

[DISCUSSION DRAFT]

118TH CONGRESS
1ST SESSION

H. R. _____

To amend the Gramm-Leach-Bliley Act to **[modernize the protection of the nonpublic personal information of consumers]**, 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 **[modernize the protection of the nonpublic personal information of consumers]**, 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; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 **“[To be added Act of 2023]”**.

6 (b) **TABLE OF CONTENTS.**—The table of contents for
7 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Protection of nonpublic personal information.

- Sec. 3. Obligations with respect to the collection and disclosure of nonpublic personal information.
- Sec. 4. Disclosure of institution privacy policy.
- Sec. 5. Rulemaking.
- Sec. 6. Enforcement.
- Sec. 7. Relation to State laws.
- Sec. 8. Definitions.
- Sec. 9. Obligations with respect to access and deletion of nonpublic personal information.
- Sec. 10. Obligations with respect to the international sharing of nonpublic personal information.
- Sec. 11. Repeal of expired provisions.
- Sec. 12. Sense of Congress.

1 **SEC. 2. PROTECTION OF NONPUBLIC PERSONAL INFORMA-**
2 **TION.**

3 Section 501 of the Gramm-Leach-Bliley Act (15
4 U.S.C. 6801) is amended—

5 (1) in subsection (a)—

6 (A) by inserting “and other consumers”
7 after “its customers”; and

8 (B) by striking “those customers’ non-
9 public personal information” and inserting
10 “nonpublic personal information relating to
11 those customers and consumers”; and

12 (2) in subsection (b)—

13 (A) by striking “section 505(a), other than
14 the Bureau of Consumer Financial Protection,”
15 and inserting “paragraphs (1) through (7) of
16 section 505(a)”; and

17 (B) by striking paragraphs (1), (2), and
18 (3) and inserting the following: “

1 “(1) to ensure the security and confidentiality
2 of customer and consumer nonpublic personal infor-
3 mation;

4 “(2) to protect against any anticipated threats
5 or hazards to the security or integrity of nonpublic
6 personal information; and

7 “(3) to protect against unauthorized access to
8 or use of nonpublic personal information which could
9 result in substantial harm or inconvenience to any
10 customer or consumer.”.

11 **SEC. 3. OBLIGATIONS WITH RESPECT TO THE COLLECTION**
12 **AND DISCLOSURE OF NONPUBLIC PERSONAL**
13 **INFORMATION.**

14 (a) IN GENERAL.—Section 502 of the Gramm-Leach-
15 Bliley Act (15 U.S.C. 6802) is amended—

16 (1) in the heading, by striking “**DISCLOSURES**
17 **OF**” and inserting “**THE COLLECTION AND DIS-**
18 **CLOSURE OF NONPUBLIC**”;

19 (2) in subsection (a), by inserting before “dis-
20 close” the following: “collect nonpublic personal in-
21 formation from a consumer or”;

22 (3) in subsection (b), by amending paragraph
23 (1) to read as follows:

24 “(1) IN GENERAL.—A financial institution may
25 not collect nonpublic personal information from a

1 consumer or disclose nonpublic personal information
2 to a nonaffiliated third party unless the consumer is
3 given the opportunity, before the time that such in-
4 formation is initially collected or disclosed, to direct
5 that such information not be collected or disclosed to
6 such third party.”;

7 (4) in subsection (d), by striking “tele-
8 marketing, direct mail marketing, or other mar-
9 keting through electronic mail to the consumer” and
10 inserting “marketing to the consumer, regardless of
11 medium”;

12 (5) in subsection (e)—

13 (A) by striking “(e) GENERAL EXCEP-
14 TIONS.—” and all that follows through the end
15 of paragraph (2) and inserting the following:

16 “(e) EXCEPTIONS.—The general collection and dis-
17 closure procedures provided in subsections (a) and (b)
18 shall not prohibit or otherwise limit the collection or dis-
19 closure of nonpublic personal information—

20 “(1) if the collection or disclosure is—

21 “(A) necessary to effect, administer, or en-
22 force a transaction requested or authorized by
23 the consumer;

1 “(B) in connection with servicing or proc-
2 essing a financial product or service requested
3 or authorized by the consumer;

4 “(C) with the consent or at the direction of
5 the consumer, and the financial institution ob-
6 tains from the consumer evidence of the con-
7 sumer’s authorization for such collection or dis-
8 closure; or

9 “(D) in connection with—

10 “(i) maintaining or servicing the con-
11 sumer’s account with the financial institu-
12 tion, or with another entity as part of a
13 private label or co-brand credit card pro-
14 gram or an extension of credit on behalf of
15 such entity; or

16 “(ii) a proposed or actual
17 securitization, secondary market sale (in-
18 cluding sales of servicing rights), or similar
19 transaction related to an account or a
20 transaction of the consumer;

21 “(2) to a nonaffiliated third party to perform
22 services for, or functions on behalf of, the financial
23 institution, including marketing of the financial in-
24 stitution’s own products or services, or financial
25 products or services offered pursuant to joint agree-

1 ments between two or more financial institutions
2 that comply with the requirements imposed by the
3 regulations prescribed under section 504, if the fi-
4 nancial institution fully discloses the providing of
5 such information and enters into a contractual
6 agreement with the third party that requires the
7 third party to maintain the confidentiality of such
8 information;”;

9 (B) in paragraph (3)—

10 (i) in subparagraph (A)—

11 (I) by striking “or security” and
12 inserting “security, or integrity”; and

13 (II) by inserting before the semi-
14 colon the following: “, as well as the
15 systems, processes, and services that
16 handle such records”; and

17 (ii) in subparagraph (B), by inserting
18 after “fraud,” the following: “identity
19 theft,”;

20 (C) in paragraph (5), by striking “Bureau
21 of Consumer Financial Protection”; and

22 (D) in paragraph (7)—

23 (i) by striking “or exchange” and in-
24 serting “exchange, or similar transaction”;

25 and

1 (ii) by inserting “collection or” before
2 “disclosure”;

3 (6) by adding at the end the following:

4 “(f) NOTIFICATION TO NONAFFILIATES WHEN
5 SHARING IS TERMINATED.—

6 “(1) IN GENERAL.—If a financial institution is
7 required to terminate sharing nonpublic personal in-
8 formation of a consumer with a nonaffiliated third
9 party—

10 “(A) the financial institution shall notify
11 the nonaffiliated third party that the sharing
12 has been terminated and that the nonaffiliated
13 third party may not share any nonpublic infor-
14 mation of the consumer already received from
15 the financial institution; and

16 “(B) upon receipt of a notice described
17 under subparagraph (A), the nonaffiliated third
18 party may not share any nonpublic information
19 of the consumer already received from the fi-
20 nancial institution.

21 **【“(2) RULEMAKING.—The agencies referred to**
22 **in section 504 shall issue rules to establish the re-**
23 **quirements for notices under paragraph (1), includ-**
24 **ing the form of such notices, taking into account any**
25 **privacy risks posed by such notices.】**

1 “(g) REQUIREMENTS WITH RESPECT TO THE COL-
2 LECTION OF CONSUMER ACCOUNT CREDENTIALS.—A fi-
3 nancial institution may not collect from a consumer any
4 consumer account credentials the consumer uses to access
5 an account at a nonaffiliated third party that is a financial
6 institution unless, prior to collecting the consumer account
7 credentials—

8 “(1) the financial institution clearly and con-
9 spicuously discloses to the consumer, in a form per-
10 mitted by the regulations prescribed under section
11 504—

12 “(A) that the financial institution is col-
13 lecting such consumer account credentials;

14 “(B) how such credentials will be used by
15 the financial institution; and

16 “(C) whether such credentials may be dis-
17 closed to a nonaffiliated third party; and

18 “(2) the consumer is given an opportunity to
19 direct that such credentials not be collected or to di-
20 rect that such credentials not be disclosed to any
21 nonaffiliated third party.”.

22 (b) CONFORMING AMENDMENT.—Section 509(3)(D)
23 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)(D))
24 is amended by striking “section 502(e)(1)(C)” and insert-
25 ing “section 502(e)(1)(D)(ii)”.

1 **SEC. 4. DISCLOSURE OF INSTITUTION PRIVACY POLICY.**

2 Section 503 of the Gramm-Leach-Bliley Act (15
3 U.S.C. 6803) is amended—

4 (1) in subsection (a)—

5 (A) by striking “customer relationship with
6 a consumer and not less than annually during
7 the continuation of such relationship” and in-
8 serting “customer or consumer relationship”;

9 (B) by redesignating paragraphs (1), (2),
10 and (3) as paragraphs (2), (3), and (4), respec-
11 tively; and

12 (C) by inserting before paragraph (2), as
13 so redesignated, the following:

14 “(1) collecting nonpublic personal informa-
15 tion;”;

16 (2) by redesignating subsections (b) through (f)
17 as subsections (c) through (g), respectively;

18 (3) by inserting after subsection (a) the fol-
19 lowing:

20 “(b) DISCLOSURE UPON REQUEST.—Upon the re-
21 quest of a consumer, a financial institution shall provide
22 the consumer with a copy of the disclosures required by
23 subsection (a) in writing or in electronic or other form
24 as permitted by the regulations prescribed under section
25 504.”; and

26 (4) in subsection (d), as so redesignated—

1 (A) in paragraph (1)—

2 (i) by inserting “collecting or” before
3 “disclosing nonpublic”; and

4 (ii) by striking subparagraph (B) and
5 inserting the following:

6 “(B) the purpose for which the financial
7 institution collects the nonpublic personal infor-
8 mation of consumers, as well as how the data
9 will be used;”;

10 (B) in paragraph (2), by inserting before
11 the semicolon the following: “, provided in a
12 manner that provides consumers a meaningful
13 understanding of the information that is col-
14 lected”;

15 (C) in paragraph (3), by striking “and” at
16 the end;

17 (D) in paragraph (4), by striking the pe-
18 riod at the end and inserting a semicolon; and

19 (E) by adding at the end the following:

20 “(5) if the financial institution collects non-
21 public personal information for any purpose other
22 than to provide a specific product or service con-
23 sumers are seeking—

24 “(A) a description of such information;

1 “(B) the purpose for which such informa-
2 tion is collected; and

3 “(C) the right of a customer or consumer
4 to opt out of having such nonpublic personal in-
5 formation collected or disclosed to a non-
6 affiliated third party, and the manner in which
7 a customer or consumer may make such opt out
8 election;

9 “(6) the data retention policies of the financial
10 institution, including the period of time for which
11 the institution retains the nonpublic personal infor-
12 mation relating to customers or consumers;

13 “(7) the right of a customer or consumer to di-
14 rect to have the financial institution terminate the
15 sharing of nonpublic personal information with a
16 nonaffiliated third party, and the manner in which
17 a customer or consumer may make such direction;

18 “(8) the right of a consumer or consumer to re-
19 quest that the financial institution provide the cus-
20 tomer or consumer with a list of all nonpublic per-
21 sonal information relating to the customer or con-
22 sumer held by the financial institution, and the man-
23 ner in which a customer or consumer may make
24 such request; and

1 “(9) the right of a customer or consumer to di-
2 rect to have the financial institution delete nonpublic
3 personal information of the customer or consumer
4 held by the financial institution (subject to the ex-
5 ceptions provided under section 502A(b)(3), and the
6 manner in which a customer or consumer may make
7 such direction.”.

8 **SEC. 5. RULEMAKING.**

9 Section 504 of the Gramm-Leach-Bliley Act (15
10 U.S.C. 6804) is amended—

11 (1) in subsection (a)(1)—

12 (A) by amending subparagraph (A) to read
13 as follows:

14 “(A) IN GENERAL.—The Federal banking
15 agencies, the National Credit Union Adminis-
16 tration, the Securities and Exchange Commis-
17 sion, and the Federal Trade Commission shall
18 each issue such regulations as may be necessary
19 to carry out the purposes of this subtitle with
20 respect to the persons subject to their jurisdic-
21 tion under section 505.”;

22 (B) by striking subparagraph (C) and in-
23 serting the following:

24 “(C) INSURANCE.—

1 “(i) IN GENERAL.—With respect to
2 any person engaged in providing insurance,
3 the applicable State insurance authority of
4 the State in which the person is domiciled
5 shall issue regulations as may be necessary
6 to carry out the purposes of this subtitle,
7 subject to section 505(c).

8 “(ii) LIMITATION.—Regulations
9 issued by a State insurance authority
10 under this subparagraph may be no more
11 restrictive for a person engaged in pro-
12 viding insurance than those regulations
13 issued by the agencies coordinating for
14 consistency and comparability under para-
15 graph (2).”; and

16 (2) by adding at the end the following:

17 “(c) CONSIDERATION OF COMPLIANCE COSTS.—
18 When prescribing rules under this subtitle, agencies shall
19 take into account the compliance cost such rules will im-
20 pose on small institutions.”.

21 **[SEC. 6. ENFORCEMENT.**

22 **[To be added]**

23 **SEC. 7. RELATION TO STATE LAWS.**

24 Section 507 of the Gramm-Leach-Bliley Act (15
25 U.S.C. 6807) is amended to read as follows:

1 **“SEC. 507. RELATION TO STATE LAWS.**

2 “This subtitle and the amendments made by this sub-
3 title supersede any statute or rule of a State or political
4 subdivision thereof that regulates the obligations of a fi-
5 nancial institution with respect to—

6 “(1) the collection or disclosure of personal in-
7 formation;

8 “(2) the disclosure of the financial institution’s
9 privacy policy or information about the financial in-
10 stitution’s privacy policies and practices;

11 “(3) data breach notifications related to the
12 disclosure of personal information;

13 “(4) the access to, deletion of, or other indi-
14 vidual privacy rights with respect to personal infor-
15 mation; or

16 “(5) the international sharing of personal infor-
17 mation.”.

18 **SEC. 8. DEFINITIONS.**

19 Section 509 of the Gramm-Leach-Bliley Act (15
20 U.S.C. 6809) is amended—

21 (1) in paragraph (3)(A), by inserting before the
22 period at the end the following: “and includes a data
23 aggregator”;

24 (2) in paragraph (4), by striking “personally
25 identifiable financial information” and inserting “in-
26 formation that identifies, relates to, describes, is rea-

1 sonably capable of being associated with, or could
2 reasonably be linked, directly or indirectly, with a
3 particular consumer and is”;

4 (3) in paragraph (7), by inserting “collection
5 or” before “disclosure” each place such term ap-
6 pears;

7 (4) by amending paragraph (11) to read as fol-
8 lows:

9 “(11) CUSTOMER OR CONSUMER RELATION-
10 SHIP.—

11 “(A) IN GENERAL.—The term ‘time of es-
12 tablishing a customer or consumer relationship’
13 shall be defined by the regulations prescribed
14 under section 504.

15 “(B) NON-CUSTOMERS.—In the case of a
16 consumer that is not a customer of a financial
17 institution—

18 “(i) the term ‘time of establishing a
19 customer or consumer relationship’ means
20 the time that the financial institution ob-
21 tains nonpublic personal information of the
22 consumer; and

23 “(ii) the financial institution shall be
24 deemed to be in a consumer relationship
25 with such a consumer until such time as

1 the financial institution no longer collects,
2 controls, possesses, transmits, or maintains
3 any nonpublic personal information of the
4 consumer.

5 **【“(C) EXEMPTION FOR CERTAIN TRANS-**
6 **ACTIONS.—**The agencies described in section
7 504(a)(1) shall issue rules to specify that the
8 following transactions do not, by themselves, es-
9 tablish a consumer relationship:**】**

10 **【“(i) The use of an automated teller**
11 **machine.】**

12 **【“(ii) The use of a credit card or**
13 **debit card to make a purchase.】**

14 **【“(iii) Such other similar transactions**
15 **as the agencies determine appropriate.”;**
16 **and】**

17 (5) by adding at the end the following:

18 **“(12) CONSUMER ACCOUNT CREDENTIALS.—**
19 **The term ‘consumer account credentials’ means non-**
20 **public information that a consumer uses to access an**
21 **account of the consumer at a financial institution,**
22 **including a username, password, or an answer to a**
23 **security question.**

24 **“(13) DATA AGGREGATOR.—**The term ‘data
25 aggregator’—

1 “(A) means any person that operates a
2 commercial business or enterprise for the busi-
3 ness purpose of accessing, aggregating, col-
4 lecting, selling, or sharing nonpublic personal
5 information about consumer financial accounts
6 or transactions at the direction of a consumer;
7 and

8 “(B) does not include—

9 “(i) a service provider acting at the
10 express instruction of a financial institu-
11 tion, that accesses, aggregates, collects, or
12 shares nonpublic personal information
13 about a consumer in accordance with para-
14 graphs (1), (2), (3)(A), (3)(B), (3)(C),
15 (3)(D), or (6) of section 502(2); or

16 “(ii) an attorney or accountant acting
17 on behalf of a consumer in accordance with
18 section 502(e)(3)(E).

19 “(14) PERSON ENGAGED IN PROVIDING INSUR-
20 ANCE.—The term ‘person engaged in providing in-
21 surance’ means a person that engages in the ‘busi-
22 ness of insurance’, as that term is defined in section
23 1002 of the Dodd-Frank Wall Street Reform and
24 Consumer Protection Act (12 U.S.C. 5481).”.

1 **SEC. 9. OBLIGATIONS WITH RESPECT TO ACCESS AND DE-**
2 **LETION OF NONPUBLIC PERSONAL INFORMA-**
3 **TION.**

4 (a) IN GENERAL.—Title V of the Gramm-Leach-Bli-
5 ley Act (15 U.S.C. 6801 et seq.) is amended by inserting
6 after section 502 the following:

7 **“SEC. 502A. OBLIGATIONS WITH RESPECT TO ACCESS AND**
8 **DELETION OF NONPUBLIC PERSONAL INFOR-**
9 **MATION.**

10 “(a) ACCESS TO INFORMATION.—

11 “(1) IN GENERAL.—Upon an authorized re-
12 quest from a customer or consumer, a financial in-
13 stitution shall disclose—

14 “(A) any nonpublic personal information
15 relating to the consumer or consumer held by
16 the financial institution;

17 “(B) the list of categories of nonaffiliated
18 third parties with whom the financial institution
19 shares nonpublic personal information relating
20 to the consumer or consumer; and

21 “(C) the list of categories of nonaffiliated
22 third parties from whom the financial institu-
23 tion has received nonpublic personal informa-
24 tion relating to the consumer or consumer.

1 “(2) **FORMAT.**—Disclosures described under
2 paragraph (1) shall be in a structured, commonly
3 used, and machine-readable format.

4 “(3) **EXCEPTION.**—For purposes of subpara-
5 graphs (B) and (C) of paragraph (1), a financial in-
6 stitution is not required to disclose a nonaffiliated
7 third party with whom the financial institution
8 shares or receives nonpublic personal information re-
9 lating to the customer or consumer pursuant to an
10 exception described under any of paragraphs (3)
11 through (8) of section 502(e).

12 “(b) **DELETION OF INFORMATION.**—

13 “(1) **AT THE DIRECTION OF A CUSTOMER OR**
14 **CONSUMER.**—Upon an authorized request from a
15 customer or consumer, a financial institution shall
16 delete any nonpublic personal information relating to
17 the customer or consumer held by the financial insti-
18 tution.

19 “(2) **CERTAIN INACTIVE ACCOUNTS.**—If a cus-
20 tomer or consumer has not used a product or service
21 provided by a financial institution for **【1 year】**, the
22 financial institution shall—

23 “(A) notify the customer or consumer that
24 the customer or consumer has the right to re-
25 quest the deletion of any nonpublic personal in-

1 formation relating to the customer or consumer
2 held by the financial institution, and provides
3 the customer or consumer with clear instruc-
4 tions on how to make such request; and

5 “(B) for each additional 1 year period with
6 respect to which the customer or consumer con-
7 tinues to not use a product or service of the fi-
8 nancial institution, resends the notice described
9 under subparagraph (A).

10 “(3) EXCEPTION.—

11 “(A) IN GENERAL.—This subsection shall
12 not require a financial institution to delete non-
13 public personal information if—

14 “(i) the financial institution is other-
15 wise required by law to retain the non-
16 public personal information;

17 “(ii) the nonpublic personal informa-
18 tion may be necessary to respond to a con-
19 sumer dispute under the Fair Credit Re-
20 porting Act; or

21 “(iii) the nonpublic personal informa-
22 tion may be necessary to retain for a pur-
23 pose described in an exception under sec-
24 tion 502(e).

1 “(B) LIMITATION ON RETAINED NON-
2 PUBLIC PERSONAL INFORMATION.—With re-
3 spect to nonpublic personal information that a
4 financial institution would be required to delete
5 under this subsection but for the application of
6 this paragraph, the financial institution may
7 only use such nonpublic personal information
8 for the applicable purpose described under sub-
9 paragraph (A).

10 “(c) TIMING.—A financial institution that receives an
11 authorized request from a customer or consumer under
12 this section shall respond within 45 business days.

13 “(d) RULEMAKING.—Not later than the end of the
14 1-year period beginning on the date of enactment of this
15 section, each agency or authority described in section 504
16 shall issue rules to carry out this section with respect to
17 the financial institutions subject to its jurisdiction.”.

18 (b) CLERICAL AMENDMENT.—The table of contents
19 in section 1(b) of the Gramm-Leach-Bliley Act is amended
20 by inserting after the item relating to section 502 the fol-
21 lowing:

“Sec. 502A. Obligations with respect to access and deletion of nonpublic personal information.”.

1 **[SEC. 10. OBLIGATIONS WITH RESPECT TO THE INTER-**
2 **NATIONAL SHARING OF NONPUBLIC PER-**
3 **SONAL INFORMATION.**

4 **[(a) IN GENERAL.—**Title V of the Gramm-Leach-
5 Bliley Act (15 U.S.C. 6801 et seq.), as amended by section
6 10, is further amended by inserting after section 502A
7 the following:]

8 **["SEC. 502B. OBLIGATIONS WITH RESPECT TO THE INTER-**
9 **NATIONAL SHARING OF NONPUBLIC PER-**
10 **SONAL INFORMATION.**

11 **["(a) IN GENERAL.—**A financial institution may not
12 share the nonpublic personal information relating to a cus-
13 tomer or consumer with a foreign government.]

14 **["(b) LAW ENFORCEMENT EXCEPTION.—**Subsection
15 (a) shall not apply to the sharing of the nonpublic personal
16 information relating to a customer or consumer with a for-
17 eign government authority if such sharing is—]

18 **["(1) done for legitimate law enforcement pur-**
19 **poses; or]**

20 **["(2) to a foreign government authority having**
21 **jurisdiction over the financial institution for exam-**
22 **ination, compliance, or other purposes as authorized**
23 **by law.”.]**

24 **[(b) CLERICAL AMENDMENT.—**The table of contents
25 in section 1(b) of the Gramm-Leach-Bliley Act, as amend-

1 ed by section 10, is further amended by inserting after
2 the item relating to section 502A the following:】

“Sec. 502B. Obligations with respect to the international sharing of nonpublic
personal information”.

3 **SEC. 11. REPEAL OF EXPIRED PROVISIONS.**

4 The Gramm-Leach-Bliley Act is amended—

5 (1) by striking section 508 (15 U.S.C. 6808);

6 and

7 (2) in the table of contents in section 1(b), by
8 striking the item relating to section 508.

9 **SEC. 12. SENSE OF CONGRESS.**

10 It is the sense of the Congress that the Federal agen-
11 cies implementing the Gramm-Leach-Bliley Act should im-
12 plement such Act, to the extent possible, in a technology-
13 agnostic manner so as to ensure it can adapt to different
14 business models and technologies.