Privacy

Ryan T. Miller | rmiller@aba.com | 202-663-7675 December 2025

Issue Update

Banks are subject to a variety of federal laws that govern the ways consumer personal information can be collected, used, and shared. There are also notice requirements and certain policies and procedures that must be in place. These include the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act, and CAN-SPAM. In addition, banks may be subject to banking sector-specific or comprehensive privacy laws at the state level. California in particular imposes a number of compliance obligations on banks meeting certain thresholds. Finally, certain international laws such as the European Union's General Data Protection Regulation (GDPR) could apply depending on the bank's particular circumstances.

At a base level, privacy can be understood as the permissible access to and uses of a consumer's personal information, including how and with whom it can be shared. This is distinct but related to information security, which creates safeguards for preserving those permissions. Thus, if privacy is a door, information security is the lock and key.

Many of the federal privacy laws have been on the books for many years. Meanwhile, multiple states have passed generalized privacy laws inspired by the GDPR that create consumer rights to access and delete data held by businesses. These rights often conflict with banks' legal and compliance obligations; fortunately, the state laws have some form of exemption recognizing the GLBA and FCRA protections. Nonetheless, the patchwork of state laws imposes challenges on banks and creates risks.

In addition, privacy issues have increasingly dovetailed with other topics, such as Artificial Intelligence, Section 1033 / Data Aggregation, and data governance. Data breaches, which can put millions of consumers at risk, are also tied to privacy considerations. Banks can no longer think of privacy as an ancillary issue.

Why It Matters

Banks' most important currency is trust. Financial information is among the most sensitive types of data, and consumers need to feel comfortable with what banks collect, how they use it, with whom it is shared, and why. Policymakers are increasingly looking to privacy as a concept linking several disparate topics and there is growing momentum for addressing it at the federal level in reaction to a critical mass of state activity. Congressional, CFPB, and prudential agency activity has the potential to significantly impact bank operations, especially if data access or deletion rights come into scope.

Recommended Action Items

- **Apply robust data security and privacy standards to all entities that handle sensitive personal financial information.** Stopping data breaches is critical for consumers, and also important to banks who often have the closest relationship to those affected. Data breaches impose significant costs on banks of all sizes because our first priority is to protect consumers and make them whole.
- **Urge Congress to create a comprehensive privacy law with strong preemptions and an entity-level GLBA exemption.** As banks already have a strong federal framework (reinforced by supervision), financial institutions, their affiliates, or data subject to the GLBA should be exempt from any new law.

Ryan T. Miller | rmiller@aba.com | 202-663-7675

- **Encourage Congress to take care with any GLBA updates.** The law generally works well and Congress must be thoughtful with any amendments.