118TH CONGRESS  
1ST SESSION  

H. R.  

To amend the Gramm-Leach-Bliley Act to modernize the protection of the nonpublic personal information of individuals with whom financial institutions have customer or consumer relationship, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. McHENRY 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 individuals with whom financial institutions have customer or consumer relationship, and for other purposes.

1 Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

2 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

3 (a) Short Title.—This Act may be cited as the “Data Privacy Act of 2023”.

4 (b) Table of Contents.—The table of contents for 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. Relation to State laws.
Sec. 7. Definitions.
Sec. 8. Obligations with respect to access and deletion of nonpublic personal information.
Sec. 9. Obligations with respect to the international sharing of nonpublic personal information.
Sec. 10. Repeal of expired provisions.
Sec. 11. GAO Report.
Sec. 12. Sense of Congress.
Sec. 13. Effective date.

SEC. 2. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

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

(1) in subsection (a)—

(A) by striking “of its customers” and inserting “of individuals with whom such financial institution has a customer or consumer relationship”; and

(B) by striking “those customers’ nonpublic personal information” and inserting “those individual’s nonpublic personal information”; and

(2) by adding at the end the following:

“(c) USE OF NONPUBLIC PERSONAL INFORMATION.—It shall be unlawful for a financial institution to willfully use nonpublic personal information without the
consent of an individual with whom the financial institu-

tion has a customer or consumer relationship.”.

SEC. 3. OBLIGATIONS WITH RESPECT TO THE COLLECTION

AND DISCLOSURE OF NONPUBLIC PERSONAL

INFORMATION.

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

(1) in the heading, by striking “DISCLOSURES

OF” and inserting “THE COLLECTION AND DIS-

CLOSURE OF NONPUBLIC”; 

(2) in subsection (a)—

(A) by inserting before “disclose” the fol-

lowing: “collect nonpublic personal information

from an individual with whom such financial in-

stitution has a customer or consumer relation-

ship or”; and

(B) by striking “has provided to the con-

sumer” and inserting “has provided to such in-

dividual”; and

(3) in subsection (b), by amending paragraph

(1) to read as follows:

“(1) In General.—A financial institution may

not collect nonpublic personal information from an

individual with whom such financial institution has

a customer or consumer relationship or disclose non-
public personal information to a nonaffiliated third party unless the individual with whom such financial institution has a consumer or customer relationship is given the opportunity, before the time that such information is initially collected or disclosed, to direct that such information not be collected or disclosed to such third party.”;

(4) in subsection (d)—

(A) by striking “of a consumer” and inserting “of an individual with whom such financial institution has a customer or consumer relationship”; and

(B) by striking “telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer” and inserting “marketing to the individual with whom such financial institution has a customer or consumer relationship, regardless of medium”;

(5) in subsection (e)—

(A) by striking “(e) GENERAL EXCEPTIONS.—” and all that follows through the end of paragraph (2) and inserting the following:

“(e) EXCEPTIONS.—The general collection and disclosure procedures provided in subsections (a) and (b)
shall not prohibit or otherwise limit the collection or disclosure of nonpublic personal information—

“(1) if the collection or disclosure is—

“(A) necessary to effect, administer, or enforce a transaction requested or authorized by the individual with whom the financial institution has a customer or consumer relationship;

“(B) in connection with servicing or processing a financial product or service requested or authorized by the individual with whom the financial institution has a customer or consumer relationship;

“(C) with the consent or at the direction of the individual with whom the financial institution has a customer or consumer relationship, and the financial institution obtains, from such individual, evidence of such individual’s authorization for such collection or disclosure; or

“(D) in connection with—

“(i) maintaining or servicing the account, with such financial institution or with another entity as part of a private label or co-brand credit card program or an extension of credit on behalf of such entity, of an individual with whom such fi-
financial institution or entity has a customer
or consumer relationship;

“(ii) a proposed or actual
securitization, secondary market sale (in-
cluding sales of servicing rights), or similar
transaction related to an account or a
transaction of the individual which whom
such entity or financial institution has a
customer or consumer relationship; or

“(2) to a nonaffiliated third party to perform
services for, or functions on behalf of, the financial
institutions, including marketing of the financial in-
stitution’s own products or services, or financial
products or services offered pursuant to joint agree-
ments between two or more financial institutions
that comply with the requirements imposed by the
regulations prescribed under section 504, if the fi-
nancial institution fully discloses the providing of
such information and enters into a contractual
agreement with the third party that requires the
third party to maintain the confidentiality of such
information;”;

(B) in paragraph (3)—

(i) in subparagraph (A)—
(I) by striking “or security” and inserting “security, or integrity”;

(II) by striking “pertaining to the consumer” and inserting “pertaining to the individual with whom the financial institution has a customer or consumer relationship”;

(III) by inserting before the semicolon the following: “, as well as the systems, processes, and services that handle such records”;

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

(iii) in subparagraph (C), by striking “for resolving customer disputes or inquiries” and inserting “for resolving disputes or inquires relating to individuals with whom the financial institution has a customer or consumer relationship”;

(iv) in subparagraph (D), by striking “relating to the consumer” and inserting “relating to the individual with whom the financial institution has a customer or consumer relationship”; and
(v) in subparagraph (E), by striking “behalf of the consumer” and inserting “behalf of the individual with whom the financial institution has a customer or consumer relationship”; and

(C) in paragraph (7)—

(i) by striking “or exchange” and inserting “exchange, or similar transaction”; (ii) by striking “consumers of such business or unit” and inserting “individuals with whom such business or unit have a customer or consumer relationship”; and (iii) by inserting “collection or” before “disclosure”;

(6) by adding at the end the following:

“(f) Notification to Nonaffiliates When Sharing Is Terminated.—

“(1) In general.—If a financial institution is required to terminate sharing nonpublic personal information, of an individual with whom such financial institution has a customer or consumer relationship, with a nonaffiliated third party—

“(A) the financial institution shall notify the nonaffiliated third party that the sharing has been terminated and that such nonaffiliated
third party may not share any nonpublic information of the individual already received from the financial institution; and

“(B) upon receipt of a notice described under subparagraph (A), the nonaffiliated third party may not share any nonpublic information of such individual already received from the financial institution.

“(2) Rulemaking.—The agencies referred to in section 504 shall issue rules to establish the requirements for notices under paragraph (1), including the form of such notices, taking into account any privacy risks posed by such notices.

“(g) Requirements With Respect to the Collection of Consumer Account Credentials.—A financial institution may not collect from an individual with whom such financial institution has a customer or consumer relationship account credentials such individual uses to access an account at a nonaffiliated third party that is a financial institution unless, prior to collecting the consumer account credentials—

“(1) the financial institution clearly and conspicuously discloses to the consumer, in a form permitted by the regulations prescribed under section 504—
“(A) that the financial institution is collecting such account credentials;

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

“(C) whether such credentials may be disclosed to a nonaffiliated third party; and

“(2) such individual is given an opportunity to direct that such credentials not be collected or to direct that such credentials not be disclosed to any nonaffiliated third party.”.

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

SEC. 4. DISCLOSURE OF INSTITUTION PRIVACY POLICY.

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

(1) in subsection (a)—

(A) by striking “customer relationship with a consumer” and inserting “customer or consumer relationship”; 

(B) by striking “clear and conspicuous disclosure to such consumer” and inserting “clear and conspicuous disclosure to such individual
with whom such financial institution has a customer or consumer relationship’’;

(C) by redesignating paragraphs (1), (2), and (3) as paragraphs (2), (3), and (4), respectively;

(D) by inserting before paragraph (2), as so redesignated, the following:

“(1) collecting nonpublic personal information;”;

(E) in paragraph (3), as so redesignated, by striking “have ceased to be customers of” and inserting “have ceased to have a customer or consumer relationship with”; and

(F) in paragraph (4), as so redesignated, by striking “personal information of consumers” and inserting “personal information of individuals with whom such financial institution has a customer or consumer relationship”;

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

(3) in paragraph (3), as so redesignated, by striking “ceased to be customers of the financial institution” and inserting “ceased to have a customer or consumer relationship with the financial institution”; and
(4) in paragraph (4), as so redesignated, by striking “nonpublic personal information of consumers” and inserting “nonpublic personal information of individual with whom the financial institution has a customer or consumer relationship”.

(5) by inserting after subsection (a) the following:

“(b) DISCLOSURE UPON REQUEST.—Upon the request of an individual with whom a financial institution has a customer or consumer relationship, a financial institution shall provide such individual with a copy of the disclosures required by subsection (a) in writing or in electronic or other form as permitted by the regulations prescribed under section 504.”; and

(6) in subsection (d), as so redesignated—

(A) in paragraph (1)—

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

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

“(B) the purpose for which the financial institution collects the nonpublic personal information of individuals with whom the financial institution has a customer or consumer relationship, as well as how the data will be used;”;
(B) in paragraph (2), by inserting before
the semicolon the following: “, provided in a
manner that provides individuals with whom the
financial institution has a customer or con-
sumer relationship a meaningful understanding
of the information that is collected”;
(C) in paragraph (3), by striking “and” at
the end;
(D) in paragraph (4), by striking the pe-
riod at the end and inserting a semicolon; and
(E) by adding at the end the following:
“(5) if the financial institution collects non-
public personal information for any purpose other
than to provide a specific product or service such an
individual is seeking—
“(A) a description of such information;
“(B) the purpose for which such informa-
tion is collected; and
“(C) the right of such individual to opt out
of having such nonpublic personal information
collected or disclosed to a nonaffiliated third
party, and the manner in which such individual
may make such opt out election;
“(6) the data retention policies of the financial
institute, including the period of time for which
the institution retains the nonpublic personal information relating to such individual;

“(7) the right of such individual to direct the financial institution to terminate the sharing of nonpublic personal information with a nonaffiliated third party, and the manner in which such individual may make such direction;

“(8) the right of such individual to request that the financial institution provide the individual with a list of all nonpublic personal information relating to the individual held by the financial institution, and the manner in which the individual may make such request; and

“(9) the right of such individual to direct the financial institution to delete nonpublic personal information of the individual held by the financial institution (subject to the exceptions provided under section 502A(b)(3), and the manner in which the individual may make such direction.”;

(7) in subsection (f), as so redesignated—

(A) in paragraph 2(A), by striking “to consumers” and inserting “to individuals with whom a financial institution has a customer or consumer relationship”; and
(B) in paragraph 2(C), by striking “enable consumers” and inserting “enable individuals with whom a financial institution has a customer or consumer relationship”; and

(8) in subsection (g), as so redesignated, by striking “sent to consumers” and inserting “sent to individuals with whom a financial institution has a customer or consumer relationship”.

SEC. 5. RULEMAKING.

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

(1) in subsection (a)(1)—

(A) by striking subparagraph (D) and inserting the following:

“(D) INSURANCE.—

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

“(ii) LIMITATION.—Regulations issued by a State insurance authority under this subparagraph may be no more
restrictive for a person engaged in providing insurance than those regulations issued by the agencies coordinating for consistency and comparability under paragraph (2).”; and

(2) by adding at the end the following:

“(c) CONSIDERATION OF COMPLIANCE COSTS.—When prescribing rules under this subtitle, agencies shall take into account the compliance cost such rules will impose on small institutions.”.

**SEC. 6. RELATION TO STATE LAWS.**

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

“SEC. 507. RELATION TO STATE LAWS.

“This subtitle and the amendments made by this subtitle supersede any statute or rule of a State or political subdivision thereof that regulates the obligations of a financial institution with respect to—

“(1) the collection or disclosure of personal information;

“(2) the disclosure of the financial institution’s privacy policy or information about the financial institution’s privacy policies and practices;
“(3) the access to, deletion of, or other individual privacy rights with respect to personal information; or
“(4) the international sharing of personal information.”.

SEC. 7. DEFINITIONS.

Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended—
(1) in paragraph (3)(A), by inserting before the period at the end the following: “and includes a data aggregator”;
(2) in paragraph (4), by striking “personally identifiable financial information” and inserting “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual and is”;
(3) in paragraph (7), by inserting “collection or” before “disclosure” each place such term appears;
(4) by striking paragraph (9);
(5) by amending paragraph (11) to read as follows:
“(11) CUSTOMER OR CONSUMER RELATIONSHIP.—
“(A) IN GENERAL.—The term ‘customer or consumer relationship’ means a customer relationship or a consumer relationship.

“(B) CUSTOMER RELATIONSHIP.—The term ‘customer relationship’ shall have the meaning given the term in rules issued pursuant to section 504.

“(C) CONSUMER RELATIONSHIP.—The term ‘consumer relationship’ shall have the meaning given the term in rules issued pursuant to section 504 and such meaning shall—

“(i) include situations in which a financial institution obtains nonpublic information from an individual with whom the financial institution does not have a customer relationship; and

“(ii) deem a financial institution to no longer to be in a consumer relationship with an individual at such time as the financial institution no longer collects, controls, possesses, transmits, or maintains any nonpublic personal information of such individual.

“(D) TREATMENT OF CERTAIN TRANSACTIONS.—When the terms ‘customer relation-
ship’ and ‘consumer relationship’ are defined by rule, it shall be specified that the following transactions do not, by themselves, establish a consumer relationship or a consumer relationship:

“(i) The use of an automated teller machine.

“(ii) The use of a credit card or debit card to make a purchase.

“(iii) Such other similar transactions as the agencies determine appropriate.”;

and

(6) by adding at the end the following:

“(12) ACCOUNT CREDENTIALS.—The term ‘account credentials’ means nonpublic information that an individual with whom a financial institution has a customer or consumer relationship uses to access an account of the individual at such financial institution, including a username, password, or an answer to a security question.

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

“(A) means any person that operates a commercial business or enterprise for the business purpose of accessing, aggregating, col-
lecting, selling, or sharing nonpublic personal information about financial accounts or transactions, relating to an individual; and

“(B) does not include—

“(i) a service provider acting at the express instruction of a financial institution, that accesses, aggregates, collects, or shares nonpublic personal information about an individual with whom such financial institution has a customer or consumer relationship in accordance with paragraphs (1), (2), (3)(A), (3)(B), (3)(C), (3)(D), or (6) of section 502(2); or

“(ii) an attorney or accountant acting on behalf of an individual with whom such attorney or accountant has a customer or consumer relationship, in accordance with section 502(e)(3)(E).

“(14) PERSON ENGAGED IN PROVIDING INSURANCE.—The term ‘person engaged in providing insurance’ means a person that engages in the ‘business of insurance’, as that term is defined in section 1002 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (12 U.S.C. 5481).”
SEC. 8. OBLIGATIONS WITH RESPECT TO ACCESS AND DELETION OF NONPUBLIC PERSONAL INFORMATION.

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

"SEC. 502A. OBLIGATIONS WITH RESPECT TO ACCESS AND DELETION OF NONPUBLIC PERSONAL INFORMATION.

"(a) ACCESS TO INFORMATION.—

"(1) IN GENERAL.—Upon an authorized request from an individual with whom a financial institution has a customer or consumer relationship, a financial institution shall disclose—

"(A) any nonpublic personal information relating to such individual held by the financial institution;

"(B) the list of categories of nonaffiliated third parties with whom the financial institution shares nonpublic personal information relating to such individual; and

"(C) the list of categories of nonaffiliated third parties from whom the financial institution has received nonpublic personal information relating to such individual."
“(2) FORMAT.—Disclosures described under paragraph (1) shall be in a structured, commonly used, and machine-readable format.

“(3) EXCEPTION.—For purposes of subparagraphs (B) and (C) of paragraph (1), a financial institution is not required to disclose a nonaffiliated third party with whom the financial institution shares or receives nonpublic personal information relating to such individual pursuant to an exception described under any of paragraphs (3) through (8) of section 502(e).

“(b) DELETION OF INFORMATION.—

“(1) IN GENERAL.—Upon an authorized request from an individual with whom a financial institution has a customer or consumer relationship, a financial institution shall delete any nonpublic personal information relating to such individual held by the financial institution.

“(2) CERTAIN INACTIVE ACCOUNTS.—If such individual has not used a product or service provided by a financial institution for 1 year, the financial institution shall—

“(A) notify such individual that such individual has the right to request the deletion of any nonpublic personal information relating to
such individual held by the financial institution, and provide such individual with clear instructions on how to make such request; and

“(B) for each additional 1-year period with respect to which such person continues to not use a product or service of the financial institution, resend the notice described under subparagraph (A).

“(3) EXCEPTION.—

“(A) IN GENERAL.—This subsection shall not require a financial institution to delete nonpublic personal information if—

“(i) the financial institution is otherwise required by law to retain the nonpublic personal information;

“(ii) the nonpublic personal information may be necessary to respond to a dispute under the Fair Credit Reporting Act; or

“(iii) the nonpublic personal information may be necessary to retain for a purpose described in an exception under section 502(e).

“(B) LIMITATION ON RETAINED NONPUBLIC PERSONAL INFORMATION.—With re-
spect to nonpublic personal information that a financial institution would be required to delete under this subsection but for the application of this paragraph, the financial institution may only use such nonpublic personal information for the applicable purpose described under subparagraph (A).

“(c) TIMING.—A financial institution that receives an authorized request, under this section, from an individual with whom such financial institution has a customer or consumer relationship, shall respond within 45 business days.

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

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

“Sec. 502A. Obligations with respect to access and deletion of nonpublic personal information.”.
SEC. 9. OBLIGATIONS WITH RESPECT TO THE INTERNATIONAL SHARING OF NONPUBLIC PERSONAL INFORMATION.

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

“SEC. 502B. OBLIGATIONS WITH RESPECT TO THE INTERNATIONAL SHARING OF NONPUBLIC PERSONAL INFORMATION.

“(a) IN GENERAL.—A financial institution may not share with a foreign government nonpublic personal information relating to an individual with whom such financial institution has a customer or consumer relationship.

“(b) LAW ENFORCEMENT EXCEPTION.—Subsection (a) shall not apply to the sharing of the nonpublic personal information relating to such an individual with a foreign government authority if such sharing is—

“(1) done for legitimate law enforcement purposes; or

“(2) to a foreign government authority having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Gramm-Leach-Bliley Act, as amend-
ed by section 10, is further amended by inserting after
the item relating to section 502A the following:

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

3 SEC. 10. REPEAL OF EXPIRED PROVISIONS.

The Gramm-Leach-Bliley Act is amended—

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

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

9 SEC. 11. GAO REPORT.

The Comptroller General of the United States shall,
not later than 1 year after the date of the enactment of
this Act, submit to the Congress a report that assesses—

(1) whether the safeguard standards promul-
gated pursuant to section 501 of the Gramm-Leach-
Bliley Act, including but not limited to protecting
against unauthorized disclosure, are effective in pro-
tecting individuals with whom financial institutions
have a customer or consumer relationship; and

(2) whether the enforcement regime with re-
spect to those standards are effective in protecting
customers and consumers, and whether additional
remedies are necessary.
SEC. 12. SENSE OF CONGRESS.

It is the sense of the Congress that the Federal agencies implementing the Gramm-Leach-Bliley Act should implement such Act, to the extent possible, in a technology-agnostic manner so as to ensure it can adapt to different business models and technologies.

SEC. 13. EFFECTIVE DATE.

The amendments made by this Act shall take effect on the date that is the earlier of—

(1) the date that is one year after the date on which all rulemaking required under this Act is complete; or

(2) the date that is 2 years after the date of the enactment of this Act.