

The Gramm-Leach Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the [Financial Privacy Rule](#) and the [Safeguards Rule](#). These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. For a summary overview of the Financial Privacy Rule, see:

<http://www.ftc.gov/bcp/online/pubs/buspubs/glbshort.shtm>.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

The Pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."

Under federal law — the Gramm-Leach-Bliley Act — it's illegal for anyone to:

- Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents.
- Pretext for sensitive consumer information.

The GLBA has provisions that require the financial institution to take all precautions necessary to protect and defend the consumer and associated nonpublic information. Pretexting is illegal and punishable by law beyond any recognition by the GLBA

Enforcement.

The FTC, the federal banking agencies, (1) other federal regulatory authorities, (2) and state insurance authorities enforce the GLB Act. Each agency has issued substantially similar rules implementing GLB's privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance providers. The FTC has jurisdiction over any financial institution or other person not regulated by other government agencies.

The FTC may bring enforcement actions for violations of the Privacy Rule. The FTC can bring actions to enforce the Privacy Rule in federal district court, where it may seek the full scope of injunctive and ancillary equitable relief. The FTC also has authority under Section 5 of the FTC Act to examine privacy policies and practices for deception and unfairness.

Footnotes:

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

Does the Privacy Rule apply to me?

The Privacy Rule applies to companies who:

- Extend credit to someone (for example, through a retail installment contract) in connection with the purchase of a product for personal, family, or household use;
- Arrange for someone to finance or lease for personal, family, or household use; or
- Provide financial advice or counseling to individuals.

If you engage in these activities, any personal information that you collect to provide these services is covered by the Privacy Rule. Examples of personal information include someone's name, address, phone number, or other information that could be used to identify them individually. The Privacy Rule applies if you collect personal information about someone in connection with the potential financing or leasing of a product, even if that person does not fill out a formal application. The Privacy Rule does not apply to you if a person buys a product with cash or arranges financing on their own through another lender.

Consumer/Client Privacy Rights

Under the *GLBA*, financial institutions must provide their clients a privacy notice that explains what information the company gathers about the client, where this information is shared, and how the company safeguards that information. This privacy notice must be given to the client prior to entering into an agreement to do business. There are exceptions to this when the client accepts a

delayed receipt of the notice in order to complete a transaction on a timely basis. This has been somewhat mitigated due to online acknowledgement agreements requiring the client to read or scroll through the notice and check a box to accept terms.

The privacy notice must also explain to the customer the opportunity to 'opt-out'. Opting out means that the client can say "no" to allowing their information to be shared with affiliated parties. The *Fair Credit Reporting Act* is responsible for the 'opt-out' opportunity, but the privacy notice must inform the customer of this right under the GLBA. The client cannot opt-out of:

- information shared with those providing priority service to the financial institution
- marketing of products or services for the financial institution
- when the information is deemed legally required.

GLBA Enforced

Violation of the *GLBA* may result in a civil action brought by the United States Attorney General. The penalties, as amended under the [Financial Institution Privacy Protection Act](#) of 2003 (108th CONGRESS - 1st Session - S. 1458; To amend the *Gramm-Leach-Bliley Act* to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes.

In The Senate of the United States, July 25 (legislative day, JULY 21), 2003) include, Section 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6805) is amended by adding at the end the following:

“(e) CIVIL PENALTIES- The Attorney General of the United States may bring a civil action in the appropriate district court of the United States against any financial institution that engages in conduct constituting a violation of this title, and, upon proof of such violation--

(1) The financial institution shall be subject to a civil penalty of not more than \$100,000 for each such violation; and

(2) the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation.’

EXAMPLE:

By Robert Westervelt, News Editor, 31 Oct 2006 | SearchSecurity.com

The costs associated with [high-profile data breaches](#) are skyrocketing, according to a survey of companies that recently experienced customer data loss.

Data breaches cost companies an average of \$182 per compromised record, a 31% increase over 2005, according to the survey conducted by the Elk Rapids, Mich.-based Ponemon Institute.

Ponemon studied 31 companies that experienced a data breach. The total costs for each loss ranged from less than \$1 million to more than \$22 million, according to the 2006 findings.

Costs resulting from a data breach can include printing and postage of notification letters, hiring a law firm to address legal issues, offering credit monitoring subscriptions to customers, implementing a customer support hotline and contract call center, as well as customer defections.

IT had no direct costs other than to put subsequent preventative measures in place, the survey said. The costs were borne primarily by marketing to avoid customer turnover and customer support.

The Federal Trade Commission (FTC) uses an extremely broad definition of the term "financial institution" for the purposes of GLB compliance. In fact, almost any organization that works with people's money is considered a financial institution. Some inclusions are obvious – nobody would question whether a bank, credit union or brokerage would need to comply with GLB. However, there are many less obvious inclusions as well. Some examples from the FTC include:

- Preparers of income tax returns
- Consumer credit reporting agencies and credit counseling services
- Real estate transaction settlement services
- Debt collection agencies

In addition to the direct providers of those services, **any organization that receives data from those providers must also comply with GLB requirements.** For more detailed listings of the types of activities covered under the Act, [consult the FTC Web site.](#)

Do GLB's provisions apply to your business?

What does that mean to you as an information security professional?

There are three provisions of GLB that restrict the collection and use of consumer data. The first two, the Financial Privacy Rule and the Pretexting Provisions, detail responsible business practices and are mainly outside the scope of information security duties. The Safeguards Rule, which went into effect during 2003, requires that included institutions take proactive steps to ensure the security of customer information. At a minimum, institutions must:

- Appoint an individual or group to bear specific responsibility for GLB compliance.
- Identify risks to customer information and assess existing safeguards.
- Implement safeguards that are needed to fill any gaps.
- Monitor the effectiveness of all safeguards.
- Ensure service providers are capable of meeting GLB requirements.
- Adjust the organization's security program as necessary when circumstances change.

[Compliance](#) with the Gramm-Leach-Bliley Act is a serious matter. Failure to comply has serious consequences for individuals and organizations found guilty. If GLB applies to your organization, you should definitely consult legal counsel to determine any steps that may be necessary to bring your activities into compliance with the law.