Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 25, 2026

Data Privacy vs. Bank Secrecy: Regulating the Flow of Information Within Bank-Fintech Partnerships

Banks are increasingly interconnected with nonbank financial technology. As this trend continues, policy responses to update regulatory frameworks may be proposed.

Bank-nonbank relationships—particularly ones involving data transfers—are often subject to different regulatory requirements across a range of legal frameworks. When policymakers change or update one set of rules for banks, it could cause confusion, inconsistencies, or even conflicting incentives among market participants.

For example, financial institutions, including depository institutions such as banks and credit unions, are required to understand whom their customers are and what their purposes are for establishing accounts. This serves as a foundational element of the anti-money laundering (AML) regulatory framework in the U.S. financial sector. Concurrently, banks are required to protect consumer nonpublic personal information (NPI). Further, banks are responsible for ensuring that any partnerships they engage in comply with relevant banking laws, including AML and data privacy provisions.

This In Focus explains how banks manage information in a manner that complies with three laws—the Bank Secrecy Act (P.L. 91-508), the Graham-Leach-Bliley Act (P.L. 106-102), and the Bank Service Company Act (P.L. 87-856)—particularly in light of increased partnership activity between banks and nonbank financial technology companies (fintechs).

Anti-Money Laundering

The statutory foundation for AML policies was established in the 1970s in the Bank Secrecy Act (BSA, 31 U.S.C. §5311 et seq). At a general level, this framework requires financial institutions to keep certain records and report certain transactions. Over time, the regulations implementing this framework have been updated to reflect new ways of conducting transactions and to include novel business models. Further, in 2003, bank and credit union regulators jointly issued the Customer Identification Programs (CIP) rulemaking, which implemented provisions of the USA PATRIOT Act (P.L. 107-56) by setting "standards for financial institutions regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution." Essentially, a depository institution is responsible for obtaining, at a minimum, the following information from a customer prior to opening an account: the customer's name, date of birth, address (for an individual), and Tax Identification Number (TIN) or Social Security Number.

The CIP requirements in the BSA generally apply to all financial institutions, including banks, credit unions, broker/dealers, insurance companies, exchanges, money transmitters, and several others. Financial technology firms are not explicitly covered, but Section 5312(a)(2) does include "any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage" and "any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters." Further, BSA policy is broadly developed by the Financial Crimes Enforcement Network (FinCEN), the bureau in Treasury responsible for AML. However, the CIP regulations are implemented by the various financial regulators. These policies may change with changes in agency leadership.

Gramm-Leach-Bliley

In the financial system, data privacy is governed by Title V of the Gramm-Leach-Bliley Act (GLBA, 15 U.S.C. §6801 et seq). Financial institutions, including banks, are required to develop and give notice of their privacy policies to their own customers and must give notice and an opportunity for a consumer to "opt out" before disclosing any personal financial information to an unaffiliated third party. The provision also requires financial regulators to issue regulations to safeguard personal financial information.

The privacy provisions in GLBA apply to institutions that engage in "activities that are financial in nature." While financial technology is not explicitly listed as an activity that meets this definition, the statute requires regulators to consider "changes … in the technology for delivering financial services" and "whether such activity is necessary or appropriate to allow [a bank] to compete effectively with any company seeking to provide financial services [or] efficiently deliver information and services that are financial in nature through the use of technological means."

Further, under the Consumer Financial Protection Bureau's 2024 open banking rulemaking (12 C.F.R part 1033, subparts B and C), authorized third parties that seek access to covered data on behalf of a consumer to provide a product or service that the consumer requested must satisfy the applicable safeguard rules under GLBA. For more on the open banking rule, see CRS In Focus IF13117, *Access to Consumer Financial Data: Open Banking and the CFPB's Section 1033 Rule*, by Karl E. Schneider.

Bank Service Company Act

Banks often partner or contract with other firms to facilitate certain services. For example, a bank may use a data processor to help manage its marketing with clients. Bank regulators examine banks for safety and soundness as well as for compliance with certain banking laws. They also supervise the relationships banks hold with third parties pursuant to their authorities under the Bank Service Company Act (12 U.S.C. §1861 et seq.).

The provisions under this law apply to permissible bank service company activities, including check and deposit sorting and posting, bookkeeping, accounting, statistical, or other related activities. There is no explicit reference to fintech activities, though fintechs often perform these functions.

Regulating Bank-Fintech Partnerships

Consumers can interact with banks directly through local branches or online through the internet or banking apps. Similarly, consumers can use fintechs to access various financial services. Sometimes, a consumer interacts with a fintech to obtain banking services, and behind the scenes a bank is performing the banking service, while the fintech is running the consumer interface.

Banking as a Service

One way banks and fintechs work together is in a model referred to as "banking as a service." In this model, a fintech pays a bank to provide core banking services, and those services are effectively white labeled for consumption on the fintech's platform.

Consider the following example: A customer uses a fintech app to open a checking account and deposit a cash balance that was previously held in a digital wallet. To open the bank account, the bank now faces a number of regulatory requirements:

- The bank must be able to verify the customer's identity and purpose for opening the account.
- The bank must be able to disclose its privacy policies to the customer and provide the customer with an opportunity to opt out of certain third-party disclosures.
- The bank relationship with the fintech(s) is subject to supervisory oversight by the bank regulators.

If the customer later wants to apply for a personal loan, the fintech app may use a data aggregator to highlight certain credit options that the customer could qualify for. While the data aggregator may rely on publicly available data, it may be able to draw insights that serve as a proxy for sensitive information.

Exceptions to Bank CIP Requirements

Typically, a bank must obtain CIP information from the customer except with respect to credit card accounts, where banks are allowed to obtain such information "from a third-party source prior to extending credit to the customer." (See 31 C.F.R. §1020.220(a)(2)(i)(C).) The BSA (as amended by Section 326 of the USA PATRIOT Act) provides financial agencies the authority to exempt financial institutions from these regulations.

In June 2025, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and FinCEN jointly issued an order that would exempt banks from needing to directly obtain TINs from customers. Instead, they could "use an alternative collection method to obtain TIN information from a third-party source rather than the customer." In July 2025, the Federal Reserve joined the other regulators in issuing a similar exemption order.

These agencies believe that the "importance of collecting TIN information from the customer rather than through another method for identification and verification purposes has lessened … particularly in light of the availability of new methods that a bank can use alongside TIN information to form a reasonable belief that the bank knows the true identity of each customer."

Relevant Policy Issues

Several questions arise over how or whether the layer of technology that sits between a fintech and a bank makes it easier or more difficult for the bank to comply with various laws. For example:

- Can a bank effectively verify the identity of a potential customer when there is no in-person interaction?
- Can the bank rely on the transmission of information through a fintech app?
- Is the technology that connects the bank to the fintech secure enough to adequately safeguard the customers' NPI?
- Can the bank and its regulators examine the operations of the partnership?

Privacy concerns are elevated when sensitive information is used, and the bank account initiation process is one where significant NPI can be exposed. Further, data privacy regulations under GLBA only apply to "customers" and not "consumers"—this distinction is potentially important in protecting the flow of information at account opening.

The statutory and regulatory language in the implementation of Title V of GLBA suggests that the data privacy and safeguard provisions apply only to a customer, defined as a "consumer who has a customer relationship" with the financial institution. According to Title 12, Section 1016.3, of the *Code of Federal Regulation*, this definition does not appear to include the consumer onboarding process.

To the extent this is true, the potential gap in the regulatory framework could mean that a consumer who relies on fintech enterprises to enter the banking system could be exposed to vulnerabilities in the security of consumer NPI.

Andrew P. Scott, Specialist in Financial Economics

IF13168

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.