AMENDMENT TO THE RULES COMMITTEE PRINT
118-10
OFFERED BY MR. McHENRY OF NORTH CAROLINA

In title XVIII of division A, add at the end the following:

Subtitle D—Data Privacy

SEC. 1861. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This subtitle may be cited as the "Data Privacy Act of 2023”.

(b) TABLE OF CONTENTS.—The table of contents for this subtitle is as follows:

Subtitle D—Data Privacy

Sec. 1861. Short title; table of contents.
Sec. 1862. Protection of nonpublic personal information.
Sec. 1863. Obligations with respect to the collection and disclosure of nonpublic personal information.
Sec. 1864. Disclosure of institution privacy policy.
Sec. 1865. Rulemaking.
Sec. 1866. Relation to State laws.
Sec. 1867. Obligations with respect to access and deletion of nonpublic personal information.
Sec. 1868. Obligations with respect to the international sharing of nonpublic personal information.
Sec. 1869. Definitions.
Sec. 1870. Repeal of expired provisions.
Sec. 1871. GAO report.
Sec. 1872. Sense of Congress.
Sec. 1873. Effective date.
SEC. 1862. 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.—Unless otherwise permitted under section 502(e), it shall be unlawful for a financial institution to willfully use nonpublic personal information without the consent of an individual with whom the financial institution has a customer or consumer relationship.”.

SEC. 1863. 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)—

(A) by inserting before “disclose” the following: “collect nonpublic personal information from an individual with whom such financial institution has a customer or consumer relationship or”; and

(B) by striking “has provided to the consumer” and inserting “has provided to such individual”; 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 nonpublic 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) in the heading, by striking “GENERAL”;

(B) by striking “Subsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information” and inserting “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”; 

(C) by striking paragraphs (1) and (2) and inserting the following:

“(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 financial institution or entity has a customer or consumer relationship; 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 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 institution, including marketing of the financial institution’s own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial 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;”;

(D) 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

(E) 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 infor-
mation 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 fi-
nancial institution.

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

“(g) Requirements With Respect to the Col-
lection of Account Credentials.—A financial insti-
tution may not collect from an individual with whom such
financial institution has a customer or consumer relation-
ship account credentials such individual uses to access an
account at a nonaffiliated third party that is a financial
institution unless, prior to collecting the account creden-
tials—

“(1) the financial institution clearly and con-
spicuously discloses to the individual, in a form per-
mitted 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. 1864. 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 cus-
tomer or consumer relationship’’;

(C) by redesignating paragraphs (1), (2),
and (3) as paragraphs (2), (3), and (4), respec-
tively;

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

“(1) collecting nonpublic personal informa-
tion’’;

(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 con-
sumers” 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) by inserting after subsection (a) the fol-
lowing:

“(b) DISCLOSURE UPON REQUEST.—Upon the re-
quest of an individual with whom a financial institu-
tion has a customer or consumer relationship, a financial insti-

(887714|1)
...tion 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

(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 individuals with whom the financial institution has a customer or consumer relationship, as well as how the information 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 consumer 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 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 such an individual is seeking—

“(A) a description of such information;

“(B) the purpose for which such information 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 institution, including—

“(A) the period of time for which the financial institution retains the nonpublic personal information relating to such individual; or

“(B) the criteria used by the financial institution to determine the period of time for which such information is retained;

“(7) the right of such individual to direct the financial institution to terminate the sharing of non-
public 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.”;

(5) 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
(6) 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. 1865. 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 para-
graph (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 im-
pose on small institutions.”.

SEC. 1866. 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 sub-
title supersede any statute or rule of a State or political
subdivision thereof that regulates the obligations of a fi-
nancial institution with respect to—

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

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

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

“(4) the international sharing of personal infor-
mation.”.
SEC. 1867. 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 non-public personal information if—

“(i) the financial institution is otherwise required by law to retain the non-public 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 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 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. 1868. 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 1867, 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.

“(c) PROHIBITION ON INFORMATION SHARING INVOLVING A FOREIGN ADVERSARY.—
“(1) IN GENERAL.—The exception described under subsection (b) shall not apply to the sharing of nonpublic personal information by a financial institution with the government of a foreign adversary, as determined pursuant to section 7.4(a) of title 15, Code of Federal Regulations, unless the appropriate Federal regulator—

“(A) authorizes the financial institution, in writing, and not less frequently than once every two years, to engage in the sharing; and

“(B) specifies in the authorization the categories of information that, in the determination of the Secretary, qualify for the exemption described under subsection (b).

“(2) REPORTS TO CONGRESS.—Each Federal regulator shall issue an annual report on the authority provided under paragraph (1), which shall include a copy of any unexpired authorization made by the Federal regulator under that paragraph, to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate.

“(3) APPROPRIATE FEDERAL REGULATOR DEFINED.—In this subsection—
“(A) with respect to a financial institution, the term ‘appropriate Federal regulator’ means the Federal agency described in section 505(a) (other than the Bureau of Consumer Financial Protection) with enforcement jurisdiction with respect to the financial institution; and

“(B) the term ‘Federal regulator’ means each Federal agency described in section 505(a) (other than the Bureau of Consumer Financial Protection).”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Gramm-Leach-Bliley Act, as amended by section 1867, 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. 1869. 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 cus-
tomer relationship; and

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

“(D) TREATMENT OF CERTAIN TRAN-
SACTONS.—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 relation-
ship:

“(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 personal 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, collecting, 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(e); 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(c)(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. 1870. 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. 1871. GAO REPORT.

(a) IN GENERAL.—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 promulgated pursuant to section 501 of the Gramm-Leach-Bliley Act, including protecting against unauthorized
disclosure, are effective in protecting 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.

(b) DEFINITIONS.—In this section, the terms “cus-
tomer or consumer relationship” and “financial institu-
tion” have the meaning given those terms, respectively,
under section 509 of the Gramm-Leach-Bliley Act (15

SEC. 1872. SENSE OF CONGRESS.

It is the sense of the Congress that the Federal agen-
cies implementing the Gramm-Leach-Bliley Act should im-
plement 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. 1873. EFFECTIVE DATE.

The amendments made by this subtitle shall take ef-
fect 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 subtitle is
complete; or
(2) the date that is 2 years after the date of the enactment of this Act.