Gramm-Leach-Bliley Act

From Wikipedia, the free encyclopedia

The **Gramm-Leach-Bliley Act**, also known as the **Gramm-Leach-Bliley Financial Services Modernization Act**, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999), is an Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The Glass-Steagall Act prohibited a bank from offering investment, commercial banking, and insurance services. The Gramm-Leach-Bliley Act (GLBA) allowed investment and commercial banks to consolidate, for example Citigroup and Salomon Brothers. The combined industry is known as the financial services industry.

The Act was desired by many of the largest banks, brokerages, and insurance companies in the country at the time. The justification was that people usually put more money in investments in a good economy, but when it turns bad, they put their money into savings accounts. With the new Act, they would do both with the same company, so the company would be doing well in all economic times. This has to some extent proven out.

Prior to the passage of the Act, most financial services companies were doing this anyway. On the retail/consumer side, a bank called Norwest led the charge in offering all types of financial services products in 1986. Also at the time American Express attempted to own almost every genre of financial business (although there was little synergy between them). Things culminated in 1997 when Travelers, a financial services company with everything but a retail/commercial bank, bought out Citibank, creating the largest and most profitable company in the world. At the time this was technically illegal, and was a large impetus for the passage of the Gramm-Leach-Bliley.

Also prior to the passage of the Act, there were many relaxations to the Glass-Steagall Act. For example, a few years before, Commercial Banks were allowed to get into investment banking, and before that banks were also allowed to get into stock and insurance brokerage. The only main operation they weren't allowed to do was insurance underwriting (something rarely done by banks even after the passage of the act).

Since the passage of the GLBA, much consolidation has occurred in the financial services industry, but not as much as some expected. Retail banks for example, do not tend to buy insurance underwriters, since they expect they can make more money selling other companies insurance products in their branches (this is called insurance brokerage). Many other retail banks have been slow to adopt investments and insurance products, and to package those products in a convincing way. Brokerage companies have had a hard time getting into banking, because they do not have a large branch and backshop footprint. Banks have recently tended to buy other banks, such as the recent Bank of America and Fleet Boston merger, yet they have had less success integrating with investment and insurance companies. Many banks have expanded into investment banking, but have found it hard to package it with their banking services, without resorting to questionable tie-ins which caused scandals at Smith Barney.

Senator Phil Gramm led the Senate Banking Committee which sponsored the Act; he later joined UBS Warburg, at the time the investment banking arm of the largest Swiss bank.

Some restrictions remain to provide some amount of separation between the investment and commercial banking operations of a company. For example, the commercial banks aren't allowed to pay commission to their employees who convince customers to also use some investment services. They are only allowed to pay them a small fee for simply setting up appointments to meet with a financial advisor. Much of the debate about financial privacy is specifically centered around allowing or preventing the banking brokerage and insurances divisions of a company from working together.

In terms of compliance, the key rules under the act include *The Financial Privacy Rule* which governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information. *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.

Privacy

- GLBA compliance is not voluntary; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity
- Major Components put into place to govern the collection, disclosure, and protection of consumers' nonpublic personal information; or personally identifiable information:
  - #Financial Privacy Rule
  - #Safeguards Rule
  - #Pretexting Protection

Financial Privacy Rule

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. § 6801 through 15 U.S.C. § 6809)

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt-out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement. In summary, the financial privacy rule provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer's personal nonpublic information.

Safeguards Rule

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. § 6801 through 15 U.S.C. § 6809)

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule also applies to information of those no longer consumers of the financial institution.) This plan must include: (1)denoting at least one employee to manage the safeguards, (2)constructing a thorough risk management on each department handling the nonpublic information, (3)develop, monitor, and test a program to secure the information, and (4)change the safeguards as needed with the changes in how information is collected, stored, and used. This rule is intended to do what most businesses ought already to be doing; protect their clients. The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the GLBA.

Pretexting Protection

(Subtitle B: Fraudulent Access to Financial Information, codified at 15 U.S.C. § 6821 through 15 U.S.C. § 6827)

Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (i.e., using a "phony" website or email to collect data). 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.

Financial Institutions Defined

The GLBA defines “financial institutions” as: …”companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission (FTC) has jurisdiction over financial institutions similar to, and including, these: (1)non-bank mortgage lenders, (2)loan brokers, (3)some financial or investment advisers, (4)debt collectors, (5)tax return preparers, (6)banks, and (7)real estate settlement service providers. These companies must also be considered significantly engaged in the financial service or production that defines them as a “financial institution”.

Insurance has jurisdiction first by the state, provided the state law at minimum complies with the GLBA. State law can require greater compliance, but not less than what is otherwise required by the GLBA.

Consumer vs. Customer Defined

The Gramm-Leach-Bliley Act defines a ‘consumer’ as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." (See 15 U.S.C. § 6809(9).} A ‘customer’ is a consumer that has developed a relationship with privacy rights protected under the GLBA. A ‘customer’ is not someone using an automated teller machine (ATM) or having a check cashed at a cash advance business. These are not ongoing relationships like a ‘customer’ might have; i.e. a mortgage loan, tax advising, or credit financing. A business is not an individual with personal nonpublic information, so a business cannot be a customer under the GLBA. A business, however, may be liable for compliance to the GLBA depending upon the type of business and the activities utilizing individual’s personal nonpublic information.

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 consumer of 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 consumer 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,

- ”the financial institution shall be subject to a civil penalty of not more than $100,000 for each such violation”
- “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”.

History

For more about the history of financial privacy governances and the GLBA, see “History of the GLBA” at http://www.epic.org/privacy/glba.

FYI: Websites for Compliance Information

- “Disclosure of Nonpublic Personal Information” - http://www.ftc.gov/privacy/glbact/glbsub1.htm

- “Financial Institutions and Customer Data: Complying with the Safeguards Rule” - http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm

- “Gramm-Leach-Bliley Act Compliance Is Now Required With Every Search For Non-Public Information” - http://www.aaronspi.com/GLB.htm

FYI: Websites for Consumer/Client Rights Information

- “Disclosure of Nonpublic Personal Information” - http://www.ftc.gov/privacy/glbact/glbsub1.htm

- “What Can You Do To Protect Your Privacy” - http://www.epic.org/privacy/glba/#reduce

- “Privacy Choices for Your Personal Financial Information”- http://www.ftc.gov/bcp/conline/pubs/credit/privchoices.htm

- “Pretexting: Your Personal Information Revealed” - http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm

References

- Financial Privacy: The Gramm-Leach Bliley Act, Federal Trade Commission, 1999 - http://www.ftc.gov/privacy/glbact

- Gramm-Leach-Bliley Act,15 USC, Subchapter I, Sec. 6801-6809, Disclosure of Nonpublic Personal Information, 1999 - http://www.ftc.gov/privacy/glbact/glbsub1.htm

- Gramm-Leach-Bliley and You, Chapple, Mike, November 18, 2003 - http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci937043,00.html

- Gramm-Leach-Bliley Act Financial Privacy Provisions:The Federal Government Imposes Broad Requirements to Address Consumer Privacy Concerns, Ledig, Robert H. - http://www.ffhsj.com/bancmail/bmarts/ecdp_art.htm

- The Gramm-Leach-Bliley Act: The Financial Privacy Rule, Federal Trade Commission - http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html

- In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, Federal Trade Commission - http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

- The Gramm-Leach-Bliley Act – "History of the GLBA", Electronic Privacy Information Center - http://www.epic.org/privacy/glba/#reduce

- 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 - http://thomas.loc.gov/cgi-bin/query/z?c108:S.1458.IS: