Protecting Privacy and Helping Homeowners

State data protection Bills Must Not Unintentionally Impede Homeownership

FAQs

What is the GLBA?

The GLBA, or Gramm-Leach-Bliley Act, is federal law that established several important privacy and data security requirements for financial institutions, including:

- The *Safeguards Rule* under the jurisdiction of the FTC requires the implementation of written security measures to keep customer information secure. Safeguards must be customized to the institution's size, complexity, and the sensitivity of customer information handled. Institutions must designate an employee to manage their safeguards program, conduct risk analysis, and monitor and update the program in response to changing business needs and risks.
- The *Financial Privacy Rule* under the jurisdiction of the FTC requires financial institutions to provide a privacy notice to their customers at the beginning of the relationship explaining what data they collect, how it is used, if it is shared with unaffiliated third parties, and how it will be protected. It also mandates that consumers be provided with an option to op-out of the disclosure of their nonpublic personal information to unaffiliated third parties.
- The *Pretexting Prohibition* under the jurisdiction of the FTC prohibits a financial institution from gaining access to personal nonpublic information without proper authority to do so, or through false pretenses.

Does GLBA apply to state licensed financial institutions?

Yes, the act covers ALL financial institutions engaged in financial activities.

Who does the GLBA cover?

The GLBA covers particular entities. Therefore, subsequent privacy acts that have an entity level GLBA exemption would safeguard those institutions that are already subject to the GLBA. This is different from the California Consumer Protection Act (CCPA), which creates a data level exemption for information that is covered by the GLBA. Therefore, under the CCPA institutions are not fully exempt and still must make sure they are complying with both statutes individually.

The entities that GLBA applies to are *financial institutions*, a term defined as any business that is "significantly engaged" in "financial activities." The GLBA uses the definition of "financial activities" found in section 4(k) of the Bank Holding Company Act, which includes most financial products or services., including:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders
- Providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors
- Brokering loans
- Servicing loans
- Debt collecting
- Providing real estate settlement services

What does "significantly engaged" mean as defined in GLBA?

The determination of whether a business is "significantly engaged" in financial activities depends on the business's unique facts and circumstances. In making this assessment, the existence of a formal arrangement and the frequency of the financial activities are two particularly important factors to consider. Some examples of businesses that are significantly engaged in financial activities include:

- Bank and nonbank mortgage lenders
- Mortgage brokers
- Personal property or real estate appraisers
- Personal property or real estate appraisers
- Professional tax preparers, and
- Courier services
- Financial counselors

What does the GLBA protect?

The GLBA protects information from a "consumer" that is "nonpublic personal information." An individual is a "consumer" if they obtain, or previously obtained, a financial product or service to be used primarily for personal, family, or household purposes. "Nonpublic personal information" is "personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution." The GLBA does not cover information that is generally made lawfully available to the public and that the individual can direct that it not be made public and has not done so. The Federal Trade Commission's website provides the following helpful examples of nonpublic personal information:

- *any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);*

- *any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or*
- *any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).*

(See https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#obligations.)

Who does the GLBA protect?

The GLBA's rules, the Safeguards Rule and the Financial Privacy Rule, protect "consumers" and "customers." An individual is a "consumer" if they obtain, or previously obtained, a financial product or service to be used primarily for personal, family, or household purposes. A business client (e.g. corporation, partnership, trust, etc.), or an individual client who engages a financial institution for a commercial purpose, is not a "consumer" and would not be covered by the Safeguards Rule and the Financial Privacy Rule.

A "customer" is a type of consumer with a continuing relationship with the financial institution. In determining whether a consumer qualifies as a customer, one must assess the nature of the relationship. For example, an individual who uses a credit union's ATM, but is not a member of that credit union, is a consumer of the credit union, but not the credit union's customer.

The FTC has issued special rules for certain multi-party transactions. For lending transactions involving lender, borrower, and loan servicer, the FTC's website explains:

> "*A financial institution establishes a customer relationship with an individual when it originates a loan. If the financial institution sells the loan but maintains the servicing rights, it continues to have a customer relationship with the individual. If the financial institution transfers the servicing rights but retains an ownership interest in the loan, the individual is a "consumer" of that institution and a "customer" of the institution with the servicing rights. If other institutions hold an ownership interest in the loan (but not the servicing rights), the individual is their consumer, too.*"
>
> *(See* https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#obligations.)

What are the GLBA's requirements?

Safeguards Rule: Under the Safeguards Rule, financial institutions must adopt an information security program to protect customer information. To comply, each

financial institution must implement a written information security program that's tailored to the institution's size, complexity, nature of activities, and the sensitivity of customer information handled. Additionally, they must:

- Designate an employee to coordinate the information security program
- Identify and assess internal and external information security risks
- Regularly assess the effectiveness of safeguards through monitoring and testing
- Select service providers with adequate safeguards and oversee their compliance with safeguards
- Evaluate and adjust the security program as needed

Financial Privacy Rule: The Financial Privacy Rule requires financial institutions to provide customers with privacy notices when the customer relationship is established and annually thereafter. The privacy notice must explain how customer's nonpublic information will be collected, used, and whether it will be shared with nonaffiliated third parties. If nonpublic information will be shared, the notice must also inform the customer of their right to opt-out.

Before sharing nonpublic information with nonaffiliated third parties, financial institutions must also provide privacy notices to consumers who are not customers, which may include former customers. While these notices must also provide the recipient with reasonable opportunity to opt-out of information sharing, there are generally less requirements for notices to non-customer consumers (e.g. short-form notice, no annual delivery requirement).

Who is responsible for enforcing the GLBA?

GLBA enforcement authority lies with the FTC for non-banking financial institutions, and with various federal financial regulators for banking institutions, including:

- The Federal Reserve Board
- Office of Thrift Supervision
- Office of the Comptroller of the Currency
- Federal Deposit Insurance Corporation
- National Credit Union Administration
- Securities and Exchange Commission
- Commodity Futures Trading Commission

Additionally, states are responsible for enforcing the law with respect to insurance providers.

Have any other states adopted this language or anything like it into their laws?

Yes, Nevada recently adopted a privacy law that gives consumers the right to direct businesses not to sell their personal information. The Nevada law applies to anyone who, for commercial purposes:

- owns or operates an internet website or online service;
- that collects and maintains covered information from consumers; and
- purposefully avails itself of the privilege of conducting activities in Nevada.

The type of information covered includes any data that is gathered and maintained by an operator via website or online service. This would include information such as an email address, name, telephone number, social security number, physical address, any other information concerning a person collected and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable. Significantly, Nevada included a Gramm-Leach-Bliley entity exemption in light of the significant federal data protection framework described above. Nevada therefore departs from the language used by California in the CCPA, as that legislation contains a data level exemption that doesn't cover GLBA entities in full.

Along with Nevada, other states, including Massachusetts, New Jersey, New York, Maryland, North Dakota, and Hawaii are considering draft privacy legislation.