UNITED STATES HOUSE COMMITTEE ON
FINANCIAL SERVICES
CHAIRMAN FRENCH HILL

Section-by-Section: GUARD Financial Data Act

TITLE I—IMPROVEMENTS TO TREATMENT OF CONSUMER FINANCIAL DATA

Sec. 101. Subtitle and Section Heading Alterations.
Section 101 makes alterations to the headings and table of contents for Subtitle A and Section 502 of Title V of the *Gramm-Leach-Bliley Act* (GLBA) to reflect the changes made by the legislation.

Sec. 102. Data Minimization.
Section 102 requires financial institutions to limit their collection and disclosure of consumers' nonpublic personal information (NPI) to that which is adequate, relevant, and reasonably necessary for each purpose for which the NPI is collected or disclosed. Section 102 incorporates the existing GLBA exceptions under section 502(e) for collection and disclosure of NPI.

For disclosure of NPI, this section also incorporates other necessary exceptions for disclosures to service providers, disclosures to third parties under section 1033 of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Dodd-Frank), disclosures to consumer reporting agencies under the *Fair Credit Reporting Act* (FCRA), disclosures to financial regulatory agencies and self-regulatory organizations, and disclosures required by other laws.

Sec. 103. Continuing Consumer Opt-Out Right.
Section 103 codifies into statute the ability of consumers to exercise their right to opt-out of disclosures of NPI to nonaffiliates at any time, as exists in current regulation, subject to existing GLBA exceptions, to create greater durability of the continuing opt-out right.

Sec. 104. Limits on Use of Consumer Access Credentials.
Section 104 requires that before using a consumer's username, password, or other access credentials to access that consumer's account at or obtain NPI from a financial institution, a financial data aggregator or nonaffiliated third party must provide a notice to the consumer of how the access credentials will be used, whether the access credentials will be disclosed to another nonaffiliated third party, the risks associated with access credential-based methods, and the measures taken to ensure privacy and security of consumer NPI obtained with access credentials.

The financial data aggregator or nonaffiliated third party must also provide a consumer an opportunity to opt-out of use of their access credentials for such purposes. If a consumer has received this notice and opportunity to opt-out, the financial institution receiving the request may not deny disclosure of the consumer's data to the financial data aggregator or nonaffiliated third party. Section 104 also requires that financial institutions, financial data aggregators, and nonaffiliated third parties comply with requirements of section 1033 of Dodd-Frank that relate to access credential-based data access methods.

Sec. 105. Additional Information to Be Included in Notices to Consumers.
Section 105 requires that, in addition to existing notice information requirements, a financial institution must provide the following information in notices before disclosing a consumer's NPI to a nonaffiliated third party: 1) categories of purposes for collection and disclosure of NPI; 2) categories of practices with respect to retention of NPI; 3) categories of practices with respect to the use of artificial intelligence for collection, processing, and use of NPI; 4) whether NPI is processed in, retained in, or disclosed to China, Iran, North Korea, or Russia; 5) an explanation of how a consumer can exercise their continuing opt-out right (codifying current regulation); 6) an explanation of how a customer can access copies of a financial institution's privacy disclosures; and 7) an explanation of how a customer or former customer can request disclosure of or deletion of their NPI under Section 107 of this legislation.

Section 105 also directs regulatory agencies to promulgate a new model disclosure form integrating this new information and creates a safe harbor whereby a financial institution will be deemed in compliance with its notice requirements if it uses the current model form for a period of two years after the regulatory agencies finalize the new model form.

Sec. 106. Customer Access to Privacy and Disclosure Policies.
Section 106 requires a financial institution to provide a customer, at any time upon request, a copy of the privacy notice given when NPI is disclosed to a nonaffiliated third party.

Sec. 107. Requests for Disclosure of or Deletion of Nonpublic Personal Information.
Section 107 allows a current or former customer of a financial institution to request access to their NPI held by that financial institution pursuant to the requirements of section 1033 of Dodd-Frank and to receive a list of the categories of nonaffiliated third parties to whom NPI has been disclosed with such category disclosures subject to existing exceptions contained in GLBA's section 502 notice and opt-out regime.

Section 107 also allows a former customer to request deletion of their NPI at a financial institution with whom the former customer no longer has a relationship. It includes exceptions where the NPI is needed for continuing purposes under existing notice and opt-out exceptions in section 502(e) of GLBA, consumer reporting agencies under FCRA, consumer credit disputes under FCRA, and if required by law.

Financial institutions are required to create identity verification procedures to safeguard against fraudulent deletion requests and are given an initial response period limit of 45 days, which can be extended if the former customer submits numerous or complex requests with the former customer to be notified of such extension and the reason for it. Former customers may appeal a denial of a deletion request and are afforded two free deletion requests per year, after which a financial institution may charge a fee for subsequent requests.

Sec. 108. Opt-In for Sensitive Nonpublic Personal Information.
Section 108 requires financial institutions to provide a notice to and obtain the consent of a consumer before collecting or disclosing their sensitive nonpublic personal information ("sensitive NPI") to a nonaffiliated third party. Sensitive NPI includes highly personal demographic information, genetic or biometric data, and precise geolocation data.

A consumer may revoke their consent to collection or disclosure of sensitive NPI at any time. Necessary exceptions are included for protecting confidentiality and security of sensitive NPI by a financial institution, fraud prevention and mitigation, required disclosures to a financial institution's regulators and self-regulatory organizations, and required disclosures to comply with legal processes or investigations by Federal, state, or local law enforcement and judicial authorities.

TITLE II—REGULATORY CONSIDERATION FOR SMALL FINANCIAL INSTITUTIONS

Sec. 201. Regulatory Consideration for Small Financial Institutions.
Section 201 requires regulatory agencies to consider the effects of GLBA regulations on financial institutions with $15 billion or less in assets, including their resource, technical, and personnel limitations in complying. This $15 billion threshold is indexed to nominal GDP and will be adjusted every five years on a going forward basis.

TITLE III—RELATION TO OTHER LAWS

Sec. 301. Relation to State Laws.
Section 301 preempts state financial and nonfinancial consumer data privacy and security laws from being applied at an entity-level to GLBA-covered financial institutions and at a data-level to GLBA-covered NPI. Section 301 also ensures that state insurance authorities retain the ability to promulgate and enforce regulations for insurance companies that are consistent with, comparable to, and no more restrictive than the regulations promulgated by Federal regulators.

TITLE IV—ADDITIONS TO DEFINITIONS

Section 401. Additions to Definitions.
Section 401 makes necessary amendments to existing GLBA definitions, codifies existing regulatory definitions for durability, and adds new definitions.

Financial Institution. Section 401 adds "financial data aggregator" into the existing definition of financial institution.

Nonpublic Personal Information. Section 401 amends the current GLBA definition of NPI to include access credentials, biometric data, and precise geolocation data that a financial institution obtains from a consumer in the course of providing that consumer financial products and services.

Access Credentials. Section 401 adds a definition of "access credentials," which is personally identifiable nonfinancial information used by a consumer to access an account at a financial institution, including usernames, passwords, answers to a security question, and similar types of information.

Artificial Intelligence. Section 401 adds a definition of "artificial intelligence," which is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Biometric Data. Section 401 adds a definition of "biometric data," which is personally identifiable nonfinancial information generated by automatic measurements of biological characteristics.

Consent. Section 401 adds a definition of "consent," which is a clear affirmative act of a consumer that is freely given, specific, informed, and unambiguous, including writings and electronic writings of a consumer that manifest consent by a consumer to a given action.

Covered Nation. Section 401 adds a definition of "covered nation" that includes China, Iran, North Korea, and Russia for the purpose of informing a consumer whether the consumer's NPI is processed in, retained in, or disclosed to one of those countries.

Customer. Section 401 codifies into statute, the current regulatory definition of "customer," which is defined as a consumer who has a customer relationship with a financial institution.

Customer Relationship. Section 401 codifies into statute, the current regulatory definition of "customer relationship," which is defined as a continuing relationship between a consumer and a financial institution under which the financial institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

Financial Data Aggregator. Section 401 adds a definition of "financial data aggregator," which is a commercial enterprise with the primary business purpose of accessing, aggregating, collecting, processing, selling, or otherwise disclosing NPI with exceptions for firms performing services on behalf of financial institutions, consumer reporting agencies under FCRA, fiduciaries acting on behalf of a consumer, nonfinancial retail and other nonfinancial firms that obtain NPI for the purpose of making or receiving payments, and self-regulatory organizations that receive NPI from member financial institutions.

Former Customer. Section 401 adds a definition of "former customer" in order to differentiate such individuals from current customers for the purposes of the former customer deletion request right.

Precise Geolocation Data. Section 401 adds a definition of "precise geolocation data," which includes information derived from global positioning systems and similar methods that can accurately identify the location of a consumer to within one-third of a mile.

Self-Regulatory Organization. Section 401 incorporates a definition of "self-regulatory organization."

Sensitive Nonpublic Personal Information. Section 401 adds a definition of "Sensitive NPI," which is personally identifiable nonfinancial information of a consumer that discloses the consumer's racial or ethnic origin, religious belief, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data of a consumer that is disclosed for the purpose of uniquely identifying a specific consumer; and precise geolocation data.

State. Section 401 adds a definition of "State," which is any State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.