Articles + Publications | May 4, 2026

Federal Privacy Bills Introduced: GUARD Financial Data Act and SECURE Data Act

WRITTEN BY

Theodore P. Augustinos | Kim Phan

On April 22, the U.S. House of Representatives Financial Services Committee and the Energy and Commerce Committee jointly unveiled a paired privacy package that, taken together, would substantially recast the federal obligations for the treatment of consumer data. The “Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act” (the GUARD Financial Data Act) would update and enhance Title V of the Gramm?Leach?Bliley Act (GLBA) for financial institutions. The “Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act” (the SECURE Data Act) would create a national, cross?sector privacy framework that would have applicability and features similar to the current patchwork of state comprehensive privacy laws, with strong entity-level and data-level exemptions for financial institutions and financial data subject to GLBA (and for HIPAA-covered entities and business associates, certain nonprofits, and institutions of higher education).

Although both bills are in the early stages of the legislative process, they signal a deliberate effort to modernize the privacy rights of consumers and the related requirements for businesses, including financial institutions, and to preempt (for the financial services industry) the patchwork of state privacy laws that have emerged in recent years.

GUARD Financial Data Act

The GUARD Financial Data Act is framed as an update to the obligations for how financial institutions “treat,” not merely how they disclose their collection, use and sharing of, consumer financial data. The bill would retitle GLBA Title V’s subtitle A from “Disclosure” to “Treatment,” emphasizing data lifecycle obligations around collection, use, retention, and sharing of nonpublic personal information (NPI).

Another core feature is a new statutory “data minimization” requirement in GLBA § 502. Financial institutions would be required to limit the collection and disclosure of NPI to what is “adequate, relevant, and reasonably necessary” for each stated purpose, subject to the existing GLBA exceptions and other legal obligations. The provision is drafted to preserve the ability to disclose NPI for core functions, such as those currently excepted from the existing GLBA rights to opt-out and limit, as well as Consumer Financial Protection Bureau (CFPB) data?access requirements under § 1033 of the Dodd-Frank Act (CFPB 1033 Rule), and the Fair Credit Reporting Act (FCRA).

The bill would also clarify the durability of consumer control rights within the GLBA’s familiar opt?out framework. Privacy notices would need to be accessible in a way that allows consumers to find and act on their ability to opt out of certain third?party sharing “at any time” after the initial notice.

The bill would add a new opt?in regime for “sensitive nonpublic personal information,” defined to include categories such as biometric data and precise geolocation when used in connection with financial activities, as well as certain intimate personal attributes. For this subset of NPI, a financial institution would not be able to collect or disclose to nonaffiliates absent clear, conspicuous notice and the consumer’s affirmative consent, which could be revoked at any time.

The bill also introduces access and deletion concepts into GLBA. A new § 503A would require financial institutions, on request from a customer or former customer, to disclose NPI they hold and to list categories of affiliates and nonaffiliated third parties to whom NPI has been disclosed (subject to exceptions). Former customers would have a statutory right to request deletion of their NPI, again with exceptions where retention is required by law, needed for certain GLBA?permitted purposes, or necessary for FCRA obligations. The provision includes verification requirements, timeframes to respond (with limited extensions), and a capped number of free annual requests, with a fee option for additional requests.

Privacy notices would become considerably more detailed. GLBA § 503(c) would be expanded to require disclosures about why NPI is collected and shared, retention practices, the financial institution’s use of artificial intelligence in handling NPI, whether NPI is processed or retained in or disclosed to a “covered nation,” and the mechanics for exercising opt?out, access, and deletion rights. The bill would direct regulators to update the GLBA model privacy form and to provide a safe harbor transition period while financial institutions move to any new model.

The bill also responds to long?running concerns about credential?based data aggregation. A new § 502(g) would impose notice and opt?out obligations on financial data aggregators and other nonaffiliated third parties using consumer credentials to access accounts or NPI at financial institutions. Aggregators would need to explain how credentials will be used and shared, disclose associated privacy and security risks, and honor consumer direction not to use credentials. Financial institutions, in turn, would be barred from denying disclosure requests made via properly authorized credential?based access, while preserving the requirement to comply with the CFPB § 1033 Rule.

Recognizing implementation burdens, the GUARD bill directs GLBA regulators, when issuing rules, to “take into account the effects” on financial institutions with $15 billion or less in assets, including resource and staffing limitations and the relative cost of compliance. That threshold would be indexed every five years to growth in U.S. nominal GDP, signaling a long?term small?entity accommodation.

Perhaps most consequentially for the broader privacy landscape, the bill rewrites GLBA § 507 to significantly expand federal preemption. As drafted, the bill’s amendments to GLBA Title V would “supersede and preempt” state statutes, regulations, and other laws that establish consumer data privacy or security requirements for NPI or for financial institutions subject to GLBA. State insurance regulators would retain authority to enforce GLBA and to adopt consistent, but “not more restrictive,” rules for insurance entities.

SECURE Data Act

For businesses that are not GLBA financial institutions, HIPAA-covered entities and business associates, certain nonprofits, and institutions of higher education, the SECURE Data Act would create a comprehensive national

privacy framework enforced by the Federal Trade Commission (FTC) and state attorneys general, with broad preemption of state privacy laws. It would grant consumers a set of uniform rights against “controllers” that meet certain size and data?volume thresholds, while providing exemptions for entities already subject to key sectoral regimes, such as the GLBA.

Under this bill, covered consumers would have rights to confirm whether a controller is processing their personal data; obtain access to that data (subject to trade?secret protections); correct inaccuracies; delete personal data provided by or obtained about them; and, where technically feasible, receive a portable, readily usable copy of data they have provided. Consumers could also opt out of targeted advertising, the sale of personal data, and the use of purely automated profiling that has legal or similarly significant effects.

Sensitive data would receive special treatment. Controllers could not process sensitive data, including data collected from children and teens, without prior consent, and with additional protections and parental consent requirements for minors.

Controllers would be subject to core processing principles similar to emerging global standards: data minimization; limits on secondary uses incompatible with disclosed purposes absent consent; nondiscrimination against consumers for exercising rights; and affirmative prohibitions on processing in violation of federal anti?discrimination laws. Before processing, controllers would need to provide accessible, meaningful privacy notices describing the categories of personal data processed; purposes of processing; how consumers can exercise rights and appeal decisions; categories of data shared and with whom; and whether personal data is being transferred to, processed in, stored in, or sold to a covered nation.

The SECURE Data Act pairs these rights and duties with a statutory security mandate. Controllers would be required to implement “reasonable” administrative, technical, and physical safeguards tailored to the volume, sensitivity, and nature of personal data, with a rebuttable presumption of compliance available to entities that adhere to approved codes of conduct, certifications, or recognized security frameworks.

Data brokers receive specific attention. Controllers meeting a “data broker” definition (*i.e.*, those deriving at least 50% of annual revenue from selling data about individuals with whom they do not have a direct relationship) would be required to post conspicuous online notices, register annually with the FTC, and appear in a public data broker registry that includes links to their privacy policies and instructions for exercising consumer rights.

The bill also sets out obligations for processors acting on behalf of controllers, codifying contractual requirements, audit and assessment rights, confidentiality duties, and downstream subcontractor obligations, and clarifies how to treat deidentified and pseudonymous data. In general, deidentified and pseudonymous data would be insulated from certain consumer rights so long as appropriate technical and administrative safeguards are in place and re?identification is not attempted.

Enforcement authority would vest primarily in the FTC, which would treat violations as unfair or deceptive acts or practices and would be specifically empowered to proceed against common carriers. State AGs would have *parens patriae* authority to bring actions, subject to notice and coordination provisions. There is no private right of action in the bill text as introduced, and there is a built?in right to cure before federal or state enforcement could commence.

Crucially for financial institutions, the SECURE Data Act includes broad exemptions. Among others, “a financial institution subject to title V of the Gramm?Leach?Bliley Act” is expressly exempted, as are HIPAA-covered entities and business associates, certain nonprofits, and institutions of higher education. The bill would also exclude various categories of data already covered by sectoral regimes, including GLBA NPI and FCRA?regulated information. At the same time, the bill would broadly preempt state laws that “relate to the provisions of this Act,” effectively replacing state general privacy statutes with a new federal privacy law with clearsectoral carve?outs.

How the Two Bills Fit Together

Viewed together, the GUARD Financial Data Act and the SECURE Data Act appear designed as complementary pillars: the GLBA would be updated to incorporate for the financial services industry many of the privacy protections currently featured in state comprehensive privacy laws, while ensuring that such federal protections will override conflicting obligations in such state privacy laws; the SECURE Data Act would adopt current consumer data privacy provisions currently featured in state comprehensive privacy laws and replace the current state patchwork. Importantly, these bills would clarify the privacy regime applicable to the financial services industry, and eliminate the confusion caused by the varying provisions and exemptions among current state laws.

These bills are already facing opposition, including from the California Privacy Protection Agency (see here), and may undergo substantial revisions. Further consideration of issues such as preemption of state privacy laws and private rights of action is inevitable. Nevertheless, these two federal privacy bills, taken together, send a clear signal that Congress is seriously considering a federal privacy framework that could provide more certainty, efficiency, and uniformity to the privacy protections that will apply on a going forward basis to consumer data, including financial information.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber