Privacy Protection for Customer Financial Information

M. Maureen Murphy
Legislative Attorney

January 7, 2009

Congressional Research Service
7-5700
www.crs.gov
RS20185

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) (P.L. 106-102) covers financial institutions. It prohibits them from sharing nonpublic personally identifiable customer information with non-affiliated third parties without providing an opportunity to opt out and mandates various privacy policy notices. It requires financial institutions to safeguard the security and confidentiality of customer information. Finally, it delegates rulemaking and enforcement authority to the federal banking and security regulators, the Federal Trade Commission (FTC), and state insurance regulators. P.L. 109-351 requires these regulators to devise a model privacy notice so that consumers may identify and compare information disclosure practices of financial institutions. P.L. 108-159 makes certain Fair Credit Reporting Act (FCRA) preemptions of state law relative to information sharing among affiliates permanent and provides a limited opt-out of affiliate sharing of information for marketing purposes.

It is expected that in the 111th Congress, as in every Congress since 1999, there will be legislative proposals to enhance the protection offered personal financial information. This report will be updated to reflect action on major legislation. For information on other relevant data security issues, including data breach notification, see CRS Report RL33273, *Data Security: Federal Legislative Approaches*, by Gina Marie Stevens, and CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Marie Stevens.

Contents

Contacts

Background

With modern technology's ability to gather and retain data, financial services businesses have increasingly found ways to take advantage of their large reservoirs of customer information. Not only can they serve their customers better by tailoring services and communications to customer preferences, but they can profit from sharing that information with others willing to pay for customer lists or targeted marketing compilations. Although some consumers are pleased with the wider access to information about available services that information sharing among financial services providers offers, others have raised privacy concerns, particularly with respect to secondary usage.

The United States has no general law of financial privacy. The U.S. Constitution, itself, has been held to provide no protection against governmental access to financial information turned over to third parties. *United States v. Miller,* 425 U.S. 435 (1976). This means that although the Fourth Amendment to the United States Constitution requires a search warrant for a law enforcement agent to obtain a person's own copies of financial records, it does not protect the same records when they are held by financial institutions. State constitutions and laws may provide greater protection.

Various federal statutes provide a measure of privacy protection for financial records. The Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422, sets procedures for federal government access to customer financial records held by financial institutions. The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681 to 1681t, establishes standards for collection and permissible purposes for dissemination of data by consumer reporting agencies. It also gives consumers access to their files and the right to correct information therein. The Electronic Funds Transfer Act, 15 U.S.C. §§ 1693a to 1693r, describes the rights and liabilities of consumers using electronic funds transfer systems. Among them is the right to have the financial institution provide consumers with information as to the circumstances under which information concerning their accounts will be disclosed to third parties.

With the passage of the Fair Credit Reporting Act Amendments of 1996, P.L. 104-208, Div. A, Tit. II, Subtitle d, Ch. 1, § 2419, 110 Stat. 3009-452, adding 15 U.S.C.§ 1681t(b)(2), companies may share with other entities certain customer information respecting their transactions and experience with a customer without any notification requirements. Other customer information, such as credit report or application information, may be shared with other companies in the corporate family if the customers are given "clear and conspicuous" notice about the sharing and an opportunity to direct that the information not be shared, that is, an "opt out."

Under section 214 of P.L. 108-159, 117 Stat. 1952, the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), subject to certain exceptions, affiliated companies may not share customer information for marketing solicitations unless the consumer is provided clear and conspicuous notification that the information may be exchanged for such purposes and an opportunity and a simple method to opt out. Among the exceptions are solicitations based on preexisting business relationships; based on current employer's employee benefit plan; in response to a consumer's request or authorization; and as required by state unfair discrimination in insurance laws. The 2003 amendments also require the agencies to conduct regular joint studies of information sharing practices of affiliated companies and make reports to the Congress every three years.

Gramm-Leach-Bliley's Privacy Provisions

Title V of the Gramm-Leach Bliley Act (GLBA) (P.L. 106-102)[1] contains the privacy provisions enacted in conjunction with financial modernization legislation. The legislation requires that federal regulators[2] issue rules that call for financial institutions to establish standards to insure the security and confidentiality of customer records.[3] It prohibits financial institutions[4] from disclosing nonpublic personal information to unaffiliated third parties without providing customers the opportunity to decline to have such information disclosed. Also included are prohibitions on disclosing customer account numbers to unaffiliated third parties for use in telemarketing, direct mail marketing, or other marketing through electronic mail. Under this legislation, financial institutions are required to disclose, initially when a customer relationship is established and annually, thereafter, their privacy policies, including their policies with respect to sharing information with affiliates and non-affiliated third parties. Under section 503(c) of GLBA, as added by section 728 of the Financial Services Relief Act of 2006, P.L. 109-351, the federal functional regulators are required to propose model forms for GLBA privacy notices. On March 29, 2007,[5] the agencies issued a notice proposing a model form and soliciting comments, which are now under review. Final issuance of the forms could be as early as spring 2009.[6]

Regulations implementing GLBA's privacy requirements were published by the banking regulators in the *Federal Register* on June 1, 2000, by the Federal Trade Commission (FTC) on May 24, and by the SEC on June 29 (65 *Fed. Reg.* 35162, 33646, and 40334).[7] They became effective on November 13, 2000.[8] Consumers may opt out at any time. Identity theft and pretext calling guidelines were issued to banks on April 6, 2001.[9] Insurance industry compliance has been handled on a state-by-state basis by the appropriate state authority. The National Association of

---

[1] http://www.congress.gov/cgi-lis/bdquery/R?d106:FLD002:@1(106+102), tit. v, 113 Stat. 1338, 1436. 15 U.S.C. §§ 6801 - 6809.

[2] GLBA covers the federal banking regulators: the Office of the Comptroller of the Currency (national banks); the Office of Thrift Supervision (federal savings associations and state-chartered savings associations insured by the Federal Deposit Insurance Corporation (FDIC)); the Board of Governors of the Federal Reserve System (state-chartered banks which are members of the Federal Reserve System); FDIC (state-chartered banks which are not members of the Federal Reserve System, but which have FDIC deposit insurance); and the National Credit Union Administration (federal and federally-insured credit unions). Also included are the Securities and Exchange Commission (brokers and dealers, investment companies, and investment advisors). 15 U.S.C. § 6805(a) (1)-(5). For insurance companies, state insurance regulators are authorized to issue regulations implementing the GLBA privacy provisions. 15 U.S.C. § 6805(a)(6). For all other "financial institutions," the Federal Trade Commission has authority to issue rules implementing the privacy provisions of GLBA. 15 U.S.C. § 6805(a)(7).

[3] Interagency Guidelines Establishing Standards for Customer Information were published by the federal banking regulators on February 1, 2001 (66 *Fed. Reg.* 8616).

[4] GLBA covers "financial institutions" within the meaning of the Bank Holding Company Act (BHCA). Controversies have arisen because businesses involved in activities that are not necessarily performed in traditional financial institutions may meet this definition. *New York State Bar Association v. FTC*, 276 F. Supp. 2d 110 (D.D.C. 2003), held that attorneys are not covered. Section 609 of P.L. 109-351 makes it clear that certified public accountants subject to confidentiality requirements are also excluded.

[5] 72 *Fed. Reg*. 14940.

[6] 73 *Fed. Reg.* 71093 (Nov. 24, 208).

[7] *Federal Register* online at http://www.gpoaccess.gov/fr/index.html.

[8] See FTC regulations at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html. See FTC regulations at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

[9] http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0111.htm.

Insurance Commissioners (NAIC) approved a model law respecting disclosure of consumer financial and health information intended to guide state legislative efforts in the area.[10]

These privacy provisions preempt state law except to the extent that the state law provides greater protection to consumers. The FTC, in conjunction with the other federal financial institution regulators, is to make the determination as to whether or not a state law is preempted.

Public and Industry Reaction

One of the indications of the public's interest in preserving the confidentiality of personal information conveyed to financial service providers was the negative reaction to what became an aborted attempt by the federal banking regulators to promulgate "Know Your Customer" rules.[11] These rules would have imposed precisely detailed requirements on banks and other financial institutions to establish profiles of expected financial activity and monitor their customers' transactions against these profiles.

Even before the "Know Your Customer" Rules and enactment of GLBA, depository institutions and their regulators have increasingly promoted industry self-regulation to instill consumer confidence and forestall comprehensive privacy regulation by state and federal governments. One of the federal banking regulators, the Office of Comptroller of the Currency, for example, issued an advisory letter regarding information sharing.[12] To some participants in the financial services industry, preemptive federal legislation is preferable to having to meet differing privacy standards in every state. With respect to information sharing among affiliated companies, FCRA, as amended by the FACT Act preempts state law.[13] GLBA, on the other hand, leaves room for more protective state laws. In Congress, the debate continues as to whether there should be further limitations on disclosures. For example, whether consumer consent or customer opt-in should be required before certain sensitive types of information may be disclosed to third parties has been an issue in each Congress since GLBA was enacted.

The European Union Data Directive

Another incentive for a nationwide standard has been the requirements imposed upon companies doing business in Europe under the European Commission on Data Protection (EU Data Directive), an official act of the European Parliament and Council, dated October 24, 1995 (95/46/EC). This imposes strict privacy guidelines respecting the sharing of customer information and barring transfers, even within the same corporate family, outside of Europe, unless the transfer is to a country having privacy laws affording similar protection as does Europe. [14]

---

[10] http://www.naic.org.

[11] See CRS Report RS20026, *Banking's Proposed "Know Your Customer" Rules*, by M. Maureen Murphy.

[12] "Fair Credit Reporting Act," OCC AL 99-3 (March 29, 1999).

[13] See American Bankers Association v. Lockyer, 541 F.3d. 1214 (9th Cir. 2005), on remand, American Bankers Association v. Lockyer, 2005 WL 2452798 (E,.D. Cal. 2005).

[14] For an analysis of some of the differences between the European financial privacy regime and that of the United States, see Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 Berkeley J. Int'l L. 939 (2006).

Author Contact Information

M. Maureen Murphy
Legislative Attorney
mmurphy@crs.loc.gov, 7-6971