

Frequently Asked Questions

1. Does Gramm-Leach-Bliley (GLB) apply to my company?

GLB applies to "financial institutions," but financial institution is so broadly defined that it includes not just banks, credit unions, and securities brokers, but also real estate appraisers, insurance companies, automobile leasing companies, companies that operate travel agencies in connection with financial services, retailers that issue their own credit cards directly to consumers, and any other entity that is "significantly involved in financial activities."

2. When do the GLB regulations take effect?

The GLB regulations went into effect on November 13, 2000, but companies have until July 1, 2001, to come into full compliance. Seven federal agencies issued regulations implementing the privacy provisions of the Act, but we are primarily concerned here with the rules put out by the Federal Trade Commission.

3. We are complying with The DMA's Privacy Promise; do we have to follow the GLB rules, too?

Yes. Although there are similarities between the GLB regulations and the Privacy Promise, the GLB rules are law and the Privacy Promise is not, and in some areas the GLB rules require more than the Privacy Promise.

4. WHAT DOES MY COMPANY HAVE TO DO TO COMPLY?

Before you can share "non-public personal information" (NPPI) with anybody other than affiliates, you must provide the consumer with detailed notice (see "Privacy Notices" below) and the opportunity to say "no" (opt out).

NPPI is defined as personally identifiable financial information resulting from any transaction with the consumer or any service performed for the consumer. It even includes a simple list of the names and addresses of a financial institution's customers. More specifically, NPPI includes:

- information that a consumer provides on an application to obtain a loan, credit card, or other financial product or service;
- account balance information, payment history, and credit or debit card purchase history;
- any information about a consumer if it reveals that the individual is or has been a customer of the financial institution;
- any information that a consumer provides in connection with the collection or servicing of a credit account.

NPPI does not include publicly available information or consumer lists put together without using any NPPI.

An affiliate is a company that is controlled by another company. Control of a company is defined as:

- the power to vote 25 percent or more of the stock;
- the ability to control the election of a majority of the company directors; or
- the power to exercise a controlling influence over the management or policies of the company.

5. Are there any exceptions to the ban on disclosure of account numbers to nonaffiliated third parties for marketing purposes?

Yes. If a customer chooses to participate in a private label credit card program (such as a Wal-Mart Visa), the merchant and the financial institution can share the consumer's account number if the consumer is told upfront who the participants in the private label credit card are.

The rules also allow disclosures of account numbers to agents or service providers (such as telemarketing firms) for the purpose of marketing the financial institution's own products or services, as long as the agent or service provider is not allowed to debit the consumer's account without the consumer's consent.

6. Does my company have to give everybody we do business with the same kind of notice and opt out?

No. The rules make a distinction between a "consumer" and a "customer". Generally, a "consumer" is someone who has only a brief relationship with your company, such as applying for a loan but not taking it out. A "customer", on the other hand, has an on-going relationship, such as establishing an account or actually taking out a loan. Isolated transactions in which a financial institution sells the consumer airline tickets, travel insurance, or traveler's checks, or the consumer purchases checks for a personal account from a financial institution do not, without further contact, establish a "customer" relationship.

This difference matters because GLB regulations require companies to provide "consumers" with one upfront notice if they plan to share the consumer's NPPI with an unaffiliated third party, but "customers" must be provided with information on the company's privacy policy when the customer relationship is established and annually thereafter.

7. What information needs to be included in the privacy notice?

The following nine items must be included in the privacy notice:

1. Categories of personal information your company collects;
2. Categories of personal information you disclose;
3. Categories of affiliates and nonaffiliated third parties to whom you disclose the information;
4. An explanation of the right to opt out of disclosures to nonaffiliated third parties;
5. A description of the kind of disclosures to nonaffiliated parties that are exceptions to the rules and don't give the consumer the right to opt out.
6. An explanation of the ability to opt out of disclosures of information among affiliates under the Fair Credit Reporting Act (FCRA);
7. If your company discloses information to third parties (such as telemarketing agencies) to conduct marketing campaigns, etc., on your behalf, you must include a separate statement of the categories of information disclosed and the categories of third parties to whom the information will be disclosed;
8. A description of your confidentiality and security policies and practices; and
9. Categories of personal information about former customers that you disclose and to whom you disclose such information.

8. When does my company have to deliver the notice to the consumer?

You are required to deliver both an initial notice and, in the case of an ongoing "customer" relationship, annual notices.

The initial notice needs to be delivered at a "meaningful time" for both "consumers" and "customers". For consumers, the initial notice must be delivered before your company discloses any personal information about the consumer to a non-affiliated third party. If your company does not disclose any personal information about a consumer (except under the exception described in #5), you don't have to provide an initial notice. You must deliver the initial notice to customers when you establish a customer relationship (for example, when a consumer opens a credit card account or buys insurance) and at least once a year as long as the customer relationship lasts.

9. How does my company have to deliver the notice?

Notices must be provided in writing or, if the consumer agrees, electronically. You CANNOT provide the notice solely by an oral explanation, either in person or over the telephone. You can hand a printed copy of the notice to the consumer or mail it by either First-Class or Standard (A) mail. If you mail the notice, you must give the consumer a reasonable amount of time to opt out (see "Consumer Opt-Out" below); if you use Standard (A) mail rather than First-Class, you will have to allow additional time for an opt-out.

Alternatively, you can provide the privacy notice by e-mail if the consumer obtains his or her financial products or services electronically. If the consumer conducts transactions almost entirely at your Web site, you can satisfy the GLB notice requirements by "clearly and conspicuously" posting a privacy notice at your Web site and requiring consumers to acknowledge receipt of the notice before you provide them with any financial product or service.

In the case of annual privacy notices for long-term customers, if the customer uses the financial institution's Web site to access financial products and services and has agreed to accept notice on the Web site, you can satisfy the annual notice requirements by posting a privacy notice describing your current privacy practices and policies in a "clear and conspicuous" manner on your Web site. "Clear and conspicuous" means you must design your Web site so that the notice or a clear link to it cannot be overlooked.

10. Do the GLB notices need to be stand-alone documents or can they be combined with other information or material?

You are allowed to combine the notices with other information provided that, like the Web site requirements, the notice is "clear and conspicuous", which means you should make it stand out with different fonts, shading, etc.

11. Do I ever have to provide a revised privacy notice?

If you start doing things that weren't mentioned in your original privacy notice, including collecting a new category of personal information or disclosing information to a new category of nonaffiliated third party, you might have to distribute a revised privacy notice before you disclose any personal information.

12. When do I have to give customers the right to opt out?

You must provide a "reasonable opportunity to opt out" before you disclose personal information to nonaffiliated third parties. This obligation continues throughout your

relationship with a customer. If you send the opt-out notice by mail, the customer must have at least 30 days to request the opt-out after the notice is sent.

13. What are acceptable methods for providing the consumer with the opportunity to opt out?

The rules allow you to use any of the methods listed below, but one thing you can't do is make the customer write a letter.

- Designate check-off boxes in a prominent position on the relevant forms with the opt-out notice;
- Include a reply form that provides the address to which the form should be mailed;
- Provide an electronic means to opt out, such as a form that can be sent via e-mail or an opt-out procedure at your Web site;
- Provide a toll-free number that consumers can call. For example, your notice could state that "if you prefer that we not disclose personal information about you to third parties, you may call the following toll-free number: 800-_____."

14. Are there any exceptions to the notice and opt-out requirements?

You are allowed to share personal information (other than customer account numbers) without offering an opt-out with companies that run marketing campaigns for you or companies with whom you have joint marketing agreements. However, you must notify the customer that you are making the disclosures, and you must have a contract with the other company that requires it to maintain the confidentiality of the information, using it only to carry out the marketing campaign for which you supplied the information. As noted in #5 above, there is a general prohibition on the disclosure of account numbers for marketing purposes.

15. Under what other circumstances are notice and opt-out not required?

There are a series of exceptions under which notice and opt-out are not required prior to sharing personal information with nonaffiliated third parties, including:

- where the disclosure is necessary to process or service a transaction;
- to protect record security and confidentiality;
- to provide information to legal counsel and to prove that the company is complying with industry standards;
- to respond to requests from regulators, self-regulatory organizations, and law enforcement;
- to report a customer's activities to a credit bureau;
- to protect against fraud;
- to individuals or businesses with a legal interest relating to the consumer;
- in connection with a proposed or actual merger or acquisition;
- to comply with laws and legal process.

16. The rules also apply to companies such as marketers, data processors, and consumer reporting agencies that sell information, if they receive personal information from financial institutions with whom they are not affiliated. How do the regulations limit the reuse and redisclosure of personal information by these third-party companies?

If the third party receives the personal information from a financial institution under one of the exceptions previously mentioned, the recipient may reuse or redisclose the

personal information only as necessary to carry out the activity covered by the exception under which it received the information.

If the third party receives the personal information from a financial institution outside of one of the exceptions, the recipient "steps into the shoes" of the financial institution and may reuse or redisclose the information only in accordance with the privacy policies and consumer opt-out choices of the company from which the information was obtained.

17. Who will enforce the rules?

The rules will be enforced by the various federal agencies that have jurisdiction over financial institutions (and companies considered financial institutions) covered by GLB (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Securities and Exchange Commission, and the National Credit Union Administration), the State insurance authorities, and the Federal Trade Commission (FTC). Most direct marketers would almost certainly fall under FTC jurisdiction.

18. Can consumers sue for violations of the GLB Act or rules?

No. Neither the original law nor the regulations contain a private cause of action provision that would allow consumers to bring a suit for violations of the GLB Act's requirements. Enforcement is left to the Federal agencies and the State insurance agencies that have jurisdiction over financial institutions covered by the rules.

19. What role do state governments have in connection with the new law?

The GLB Act preempts only "inconsistent" state laws. It sets a floor, not a ceiling, over which states are free to pass stricter laws.

20. What should you do to prepare for GLB's effective date?

To prepare for the effective date of the GLB Act you should, at a minimum, do the following:

- assess what financial services and products you provide, others provide on your behalf, and what you provide on behalf of others;
- evaluate your company's practices in sharing personal information;
- draft or revise your company's privacy policy to include the information required under the GLB;
- draft mandatory disclosures for your company's privacy notice;
- establish a method to track and honor opt-out requests;
- ensure compliance with relevant state laws; and
- revise language in employment, service, joint venture, and mergers and acquisitions agreements to conform to GLB requirements.

21. Do the regulations distinguish between data collected prior to the effective date and data collected after the effective date?

No. Before July 1, 2001, all companies covered by the rules must provide their existing customers with both a privacy notice and a reasonable opportunity to opt out of the disclosure of their personal information regardless of when it was collected.

The rules do distinguish between existing customers and former customers. Specifically, initial notices do not have to be given to customers whose relationships have terminated

prior to July 1, 2001 (if an account is inactive on July 1, 2001, then no initial notice will be required). However, because the former customers would remain "consumers," you would have to provide a privacy and opt-out notice to them if you subsequently decided to disclose their personal information (except under one of the exceptions previously described).