than 50 per-
23 cent of the institution’s total revenue from
24 online financial data or financial data com-
25 bined with online data.

1 “(B) EXCEPTION FOR SMALLER INSTITU-
2 TIONS.—The term ‘non-financial institution’
3 does not include an institution that grosses less
4 than \$5,000,000 in annual revenue, as reported
5 to the Bureau of Consumer Financial Protec-
6 tion.”.

7 (b) CLERICAL AMENDMENT.—The table of contents
8 of the Gramm-Leach-Bliley Act is amended by inserting
9 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.”.

10 (c) RULEMAKING.—The Director of the Consumer
11 Financial Protection Bureau, in consultation with the Sec-
12 retary of Homeland Security, the Chairman of the Federal
13 Trade Commission, the Director of the National Institute
14 of Standards and Technology, the Secretary of the Treas-
15 ury, the Comptroller of the Currency, the Chairperson of
16 the Federal Deposit Insurance Corporation, the Chairman
17 of the National Credit Union Administration Board, State
18 attorneys general, and public interest group, shall issue
19 rules to carry out the requirements of this Act.