Section by Section: the Data Privacy Act of 2023

House Financial Services Committee Republicans
Chairman Patrick McHenry

Section 1: Short title. The Data Privacy Act of 2023

Section 2: Protection of Nonpublic Personal Information.

Section 2 makes explicit that GLBA's privacy provisions cover both customers and consumers. This ensures that nonpublic personal information is protected whether an individual has a customer relationship or a consumer relationship with the financial institution holding the individual's data. The section also makes clear that it is unlawful for financial institutions to willfully use nonpublic personal information without the consent of an individual with whom the financial institution maintains a customer or consumer relationship.

Section 3: Obligations with Respect to the Collection and Disclosure of Nonpublic Personal Information.

Section 3 expands the current notification obligations on a financial institution to include the nonpublic personal information that is being collected on a customer or consumer. It also provides exceptions for information necessary to effect, administer, or enforce a transaction requested by the consumer or customer, in connection with servicing or processing a request authorized by the consumer or customer, and other exceptions. The section requires financial institutions to notify nonaffiliated third parties when a consumer or customer has terminated sharing of his or her data, and to require the nonaffiliated third party to also cease sharing of the individual's data. Finally, the bill requires that financial institutions clearly and conspicuously notify customers or consumers when their account credentials are collected and how those credentials will be used or shared, and give consumers an opportunity to decline to share those credentials.

Section 4: Disclosure of Institution Privacy Policy.

Section 4 directs financial institutions to disclose information upon the request of a consumer or customer. This is in addition to the privacy notice required at the time of establishing a relationship and annually thereafter. In addition, the bill expands the information to be included in a financial institution's privacy policy disclosure, including but not limited to:

- Nonpublic personal information collected by the financial institution;
- The purpose for which the financial institution collects that nonpublic personal information;
- How that nonpublic personal information will be used;
- The data retention policies of the financial institution;
- Describe any collection of nonpublic personal information that is not necessary to provide the specific product or service the customer or consumer is seeking;
- The right of the customer or consumer to opt out of collection of certain pieces of information;
- The right of a customer or consumer to terminate collection or sharing of their nonpublic personal information;
- The right of a customer or consumer to request a list of all nonpublic personal information held by the financial institution; and
- The right of a customer or consumer to direct the deletion of the nonpublic personal information held by a financial institution unless an exception is met.

Section 5: Rulemaking.

Section 5 directs the applicable state insurance authority shall issue regulations required by this bill. The section also makes clear that in promulgating the regulations required by the bill, agencies should take into consideration the cost of compliance such rules will impose on small institutions.

Section 6: Relation to State Laws.

Section 6 makes clear that the subtitle and changes made by the bill preempt state law with respect to financial data privacy.

Section 7: Definitions.

Section 7 sets out the definition of key terms used in the bill. Nonpublic personal information is defined as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to, directly or indirectly, with a particular consumer. Account credentials is defined as nonpublic personal information that an individual uses to access and account of the individual at a financial institution. Data aggregator is defined as an entity operating a business for the purpose of accessing, aggregating, collecting, selling, or sharing nonpublic personal information. In addition, data aggregators is included in the definition of financial institutions for the purposes of title V of GLBA.

Section 8: Obligations with Respect to Access and Deletion of Nonpublic Personal Information.

Section 8 adds to the regulatory obligations of financial institutions. The section makes clear that customer and consumers have the right to access nonpublic personal information held by a financial institution. Consumers and customers have the right to know the categories of nonaffiliated third parties with whom the financial institution has shared such information, and the categories of nonaffiliated third parties from whom the financial institution has received nonpublic personal information about the customer or consumer. The section makes clear that customers and consumers have the right to request deletion of nonpublic personal information held about him or herself, with exceptions for law enforcement and other purposes. Finally, the section requires that financial institutions notify consumers or customers annually of inactive accounts. Inactive is defined as a consumer not using a product or service for a year. Consumers and customers have the right to delete nonpublic personal information held by a financial institution unless it is required by law, FCRA or another stated purpose under 502(e).

Section 9: Obligations with Respect to the International Sharing of Nonpublic Personal Information.

Section 9 directs that a financial institution shall not share the nonpublic personal information of a customer or consumer with a foreign government, with exceptions for law enforcement purposes.

Section 10: Repeal of Expired Provisions.

Section 11. GAO Report.

Section 11 directs GAO to conduct an audit within one year of enactment assessing the following: whether the safeguard standards issued pursuant to 15 U.S.C. 6801(b) are effective, including against unauthorized disclosures; and whether the enforcement regime with respect to those standards is effective.

Section 12: Sense of Congress.

Section 12 establishes a sense of Congress that regulators should implement GLBA and the amendments made by the bill in technology agnostic manner.

Section 13: Effective Date.

Section 13 specifies that the amendments made by the bill will take place on the earlier of: one year after completion of the rulemaking required under the bill; or two years after date of enactment.