

©Stephen Morris
Privacy & Security
March 2008

Privacy in the financial sector under Gramm-Leach-Bliley (1999)

Information that many would consider private – including bank balances and account numbers – is regularly bought and sold by banks, credit card companies, and other financial institutions. The Gramm-Leach-Bliley Act (GLBA), which is also known as the Financial Services Modernization Act of 1999, provides limited privacy protections against the sale of private financial information.

The GLBA primarily sought to “modernize” financial services – that is, end regulations that prevented the merger of banks, stock brokerage companies, and insurance companies. The removal of these regulations, however, raised significant risks that these new financial institutions would have access to an incredible amount of personal information, with no restrictions upon its use. Prior to GLBA, the insurance company that maintained health records was distinct from the bank that mortgaged houses and the stockbroker that traded stocks. Once these companies were permitted to merge, however, they would have the ability to consolidate, analyze and sell the personal details of their customers' lives. Because of these risks, the GLBA included three requirements to protect the personal data of individuals: First, banks, brokerage companies, and insurance companies must securely store personal financial information. Second, they must advise customers of their policies on sharing of personal financial information. Third, they must give consumers the option to opt-out of some sharing of personal financial information. This paper will demonstrate the significance of GLBA for its privacy regulations.

Legislative history

The history of the GLBA has its roots in the separation of banks, brokerage companies, and insurance companies. As a result of the financial failures of the Great Depression, Congress, in 1933, passed the Glass-Steagall Act prohibiting national and state banks from affiliating with securities companies. In 1956, Congress passed the Bank Holding Company Act that prohibited a bank from controlling a non-bank company. In 1982 Congress amended the Bank Holding Act to further forbid banks from conducting general insurance underwriting or agency activities. This changed, however, in 1999, when the GLBA¹ repealed sections of these acts and allowed banks to engage in a wide range of financial services.⁻

The GLBA redesigned the regulatory structure that had been in place since the Great Depression. The regulations adopted in the early 1930s were not part of a "well-considered overall blueprint," but were made in "immediate response to developments and crises as they occurred."⁻ Because the regulatory structure developed in such an ad hoc manner, the GLBA's reforms answer a long-felt need for coherence.

The³ 1920s, marked by a succession of bank failures, culminated in the stock market crash of 1929.⁻ The economic depression that followed led to more market failures, decreased public confidence, and engendered cries for government intervention. In response to these calls for reform, Congress passed the Glass-Steagall Act, directly responding to the belief that the stock market crash resulted from the lack of separation between lending⁴ and underwriting activities that had allowed banks to engage in speculative investments.⁻ Under the Glass-Steagall Act,

Congress separated commercial banking from investment banking, thereby prohibiting commercial banks from underwriting most securities.⁵ With the goal of eliminating conflicts of interest, Congress sought to prevent these firms from engaging in similar activities.

The Glass-Steagall Act, however, was unsuccessful in maintaining these legal barriers. Had it been effective, the Act would have minimized direct competition between commercial banks and securities firms. Instead, by 1990, the largest banks were able to participate in almost all of the securities activities that they had engaged in before the Glass-Steagall Act.⁶

Privacy risks were put onto the agenda by a series of international and domestic events. On the international front, in 1995, the EU issued the Data Protection Directive, which required that international data exchanges using EU citizens' personal data be accorded the same level of protection that their home country would afford them. This meant US companies would have to ensure when they used EU citizens' personal data they provided the same level of protection these citizens were afforded within the EU. The EU was especially concerned with the US government's preference for self-regulatory approaches to privacy and the lack of federal privacy legislation. While the EU-US agreed to a Safe Harbor proposal, which allowed for companies to self-regulate under FTC oversight, financial services industries were not included in the original agreement.⁷

In November 1997, Charter Pacific Bank of Agoura Hills, California sold millions of credit card numbers to an adult website company, which then proceeded to bill customers for access to Internet porn sites and other services they did not request. Some of the customers billed did not even own a computer. The website company had set up numerous merchant accounts under different names to avoid detection. In September 2000, the FTC announced that it has won a \$37.5 million judgment against the website company. While the bank maintained that it did not do anything wrong, it has since then stopped selling credit card numbers to merchants.⁸

In 1998, NationsBank (later merged with Bank of America) was fined millions for securities law violations because it shared customer information with its affiliate subsidiary Nations Securities. The subsidiary then convinced low risk customers to buy high-risk investments. Many NationsBank⁹ customers lost large amounts and many senior citizens lost large amounts of their life savings.¹⁰

In June 1999, the Minnesota Attorney General initiated a lawsuit against U.S. Bankcorp for sharing customer information with third party marketers in violation of its own policies without customer knowledge or authorization.¹¹ The telemarketers then illicitly charged those customers. US Bankcorp eventually settled that case, along with those brought by 39 other state attorneys general. In April 2000, Minnesota settled with the third party telemarketer, Memberworks, that US Bankcorp used. According to Memberworks' SEC filings, 19 out of the 25 largest banks in the US had contracts with it. Other prominent banks, including Chase Manhattan and Citibank, have been involved in schemes where personal account information is sold to telemarketers.

This confluence of international and domestic events prompted Congress to include Title V in its GLBA provisions, which contains limited privacy protections for financial information. The GLBA was introduced in the Senate by Senator Phil Gramm (R-TX) and in the House of Representatives by Representative James Leach (R-IA). It was signed by President Clinton and became law on November 11, 1999.¹²

Information and Privacy Protections under the GLBA

The GLBA's privacy protections only regulate financial institutions – businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing. While the Glass-Steagall Act has been criticized as a knee-jerk reaction to the crises of its time, it is clear that the GLBA is also a response to current trends.¹²—

Since the GLBA fosters the use of information, it was inevitable that privacy advocates would lobby to include reasonable limits on the use and dissemination of such information. After much debate regarding the use of financial information, drafters of the GLBA added in a plethora of privacy provisions. These provisions represent the first piece of federal legislation to establish a minimum federal standard of privacy for financial information.

We live in the “information age.” While information has always had some value, information started accruing real market value with the advent of computer technology. In the 1960s, the federal government and large private corporations used mainframe computers to store records in computerized form.¹³— Even then, these entities realized that this development would improve “operational efficiency.”¹⁴— Using computer technology to better sift through personal financial information has allowed companies to increase efficiency (and profits) by increasing revenues while cutting excess costs. Consequently, reliance on databases in digital form has only increased.

Companies gather personal information in order to make strategic decisions about people.¹⁵— Firms use computerized information to generate profiles that are used to predict response rates to various promotional offers. For example, credit card firms can provide pre-approved credit without exposing themselves to significant default risk because targeted individuals have been selected based on substantial amounts of prescreened information. Similarly, banks can make better lending decisions without having to first establish a long-term relationship with each individual customer.¹⁶— Such ready availability of information not only decreases the cost of doing business, but also increases companies' effectiveness at raising revenues. Furthermore, information is valuable in its own right. Information itself is a product that has monetary value. Some firms that profile their consumers will use the same data to compile marketing lists. These lists are then sold to other merchants to augment traditional sources of income.¹⁷—

Clearly, demand for information is high. And yet, despite this intense demand, supply comes at a relatively cheap price. The costs for collecting, manipulating, storing, and transmitting electronic data are low. The price of computers has declined while advances in technology have significantly improved computing ability to process and store enormous amounts of data. These advances have made information more readily accessible. Databases facilitate rapid searches and organizations can locate a specific entry from volumes of records in fractions of a second. Furthermore, in a networked society, the information in databases can be “seamlessly combined with other data sources to generate ever more comprehensive records of individual attributes and activities.”¹⁸—

This ability to selectively cull and collect information, as well as the capacity to correlate existing information, has been described as effectively being able to “create” new information. As such, personally-identified information is ubiquitous. It is this dissemination of information that has many people concerned about their privacy rights.

The GLBA establishes certain limits on companies' reliance on information. Subtitle A, which addresses the disclosure of customers' nonpublic personal information, contains numerous provisions that require financial institutions to establish limitations governing the disclosure of nonpublic information to nonaffiliated third parties and to provide their customers with a notice

of the company's privacy policy. Protection for this information lies in three sections: (1) section 501 requires institutions to establish a privacy policy, many of them for the first time; (2) section 503 requires that the privacy policies be disclosed at the time of establishing a customer relationship; and (3) section 502 prohibits¹⁹ firms from disclosing information to nonaffiliated third parties, subject to certain exceptions.—

In addressing the dissemination of nonpublic personal information, section 502 is at the heart of the GLBA's privacy provisions. Section 502(b)(1) provides:

A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless —

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form . . . that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.²⁰—

Accordingly, consumers must affirmatively prevent companies from sharing their nonpublic personal information with nonaffiliated firms. If consumers fail to opt-out, their inaction provides firms with an implied consent to share information with any nonaffiliated company.

However, there are many exceptions even to this minor requirement of implied consent. Firms are only required to disclose that information is in fact shared and to enter into confidentiality agreements with third parties in limited circumstances: when companies hire nonaffiliated third parties to perform services, when firms contract with third parties (e.g. a company hires an outside agency to market its own²¹ products or services), and when companies enter into joint agreements to co-offer products.— Additionally, under the section entitled "General Exceptions," firms can share information with nonaffiliates without consent for "a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit" and for "institutional risk control."²²—

Description of privacy regulations

Covered financial institutions, whether they wish to disclose personal information or not, must develop precautions to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such²³ records or information which could result in substantial harm or inconvenience to any customer.—

Financial institutions are also required to provide a notice of their information sharing policies when customers join, and annually thereafter. That notice must inform the consumer of the financial institutions' policies on: disclosing nonpublic personal information (NPI) to affiliates and nonaffiliated third parties, disclosing NPI after the customer relationship is terminated, and protecting NPI. "Nonpublic personal information" means all information on applications to obtain financial services (credit card or loan applications), account histories (bank or credit card) and the fact that an individual is or was a customer. This interpretation of NPI makes names, addresses, telephone numbers, Social Security Numbers and other data subject to the GLBA's data sharing restrictions.

The GLBA gives consumers the right to opt-out from a limited amount of NPI sharing. Specifically, a consumer can direct the financial institution to not share information with unaffiliated companies.

Consumers have no right under the GLBA to stop sharing of NPI among affiliates. An affiliate is any company that controls, is controlled by, or is under common control with another company. The individual consumer has absolutely no control over this kind of "corporate family" trading of personal information.

There are several exemptions under the GLBA that can permit information sharing over the consumer's objection. For instance, if a financial institution wishes to engage the services of a separate company, they can transfer personal information to that company by arguing that the information is necessary to the services that the company will perform. A financial institution can transfer information to a marketing or sales company to sell new products (different stocks) or jointly offered products (co-sponsored credit cards). Once this unaffiliated third party has personal information, they can share it with their own corporate family. However, they themselves cannot likewise transfer the information to further companies through this exemption.

Certain types of "pretexting" were prohibited by the GLBA. Pretexting is the practice of collecting personal information under false pretenses. Pretexters pose as authority figures (law enforcement agents, social workers, potential employers, etc.) and manufacture seductive stories (that the victim is about to receive a sweepstakes award or insurance payment) in order to elicit personal information about the victim. The GLBA prohibits the use of false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution; the use of forged, counterfeit, lost or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution; and asking another person to get someone else's customer information using false, fictitious, or fraudulent documents or forged, counterfeit, lost or stolen documents. —²⁴

Problems with the GLBA

The GLBA places the burden on the individual to protect privacy with an opt-out standard. By doing so, GLBA weakens customer power to control their financial information. The agreement's opt-out provisions do not require institutions to provide a standard of protection for their customers regardless of whether they opt-out of the agreement. This provision is based on the assumption that financial companies will share information unless expressly told not to by their customers and if customers neglect to respond, it gives institutions that freedom to disclose customer nonpublic personal information.

Often, the GLBA notices are confusing and limit the transparency of information practices. GLBA assumes a company will explain a complex set of legal definitions added to numerous exceptions to the law in a way that will allow for an informed choice and in transparent language. There are reservations about a company's desire to do this.

Moreover, according to recent studies, most privacy and opt-out policies are usually convoluted, confusing, and misleading since they are created by entities whose interests are better served when there is no effective notice. GLBA does little to deal with the lack of transparency in the privacy notices themselves. Typical privacy notices do not include any specific information about how the data is actually used. GLBA notices do inform consumers that their personal information will be shared, but they generally do not inform the individual of who will receive the information or the purposes for which it will be used.

The act also fails to enhance consumers' control over affiliate information sharing. Consumers have no opt-out right against affiliate information sharing. In today's world of mega-mergers, a bank may have over one thousand affiliates, some of which may be completely unrelated to financial services. Furthermore, financial institutions can evade opt-out requirements by exploiting the exceptions in the GLBA. The service provider/joint marketing exemption allows financial institutions to share information with non-affiliated third parties despite a consumer's opt-out.

Finally, the GLBA has weak enforcement and compensation mechanisms. GLBA's enforcement mechanisms are inadequate to assure compliance with even existing weak privacy protections. Enforcement rests solely with federal government agencies, leaving the individual no private right of action.

Conclusion

Under the GLBA, companies still have the upper hand in controlling financial information. Many in Congress, however, have already attempted to pass amendments that would provide stronger privacy protection. Yet, the momentum for increased privacy rights may have come to a halt in light of the new public concern over national security. Despite these developments, many still believe that the GLBA did not strike the proper balance between efficiency and privacy. Nevertheless, in a society that values information, any substantial trade-off that leads to decreased efficiency may be difficult to defend.

1 Donna K Peeples, Pamela Stokes, Leon Dube. "Current Issues in Consumer Privacy Policies." *S.A.M. Advanced Management Journal*. Issue 70, no. 2. April 1, 2005. p4-12.

<http://0-www.proquest.com.library.lausys.georgetown.edu/> (accessed March 12, 2008).

2 George G. Kaufman, *The US Financial System: Money, Markets, and Institutions.*, 5th Ed. 1992.

3 Helen M. Burns, *The American Banking Community and New Deal Banking Reforms 1933-1935.* 1974. p 3-6.

4 *Ibid.*, p6.

5 Burns, *op. cit.*, p3.

6 *Ibid.*

7 Jolina C Cuaresma, "The Gramm-Leach-Bliley Act." *Berkeley Technology Law Journal* 17, no. 1.

January 1, 2002. p497-517. <http://0-www.proquest.com.library.lausys.georgetown.edu/> (accessed March 14, 2008).

8 Cuaresma, *op. cit.*

9 *Ibid.*

10 *Ibid.*

11 Gramm-Leach-Bliley Act of 1999. Accessible online at <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00900:%7CTOM:/bss/d106query.html%7C>

12 Peeples, *op. cit.*

13 Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy.* 1995. p69.

14 *Ibid.*

15 James Rule et al., *The Politics of Privacy.* 1980. p154.

16 Fred H. Cate, *Privacy in the Information Age.* 1997. p2.

17 *Ibid.*

[18](#) Cate, *op. cit.*, p4.

[19](#) Gramm-Leach-Bliley Act of 1999, *op. cit.*

[20](#) Gramm-Leach-Bliley Act of 1999, *op. cit.*

[21](#) Cuaresma, *op cit.*

[22](#) *Ibid.*

[23](#) *Ibid.*

[24](#) Cuaresma, *op cit.*