TESTIMONY OF

NATHAN TAYLOR

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

UPDATING AMERICA'S FINANCIAL PRIVACY FRAMEWORK FOR THE 21ST CENTURY

MARCH 17, 2026

Chairman Hill, Ranking Member Waters and members of the Committee, my name is Nathan Taylor, and I am a partner at the law firm Morrison Foerster in the firm's Financial Services and Data, Cyber + Privacy practice groups. I have spent my legal career advising financial institutions on compliance with financial privacy laws, including Title V of the Gramm-Leach-Bliley Act ("GLBA"), as well as other privacy laws, such as the emerging state privacy laws. As co-author of the leading treatise on financial privacy law, *The Law of Financial Privacy*, it is critical that I stay abreast of developments in federal, state and international privacy laws impacting financial institutions. As a result, for more than 20 years, I have closely monitored and advised on the evolution of privacy law in the United States. I am pleased to be here today to provide background on the GLBA, as well as to discuss my views on a potential path forward as the Committee evaluates whether there is a need and, if so, the appropriate way to "modernize" the GLBA.

At the outset, I would like to stress the significance of the GLBA. Since it was enacted in 1999, the GLBA has stood as the cornerstone of financial privacy law. While Congress first passed the Fair Credit Reporting Act ("FCRA") in 1970 and the Right to Financial Privacy Act ("RFPA") in 1978, these laws continue to be more narrowly focused. The GLBA required that all financial institutions provide notice to consumers of their privacy practices, as well as allowed those consumers to dictate whether financial institutions should be permitted to disclose financial information about them to nonaffiliated third parties. In my view, the privacy rights that the GLBA includes continue to be just as meaningful in 2026 as they were in 1999.

Of course, it has been more than 25 years since Congress passed the GLBA. Over the ensuing time, privacy law in this country has evolved significantly. In particular, since California enacted the California Consumer Privacy Act ("CCPA") in 2018, we have seen a very rapid development of comprehensive state privacy laws throughout the country. These new state laws include privacy rights that are not found in the GLBA. For example, many states have enacted laws that include new privacy rights, such as the right to request access to, and the correction and/or deletion of, personal information. Moreover, since 1999, Congress has largely left the GLBA untouched, with only several substantive amendments.

With that background in mind, it begs the question: is there a need to "modernize" the GLBA? This question is an inherently subjective one. The answer depends on what you believe the GLBA should accomplish and, more particularly, what privacy rights American consumers should have with respect to financial information handled by financial institutions. It is not debatable in my view, however, that any updates to the GLBA must be done in a thoughtful manner with a clear understanding of the context in which the GLBA applies. Financial products and services are fundamentally different than, for example, social media accounts and online advertising that have driven the evolution of privacy law. It can be far harder to craft a workable and meaningful privacy right, such as the right to correct information, that would apply with respect to, for example, a consumer's 30-year mortgage, as distinct from that individual's social media account or online shopping transactions. In fact, the CCPA and all of the comprehensive state privacy laws that have followed the California law impliedly recognize this fact. Each of these state laws has specifically exempted information that is subject to the GLBA and the vast majority have exempted financial institutions that are subject to the GLBA.

Moreover, it is important to note that the GLBA is part of a broader landscape of federal consumer financial services laws. Many of these laws provide targeted rights that function similar to privacy rights, such as imposing obligations on financial institutions to provide statements (a form of access) and empowering consumers to dispute and challenge errors (a form of correction). These laws include, for example, the Truth in Lending Act (*e.g.*, credit card dispute rights), the Electronic Fund Transfer Act (*e.g.*, debit card, ATM and ACH dispute rights), the Real Estate Settlement Procedures Act (*e.g.*, loan servicing error dispute rights), and the Fair Debt Collection Practices Act (*e.g.*, rights to dispute and demand validation of debt).

In evaluating how a new privacy right, such as the right to correct personal information, could be added to the GLBA, there are many questions that should be evaluated to ensure that any such right would be both workable and meaningful, while not leading to significant unintended consequences. Take, for example, a consumer's credit card account or automobile installment loan? What information should a consumer be able to "correct"? Credit limit? Account balance? Payment history? Particularly since other federal consumer financial services laws address the accuracy of, and liability for errors in, these types of accounts, it seems clear that a correction right should not supplant those laws or even apply to "core" aspects of a financial account. For example, it would seem absurd to allow a consumer to make a correction request with respect to the APR or term on the individual's mortgage. So, what role could a correction right play? And, if the right is pared back by so many exceptions, would it be meaningful? A logical scope would be to limit the right to the type of basic information, such as contact information, that financial institutions already allow consumers to update. Needless to say, I am skeptical that a correction right could be added to the GLBA that would be meaningful to consumers and workable for financial institutions.

So, back to my original question—is there a need to "modernize" the GLBA? Here's where I come out. I believe that the GLBA has stood the test of time, providing consumers with meaningful control over the disclosure of financial information to nonaffiliated third parties. This longstanding right is broader than, for example, new state opt-out rights for the "sale" of information or "sharing" for targeted advertising, while also not showing signs of age like, for example, the federal Video Privacy Protection Act. And, importantly, the GLBA has been implemented by federal regulators that understand financial services, markets, accounts and transactions in a way that ensures that financial institutions are permitted to disclose financial information in order to support the very accounts and transactions that their customers request. That is, the federal regulators have ensured that the GLBA opt-out right does not undermine the provision of the financial products and services to which the right relates.

That said, in recognition of the evolution of privacy law since 1999, I do think certain updates to the GLBA would be appropriate. First, I believe that it would be reasonable to provide a consumer with the right to request a copy of (or "access" to) "nonpublic personal information" relating to the individual that is maintained at a financial institution. Nonetheless, I believe that it is critical that the right be limited by exceptions for certain information that would be inappropriate to share with a consumer or that could create security or other risks to financial instiuttions. For example, I believe that a financial institution should not be required to provide consumers with a copy of, among other things, information related to the filing of a Suspicious Activity Report, information subject to the attorney-client privilege, confidential supervisory information and information intended for fraud prevention or security purposes.

I believe that it would also be reasonable to provide an individual who is no longer a customer of a financial institution (*i.e.*, an individual who did have, but no longer has, a customer relationship with the financial institution) with the right to request that the financial institution delete "nonpublic personal information" relating to the individual that is maintained by the financial institution. Again, however, I believe that it is critical that the right be limited by certain exceptions. For example, I believe that a financial institution should not be required to delete information before the expiration of relevant statutes of limitations within which the consumer could sue the financial institution. I believe that the right also should not extend to information that a financial institution is required by applicable law to maintain. In addition, I believe that there should be exceptions for, among other things, information that is maintained for fraud prevention or security purposes. Nonetheless, I believe that, to the extent that a financial institution would not be required to delete information because an exception applies, the financial institution should be prohibited from using the information for purposes other than those covered by the relevant exception.

Finally, I believe that any effort to "modernize" the GLBA should ensure that the GLBA is the nationwide standard for the privacy obligations imposed on financial institutions with respect to "nonpublic personal information." While I recognize that the issue of the preemption of state laws can be controversial, I believe that preempting state laws in this area would ultimately be good for the American consumer. In particular, I believe that all Americans should be empowered with the same strong privacy rights with respect to "nonpublic personal information" maintained by financial institutions, regardless of the states in which they may live. For me, it is an unfair and inequitable result that the privacy rights that an American may have with respect to such sensitive information would be dictated solely based on where he or she may live.

Overview of Federal Financial Privacy Law

Federal financial privacy law is comprised of three distinct, but related, federal laws: the GLBA, the FCRA and the RFPA.

The GLBA imposes various privacy obligations and limitations on financial institutions with respect to information relating to individuals who obtain financial products and services from financial institutions for personal, family or household purposes. 15 U.S.C. §§ 6801 *et seq*. *See also* 12 C.F.R. pt. 1016 (CFPB). The FCRA principally regulates the disclosure of, access to, and use of "consumer reports," while functionally providing consumers with broad rights to opt out of the disclosure of consumer report and other information among affiliated businesses and to opt out of the use of various information by affiliates for marketing purposes. 15 U.S.C. §§ 1681 *et seq*. Finally, the RFPA limits access by the federal government to financial records of customers of banks and certain other financial institutions. 12 U.S.C. §§ 3401 *et seq*.

Working together, these federal financial privacy laws functionally limit the disclosure of financial information by various financial institutions to: (1) affiliates; (2) nonaffiliates; and (3) the federal government.

Title V of the Gramm-Leach-Bliley Act

In my testimony, I provide an overview of the privacy obligations and limitations imposed by the GLBA. For simplicity, my testimony focuses on the privacy rules implementing the GLBA that have been issued by the Consumer Financial Protection Bureau, namely, Regulation P. Although my testimony does not address the privacy rules issued by the other federal functional GLBA regulators, such as the Securities and Exchange Commission and the Federal Trade Commission, the GLBA privacy rules issued by the other federal regulators are substantively the same. Finally, note that my testimony does not address the data security and breach notification obligations of the GLBA or the corresponding rules.

Scope

The GLBA applies broadly, in terms of the types of entities subject to the law (*i.e.*, "financial institutions"), the types of individuals protected by the law (*i.e.*, "consumers") and the types of information subject to the law's obligations and limitations (*i.e.*, "nonpublic personal information").

Financial Institutions

All "financial institutions" are subject to the GLBA. *See, e.g.*, 15 U.S.C. § 6801(a) (providing that "[i]t is the policy of the Congress that *each financial institution* has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information") (emphasis added). *See also* 12 C.F.R. § 1016.1(b)(1) (providing that Regulation P "applies to *any financial institution* . . . that is subject to Subtitle A of Title V of the" GLBA) (emphasis added). Under the GLBA, a "financial institution" is "any institution the business of which is engaging in financial activities as described in" in Section 4(k) of the Bank Holding Company Act ("BHCA"). 15 U.S.C. § 6809(3)(A).

The application of the GLBA is not limited to "traditional" financial institutions, but applies broadly to a wide spectrum of entities engaged in "financial activities." Regulation P clarifies that a "financial institution" is "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in" Section 4(k) of the BHCA. 12 C.F.R. § 1016.3(*l*)(1).

In turn, Section 4(k) of the BHCA enumerates activities that are presumptively "financial in nature," such as lending, transferring and safeguarding money. 12 U.S.C. § 1843(k)(4). The BHCA also authorizes the Federal Reserve Board ("Board") to further define financial activities permissible for financial holding companies. 12 U.S.C. § 1843(k)(1). In this regard, the Board's Regulation Y defines activities that are "financial in nature or incidental" thereto. *See* 12 C.F.R. pt. 225. These activities cover the landscape of "traditional" financial services, such as, for example, extending credit or acting as an investment advisor. *See* 12 C.F.R. §§ 225.86, 225.28. These activities also include a wide range of "non-traditional" financial services, including, for example, real estate appraisal services, collection agency services, credit bureau services and providing educational courses and instructional materials to consumers on individual financial management matters. *See id*. Regardless, if an entity is in the business of engaging in an activity

that is financial in nature or incidental to a financial activity under Section 4(k) of the BHCA, that entity would be considered a "financial institution" for purposes of, and subject to, the GLBA.

I understand that Members of this Committee have expressed concern as to whether financial data aggregators are subject to the GLBA. In my view, the answer is unequivocally yes. For example, Regulation Y clarifies that financial activities include "[p]roviding data processing, data storage and data transmission services, facilities . . . databases, advice, and access to such services, facilities, or data-bases by any technological means, if," among other things, "[t]he data to be processed, stored or furnished are financial, banking or economic." 12 C.F.R. § 225.28(b)(14)(i). In my view, the very nature of the business of a financial data aggregator is to provide data processing services for financial and banking data. As a result, to the extent that an entity is in the business of providing data processing services for financial or banking data, like a financial data aggregator, the entity should appropriately be viewed as a "financial institution" subject to the GLBA.

Consumers / Customers

The GLBA's protections extend to any individual who applies for, obtains or has previously obtained a consumer financial product or service from a financial institution, namely, a "consumer."

In particular, a "consumer" is an individual who obtains, or has obtained, a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes.[1] 12 C.F.R. § 1016.3(e)(1). Note that a "consumer" includes an individual who applies for a financial product or service, but does not obtain the product or service (*e.g.*, a declined applicant). 12 C.F.R. § 1016.3(e)(2)(i). So, for example, a credit card issuer's "consumers" include individuals with a current credit card account, individuals who formerly had a credit card account and individuals who applied for, but did not receive or accept, a credit card account.

The GLBA also imposes distinct obligations on financial institutions with respect to their "customers." A "customer" is a specific type of "consumer." In particular, a "customer" is a "consumer" who has a continuing relationship with a financial institution in 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. 12 C.F.R. §§ 1016.3(i) (definition of "customer"), 1016.3(j)(1) (definition of "customer relationship").

As discussed later in my testimony, as a practical matter, the "consumer" / "customer" distinction is only relevant to which "consumers" must be provided an initial privacy notice and which "consumers" must be provided an annual privacy notice. The distinction has no bearing on the right to opt out of the disclosure of "nonpublic personal information" to nonaffiliated third parties, which extends to all "consumers," including "customers."

[1] The GLBA does not apply to information about companies or individuals who obtain financial products or services for business, commercial or agricultural purposes. 12 C.F.R. § 1016.1(b)(1).

Nonpublic Personal Information

The GLBA's obligations and limitations apply broadly with respect to personally identifiable information relating to "consumers." For purposes of the GLBA, "nonpublic personal information" includes any information:

(1) "[a] consumer provides to [a financial institution] to obtain a financial product or service from" the financial institution;

(2) "[a]bout a consumer resulting from any transaction involving a financial product or service between" the financial institution and the consumer; or

(3) the financial institution "obtain[s] about a consumer in connection with providing a financial product or service to that consumer."

12 C.F.R. §§ 1016.3(p)(1) (definition of "nonpublic personal information"), 1016.3(q)(1) (definition of "personally identifiable financial information").

It is important for me to stress the breadth of this critical term. As a practical matter, the GLBA applies with respect to *any* information that is personally identifiable with a "consumer" and that a financial institution collects, generates or otherwise obtains in connection with evaluating the individual for, or providing the individual with, a financial product or service.

As an example, take an individual who is a customer of a bank and has a savings account and credit card account with the bank. So long as the information is identifiable with the customer, the GLBA applies to, among many other things, the application information provided by customer to the bank and all of the transaction and account information maintained by the bank. The GLBA also applies to data obtained by the bank from third parties in connection with providing the customer with those financial products, including, for example, consumer reports obtained from consumer reporting agencies. But, the GLBA does not stop with "traditional" financial information. In fact, the information covered by the GLBA does not need to be financial at all. For example, if the customer visits the bank's branch to discuss an account issue and the individual is recorded on the bank's CCTV, the video recording would be subject to the GLBA. Similarly, if a bank employee meets with the customer at the bank and learns personal information about the customer, such as the fact that the customer has a two-year old son named Branch, a wife that loves writing and painting and a deep interest in Minor League Baseball, that personal information would be subject to the GLBA. In both examples (*i.e.*, the video recording and the information about the customer's personal life), even though such information may not be "financial," the information would have been obtained by the bank "in connection with providing" financial products to the customer and, as a result, would be considered "nonpublic personal information."

Privacy Policies

The GLBA requires that a financial institution provide individuals with its privacy policy in two different contexts: an initial notice to certain "consumers" and an annual notice to its "customers." These notice obligations are one of the two "pillars" of the GLBA, along with the disclosure opt-out right discussed later in this testimony.

Initial Notice

A financial institution must provide its "initial" privacy policy in two contexts. First, a financial institution must provide its privacy policy to an individual who becomes its "customer" no later than when the financial institution establishes a "customer relationship" with the individual. 12 C.F.R. § 1016.4(a)(1). Because the notice must be provided by the time the "customer relationship" is formed, as a practical matter, financial institutions typically provide their privacy policy during the application stage in order to ensure that if an individual is approved, the individual will have received notice before the relationship is formed. This has the practical effect that financial institutions provide their privacy policy to individuals who do not actually become their customers, such as individuals who elect not to obtain, or who are not approved for, financial products or services.

Second, a financial institution must provide its "initial" privacy policy to any "consumer" before the financial institution discloses "nonpublic personal information" about the individual to a nonaffiliated third party, other than as permitted by certain exceptions discussed further in this testimony. 12 C.F.R. § 1016.4(a)(2). This notice requirement functions in a powerful, pro-consumer way. In particular, there are many contexts in which financial institutions provide financial products and services to individuals without having an ongoing relationship with the individuals and in contexts in which it would be difficult to provide those individuals with a privacy policy.

For example, if an individual uses a Bank ABC debit card to make a withdrawal at an ATM operated by Bank XYZ, the individual is Bank ABC's "customer" because the individual has a deposit account with Bank ABC. With respect to Bank XYZ, the individual is the bank's "consumer" because the individual conducted an isolated ATM transaction with the bank, but the individual is not the bank's "customer" because there is no ongoing relationship between the bank and the individual. As a result, Bank XYZ would be prohibited from disclosing "nonpublic personal information" about the individual outside of certain exceptions unless the bank provided the individual with its initial privacy notice (and, as discussed later, an opportunity to opt out). There are numerous complexities to providing notice at an ATM, and it is likely that Bank XYZ would not provide the individual with its privacy policy during the ATM transaction. As a result, Bank XYZ would be prohibited from disclosing information about the ATM transaction to a nonaffiliated third party, other than as permitted under certain exceptions. This functions to significantly limit the extent to which Bank XYZ may disclose "nonpublic personal information" relating to the individual to nonaffiliated third parties, without the individual having to elect to opt out.

Annual Notice

In general, a financial institution must provide each "customer" with its privacy policy annually during the "customer relationship" (*i.e.*, at least once in any period of 12 consecutive months during which the customer relationship exists). 12 C.F.R. § 1016.5(a)(1). So, for example, for any "customer" who obtains a 30-year mortgage, a financial institution is likely to have an obligation to provide the individual with its privacy policy many times over the life of the loan.

In 2015, however, the GLBA was amended to provide, in pertinent part, that a financial institution is not required to provide a "customer" with an annual privacy notice if the financial institution does not disclose "nonpublic personal information" about the individual to nonaffiliated third parties outside of exceptions. 12 C.F.R. § 1016.5(e)(1). That is, a financial institution is not required, in pertinent part, to provide a "customer" with an annual privacy notice if the financial institution does not disclose "nonpublic personal information" about the individual in a manner that would require the financial institution to provide the individual with an opportunity to opt out of such disclosure. In practice, for many financial institutions, the cost savings associated with not having an annual notice obligation provides a meaningful incentive for those financial institutions to limit their sharing of information about customers with nonaffiliated third parties to only those scenarios where sharing is permitted by exceptions.

Notice Content / Model Form

The GLBA requires that a financial institution provide meaningful information about its privacy and security practices in its initial and annual privacy notices. In this regard, note that the content that is required to be included in initial and annual notices is the same.

For example, a financial institution must describe the categories of "nonpublic personal information" that it collects and discloses, as well as the categories of affiliates and nonaffiliated third parties to whom it discloses "nonpublic personal information" outside of certain exceptions. 12 C.F.R. §§ 1016.6(a)(1) – (3). A financial institution also must describe its policies and practices for protecting the confidentiality and security of "nonpublic personal information." 12 C.F.R. § 1016.6(a)(8). And, most importantly, if the financial institution is required to provide consumers with an opportunity to opt out of the disclosure of information to nonaffiliated third parties, the financial institution must include an explanation of the consumer's opt-out right, as well as the method(s) by which the consumer may exercise that right. 12 C.F.R. § 1016.6(a)(6).

It is important to highlight that a financial institution also must include any disclosure that the financial institution is required to make under the FCRA regarding a consumer's ability to opt out of the sharing of certain information among affiliates. 12 C.F.R. § 1016.6(a)(7). This is a significant requirement in several respects. First, the GLBA only limits the disclosure of information to nonaffiliated third parties (and not to affiliates). Because, however, a financial institution must include its FCRA affiliate sharing notice in its GLBA privacy policy, the GLBA becomes a vehicle for the communication of a right to limit affiliate sharing that is not included within the GLBA itself. Second, the FCRA only requires that a financial institution provide an affiliate sharing notice to an individual one time. *See* 15 U.S.C. § 1681a(d)(2)(A)(iii). Because financial institutions have an annual privacy notice obligation for their customers under the GLBA, the fact that the FCRA affiliate sharing notice must be included in the GLBA privacy policy has the effect of significantly proliferating the extent to which financial institutions provide consumers with an FCRA affiliate sharing notice.

Of note, in 2006, Congress amended the GLBA to provide that the implementing federal regulators were required to develop a model form that financial institutions could elect to use to provide consumers with their privacy policy. *See* 15 U.S.C. § 6803(e). *See also* 12 C.F.R. pt. 1016, App. (model form issued by the CFPB). In amending the GLBA, Congress specifically

provided that a financial institution that used the model form would be deemed in compliance with the GLBA's requirements for the content of a privacy policy. 15 U.S.C. § 6803(e)(4). This safe harbor provided financial institutions with a meaningful incentive to adopt the model form and led to broad adoption of the model form throughout the financial services industry.

In my view, the broad adoption of the model form has had significant, pro-consumer impacts. First, because the model form was specifically crafted by the regulators to be easy for consumers to understand and because so many financial institutions have adopted the model form, it has increased the understandability of GLBA privacy notices across the industry. Second, because of the model form's simplicity and its widespread adoption across the financial services industry, it has made it far easier for consumers to compare the privacy practices of multiple financial institutions that use the model form (by comparing multiple forms).

Nonaffiliate Disclosure Limitations

In general, the GLBA prohibits a financial institution from disclosing "nonpublic personal information" about a consumer to a nonaffiliated third party without first providing the consumer with the opportunity to opt out of the disclosure. This nonaffiliate disclosure limitation is the second "pillar" of the GLBA.

Notice and Opportunity to Opt Out

Specifically, a financial institution is prohibited from, "directly or through any affiliate," disclosing "nonpublic personal information" relating to a consumer to a nonaffiliated third party unless:

(1) the financial institution has provided the consumer with its initial privacy notice;

(2) the financial institution has provided the consumer with its opt-out notice;

(3) the financial institution has given the consumer a reasonable opportunity to opt out; and

(4) the consumer does not opt out.

12 C.F.R. § 1016.10(a)(1). As a result, in general, a financial institution may not disclose any "nonpublic personal information" to any nonaffiliated third party unless the consumer has had an opportunity, but elected not, to opt out of such disclosure.

It is important to highlight that this broad prohibition applies with respect to any "nonpublic personal information" relating to a consumer, regardless of the sensitivity of the information, regardless of the type of nonaffiliated third party to which the information will be disclosed and regardless of the context of the disclosure and its intended use (assuming, of course, that an exception does not apply). These distinctions are critical. Given its breadth, the GLBA's limitation on the disclosure of information to nonaffiliated third parties functions more broadly than the disclosure limitations of the new comprehensive state privacy laws. For example, the California Consumer Privacy Act and the Virginia Consumer Data Protection Act only provide an opt out from the "sale" of personal information or the "sharing" of personal information for certain advertising. Cal. Civ. Code § 1798.120; Va. Code § 59.1-577(A)(5).

Exceptions

The GLBA includes exceptions that permit a financial institution to disclose "nonpublic personal information" to a nonaffiliated third party without allowing the consumer to opt out or notwithstanding the fact that the consumer has previously opted out. These exceptions are intended to permit the types of sharing that are necessary for a financial institution to do business and provide the very financial products and services requested by a consumer.

First, the GLBA permits a financial institution to disclose "nonpublic personal information" to a nonaffiliated third party for the third party to perform services for, or functions on behalf of, the financial institution (*i.e.*, disclosures to service providers). 12 C.F.R. § 1016.13(a). A financial institution, however, is only permitted to disclose "nonpublic personal information" to its service provider if the financial institution has first provided its initial privacy notice to the relevant consumer and the financial institution has entered into a contract with the service provider that "prohibits the [service provider] from disclosing or using the information other than to carry out the purposes for which [the financial institution] disclosed the information." 12 C.F.R. § 1016.13(a)(1).

In addition, the GLBA includes exceptions that permit a financial institution to disclose "nonpublic personal information" to a nonaffiliated third party in order to process transactions and maintain and service accounts. *See* 12 C.F.R. § 1016.14. For example, the GLBA provides that a financial institution may disclose "nonpublic personal information": (1) "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes"; (2) in connection with "[s]ervicing or processing a financial product or service that a consumer requests or authorizes"; or (3) in connection with "[m]aintaining or servicing the consumer's account." 12 C.F.R. §§ 1016.14(a), (a)(1), (a)(2).

The GLBA also includes exceptions that permit a financial institution to disclose "nonpublic personal information" to a nonaffiliated third party in certain other contexts that are important to the operation of a financial institution. *See* 12 C.F.R. § 1016.15. For example, the GLBA includes exceptions that permit a financial institution to disclose information to a nonaffiliated third party in order "[t]o protect the confidentiality or security of" the financial institution's records or "[t]o protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability." 12 C.F.R. §§ 1016.15(a)(2)(i) – (ii). A financial institution also is permitted to disclose information to a nonaffiliated third party in order "[t]o comply with Federal, state, or local laws, rules and other applicable legal requirements," to comply with a subpoena or summons issued by relevant authorities or to respond to judicial process. 12 C.F.R. § 1016.15(a)(7).

Account Number Disclosure Limitation

In addition to its general limitation on the disclosure of information to nonaffiliated third parties, the GLBA includes a far broader limitation on the disclosure of financial account numbers for marketing purposes specifically. This limitation is intended to prevent a nonaffiliated third party from being able to directly charge a customer's account as a result of a financial institution's disclosure of "nonpublic personal information" to the third party.

Specifically, a financial institution generally is prohibited from, "directly or through an affiliate," disclosing an "account number or similar form of access number or access code for a consumer's credit card account, deposit account, share account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or" e-mail marketing to the consumer. 12 C.F.R. § 1016.12(a).

Importantly, unlike the more general nonaffiliate disclosure limitation, the account number disclosure limitation includes only two exceptions, for a financial institution's disclosure to its own service provider to market the financial institution's own products or services (as long as the service provider is not authorized to directly charge the account) or to a participant in a private label credit card program or an affinity program where the participants in the program are identified to the customer when the customer enters into the program. 12 C.F.R. § 1016.12(b).

Relation to State Law

As a general matter, the GLBA does not preempt or supersede state privacy laws. In particular, the GLBA provides that the statute "shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the [GLBA], and then only to the extent of the inconsistency." 15 U.S.C. § 6807(a).

On its face, this provision would appear to provide that the GLBA may preempt some state privacy laws. As a practical matter, however, it does not. In particular, the GLBA also provides that a State law is not inconsistent with the GLBA if the CFPB determines that the state law affords protections "greater than the protection provided" by the GLBA. 15 U.S.C. § 6807(b). This type of preemption determination is only made if an interested party initiates a complaint or submits a petition to the CFPB. *Id*. Regardless, in practice, these types of preemption determinations have not historically been made.

Evolution of State Privacy Law

Since the GLBA was enacted in 1999, many state privacy laws have been enacted, including financial privacy laws similar to the GLBA and more comprehensive privacy laws that generally regulate entities doing business in a state.

State Financial Privacy Laws

Several states, including, for example, California and Vermont, have adopted laws that are similar to, but that go beyond, the GLBA. *See* Cal. Fin. Code §§ 4050–4060; Vt. Reg. B-2018-01. For example, the California Financial Information Privacy Act prohibits a financial institution from disclosing nonpublic personal information relating to a consumer to any nonaffiliated third party, unless the financial institution has obtained the consumer's consent authorizing the disclosure of information to nonaffiliated third parties. Cal. Fin. Code § 4053(a)(1). That is, the California law requires that a financial institution obtain a consumer's "opt in" to disclosures to nonaffiliated third parties, as distinct from the opt-out opportunity required by the GLBA. The California law also requires that a financial institution provide

consumers with an opportunity to opt out of disclosures to a financial institution's joint-marketing partners, which is not required by the GLBA. Cal. Fin. Code § 4053(b)(2).

The CCPA and Similar State Laws

In 2018, California enacted what was arguably the most expansive privacy law in U.S. history, namely, the CCPA. *See* Cal. Civ. Code §§ 1798.100 – 1798.199. The CCPA imposed significant and often first-of-their-kind privacy obligations on businesses that handle personal information relating to California residents, providing California residents with corresponding privacy rights, including, for example, access, correction and deletion rights, as well as the right to opt out of the "sale" of personal information and the "sharing" of personal information for cross-contextual behavioral advertising.

Since the CCPA was enacted, nineteen states have followed California's lead and enacted comprehensive state privacy laws. Of particular note, each of these state laws, like the CCPA, specifically exempts information subject to, or handled in accordance with, the GLBA. *See, e.g.*, Cal. Civ. Code § 1798.145(e); Fla. Stat. § 501.703(2)(b); Mont. Code § 30-14-2804(f); Utah Code § 13-61-102(2)(k); Va. Code § 59.1-576(B)(ii). That is, in general, none of these state privacy laws apply to "nonpublic personal information" subject to the GLBA.

Moreover, all of the state laws that followed the CCPA have exempted *some* "financial institutions" subject to the GLBA, with the vast majority exempting *all* "financial institutions." For example, the Virginia Consumer Data Protection Act provides that the law "shall not apply to any . . . financial institution . . . subject to Title V of the" GLBA. Va. Code § 59.1-576(B)(ii). Several of these laws exempt only certain financial institutions. For example, the Oregon Consumer Privacy Act provides that the law does not apply to, among others, insured depository institutions and credit unions, as well as their affiliates and subsidiaries that are only and directly engaged in financial activities described in Section 4(k) of the BHCA. Or. Rev. Stat. §§ 646A.572(2)(*l*) (exemption), 706.008(9) (definition of "financial institution").

The Path Forward

I would like to reiterate my strong belief that the GLBA has stood the test of time, providing consumers with meaningful control over the disclosure of financial information to nonaffiliated third parties. Importantly, this longstanding right is broader than the more recent state privacy law limitations on the disclosure of personal information. Nonetheless, in recognition of the evolution of privacy law since 1999, I do think it is reasonable for Congress to evaluate the need to "modernize" the GLBA.

In order to "modernize" the GLBA, I believe any legislation that this Committee considers should address the following three principles:

(1) A federal bill should provide a consumer with the right to request that a financial institution disclose to the individual a copy of "nonpublic personal information" that the financial institution maintains about the individual (*i.e.*, an access right);

(2) A federal bill should provide a consumer with the right to request that a financial institution with which he or she no longer has a customer relationship delete "nonpublic personal information" that the financial institution maintains about the individual; and

(3) A federal bill should preempt state privacy laws to the extent that they may impose obligations or limitations on financial institutions with respect to "nonpublic personal information," to ensure that all Americans receive the same privacy rights for financial information regardless of the state in which they may live.

* * *

Thank you for the opportunity to speak with you today. I would be happy to address any questions that you may have.