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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “[To be added Act of 2023]”.

(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. 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.

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 inserting “and other consumers” after “its customers”; and

(B) by striking “those customers’ nonpublic personal information” and inserting “nonpublic personal information relating to those customers and consumers”; and

(2) in subsection (b)—

(A) by striking “section 505(a), other than the Bureau of Consumer Financial Protection,”

and inserting “paragraphs (1) through (7) of section 505(a)”;

and

(B) by striking paragraphs (1), (2), and (3) and inserting the following: “
“(1) to ensure the security and confidentiality of customer and consumer nonpublic personal information;

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

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

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 DISCLOSURE OF NONPUBLIC”;

(2) in subsection (a), by inserting before “disclose” the following: “collect nonpublic personal information from a consumer or”;

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

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

(5) in subsection (e)—

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

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

“(1) if the collection or disclosure is—

“(A) necessary to effect, administer, or en-
force a transaction requested or authorized by
the consumer;
“(B) in connection with servicing or processing a financial product or service requested or authorized by the consumer;

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

“(D) in connection with—

“(i) maintaining or servicing the consumer’s account with the 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; or

“(ii) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to an account or a transaction of the consumer;

“(2) to a nonaffiliated third party to perform services for, or functions on behalf of, the financial institution, including marketing of the financial institution’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”; and

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

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

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

(D) in paragraph (7)—

(i) by striking “or exchange” and in-
serting “exchange, or similar transaction”;
(ii) 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 a consumer with a nonaffiliated third party—

“(A) the financial institution shall notify the nonaffiliated third party that the sharing has been terminated and that the nonaffiliated third party may not share any nonpublic information of the consumer 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 the consumer 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 a consumer any consumer account credentials the consumer 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 consumer 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) the consumer 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.”.


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 not less than annually during the continuation of such relationship” and inserting “customer or consumer relationship”;

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

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

“(1) collecting nonpublic personal information;”;

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

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

“(b) DISCLOSURE UPON REQUEST.—Upon the request of a consumer, a financial institution shall provide the consumer 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

(4) 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 consumers, 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 consumers 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 period 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 consumers are seeking—
   “(A) a description of such information;
“(B) the purpose for which such information is collected; and

“(C) the right of a customer or consumer to opt out of having such nonpublic personal information collected or disclosed to a nonaffiliated third party, and the manner in which a customer or consumer may make such opt out election;

“(6) the data retention policies of the financial institution, including the period of time for which the institution retains the nonpublic personal information relating to customers or consumers;

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

“(8) the right of a consumer or consumer to request that the financial institution provide the customer or consumer with a list of all nonpublic personal information relating to the customer or consumer held by the financial institution, and the manner in which a customer or consumer may make such request; and
“(9) the right of a customer or consumer to direct to have the financial institution delete nonpublic personal information of the customer or consumer held by the financial institution (subject to the exceptions provided under section 502A(b)(3), and the manner in which a customer or consumer may make such direction.”.

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 amending subparagraph (A) to read as follows:

“(A) IN GENERAL.—The Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission shall each issue such regulations as may be necessary to carry out the purposes of this subtitle with respect to the persons subject to their jurisdiction under section 505.”;

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

“(C) 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(e).

“(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:

“(e) 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. ENFORCEMENT.]

[To be added]]

SEC. 7. 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) data breach notifications related to the disclosure of personal information;

“(4) the access to, deletion of, or other individual privacy rights with respect to personal information; or

“(5) the international sharing of personal information.”.

SEC. 8. 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 rea-
sonably capable of being associated with, or could
reasonably be linked, directly or indirectly, with a
particular consumer and is”;

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

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

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

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

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

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

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

"(C) EXEMPTION FOR CERTAIN TRANSACTIONS.—The agencies described in section 504(a)(1) shall issue rules to specify that the following transactions do not, by themselves, establish a consumer relationship:

- The use of an automated teller machine.
- The use of a credit card or debit card to make a purchase.
- Such other similar transactions as the agencies determine appropriate.

(5) by adding at the end the following:

"(12) CONSUMER ACCOUNT CREDENTIALS.—The term ‘consumer account credentials’ means non-public information that a consumer uses to access an account of the consumer at a 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, collecting, selling, or sharing nonpublic personal information about consumer financial accounts or transactions at the direction of a consumer; 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 a consumer 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 a consumer 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. 9. 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 a customer or consumer, a financial institution shall disclose—

“(A) any nonpublic personal information relating to the consumer or consumer 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 the consumer or consumer; and

“(C) the list of categories of nonaffiliated third parties from whom the financial institution has received nonpublic personal information relating to the consumer or consumer.
“(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 the customer or consumer pursuant to an exception described under any of paragraphs (3) through (8) of section 502(e).

“(b) DELETION OF INFORMATION.—

“(1) AT THE DIRECTION OF A CUSTOMER OR CONSUMER.—Upon an authorized request from a customer or consumer, a financial institution shall delete any nonpublic personal information relating to the customer or consumer held by the financial institution.

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

“(A) notify the customer or consumer that the customer or consumer has the right to request the deletion of any nonpublic personal in-
formation relating to the customer or consumer held by the financial institution, and provides the customer or consumer with clear instructions on how to make such request; and

“(B) for each additional 1 year period with respect to which the customer or consumer continues to not use a product or service of the financial institution, resends 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 consumer 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 NON-
PUBLIC 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 sub-
paragraph (A).

“(c) TIMING.—A financial institution that receives an
authorized request from a customer or consumer under
this section 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 fol-
lowering:

“Sec. 502A. Obligations with respect to access and deletion of nonpublic per-
sonal information.”.
SEC. 10. 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 the nonpublic personal information relating to a customer or consumer with a foreign government.

(b) LAW ENFORCEMENT EXCEPTION.—Subsection (a) shall not apply to the sharing of the nonpublic personal information relating to a customer or consumer 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”.

SEC. 11. 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.

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.