



## CRS Report for Congress

# Privacy Protection for Customer Financial Information

M. Maureen Murphy  
Legislative Attorney  
American Law Division

### Summary

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) (P.L. 106-102)<sup>1</sup> prohibits financial institutions from sharing nonpublic personally identifiable customer information with non-affiliated third parties without giving consumers an opportunity to opt out and requires them to provide customers with notice of their privacy policies. 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, and state insurance regulators. P.L. 109-351 requires them to devise a model privacy notice for consumers to 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. The 110<sup>th</sup> Congress is likely to consider financial privacy bills, as has every Congress since GLBA was enacted. This report will be updated to reflect action on major legislation. See CRS Report RS21427, *Financial Privacy Laws Affecting Sharing of Customer Information Among Affiliated Institutions*, by M. Maureen Murphy; CRS Report RL31758, *Financial Privacy: The Economics of Opt-In vs Opt-Out*; and CRS Report RL31847, *The Role of Information in Lending: The Cost of Privacy Restrictions*, both by Loretta Nott; CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law*, by Angie A. Welborn; and CRS Report RL32535, *Implementation of the Fair and Accurate Transactions (FACT) Act of 2003*, by Angie A. Welborn and Grace Chu.

**Background.** With modern technology's ability to gather and retain data, financial services businesses have increasingly found ways to take advantage of their large

---

<sup>1</sup> P.L. 106-102, tit. v, 113 *Stat.* 1338, 1436. 15 U.S.C. §§ 6801 - 6809. For general information on Gramm-Leach-Bliley, see CRS Report RL30375, *Major Financial Services Legislation, the Gramm-Leach-Bliley Act (P.L. 106-102): an Overview*, by F. Jean Wells and William D. Jackson.

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. While 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 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 fund transfer systems. Among them is the right to have the financial institution provide them 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.

Under section 214 of P.L. 108-159, 117 *Stat.* 1952, the Fair and Accurate Credit Transactions Act of 2003, 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 pre-existing 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 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, with the first report due no later than December 4, 2006.

**Gramm-Leach-Bliley's Privacy Provisions.** Title V of the Gramm-Leach Bliley Act (GLBA) contains the privacy provisions enacted in conjunction with financial modernization legislation. In addition to strengthening the prohibitions on identity fraud and mandating a federal study on information sharing among financial institutions and their affiliates, the legislation requires that federal regulators issue rules that call for

financial institutions to establish standards to insure the security and confidentiality of customer records.<sup>2</sup> It prohibits financial institutions<sup>3</sup> 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.

Implementing rules have been promulgated by the federal banking and securities regulators. Implementing regulations 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.<sup>4</sup> They became effective on November 13, 2000; and information may be shared thereafter provided the necessary steps have been taken by the financial institutions. See FTC regulations at [<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>]. Consumers may opt out at any time. Identity theft and pretext calling guidelines were issued to banks on April 6, 2001. [<http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr01111.htm>]. Insurance industry compliance has been handled on a state-by-state basis by the appropriate state authority. The National Association of Insurance Commissioners (NAIC) approved a model law respecting disclosure of consumer financial and health information intended to guide state legislative efforts in the area.<sup>5</sup> These privacy provisions preempt state law except to the extent that the state law provides greater protection to consumers. The Federal Trade Commission, in conjunction with the other federal financial institution regulators, is to make the determination as to whether or not a state law is preempted.<sup>6</sup>

**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.<sup>7</sup> These rules would have imposed precisely detailed requirements on banks and other financial institutions to

---

<sup>2</sup> Interagency Guidelines Establishing Standards for Customer Information were published by the federal banking regulators on February 1, 2001 (66 *Fed. Reg.* 8616).

<sup>3</sup> 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.

<sup>4</sup> *Federal Register* online at [<http://www.gpoaccess.gov/fr/index.html>].

<sup>5</sup> [<http://www.naic.org>].

<sup>6</sup> See CRS Report RL32626, *American Bankers Association v. Gould: Whether California's Financial Information Privacy Law Has Been Preempted by the Fair and Accurate Credit Transactions (FACT) Act*, by M. Maureen Murphy.

<sup>7</sup> See CRS Report RS20026, *Banking's Proposed 'Know Your Customer' Rule*, by M. Maureen Murphy.

establish profiles of expected financial activity and monitor their customers transactions against these profiles. Even before the Know Your Customer Rules and enactment of Gramm-Leach-Bliley, depository institutions and their regulators have increasingly promoted industry self-regulation as a means of instilling consumer confidence and forestalling 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.<sup>8</sup> 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.<sup>9</sup> 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.

**Legislation.** Financial privacy bills have been considered by every Congress since GLBA was enacted. The 107<sup>th</sup> Congress passed Title III of P.L. 107-56, the USA PATRIOT Act, which includes various amendments to the anti-money laundering laws and requires closer scrutiny of accounts held in the name of foreign banks and stricter procedures for identifying new customers. The 108<sup>th</sup> Congress passed the Fair and Accurate Credit Transactions Act (FACT ACT) (P.L. 108-159) which made permanent FCRA preemption of state law respecting information sharing among affiliated companies and modified the substantive provisions. Under this law, affiliated companies may share transaction and experience information with one another; they may share other consumer information if they provide the consumer notice and an opportunity to opt-out. They may not share such information for purposes of marketing solicitations unless the consumer is provided clear and conspicuous notice of the intent to share information for such purposes and a simple method of opting out. In the 109<sup>th</sup> Congress, P.L. 109-351 amended GLBA to require regulators to develop a model privacy notice so consumers may readily identify and compare data privacy practices of their financial institutions. This law makes it clear that certified public accountants subject to confidentiality requirements are not “financial institutions” under GLBA. The 109<sup>th</sup> Congress considered several bills to require businesses engaged in interstate commerce to develop security safeguards for customer information, some of which, such as S. 1332 and S. 1789 and H.R. 3997, had exceptions for financial institutions covered by GLBA. Others, such

---

<sup>8</sup> “Fair Credit Reporting Act,” OCC AL 99-3 (March 29, 1999).

<sup>9</sup> See CRS Report RL32625, *American Bankers Association v. Lockyer: Whether California’s Financial Information Privacy Law Has Been Preempted by the Fair and Accurate Credit Transactions (FACT) Act*, by M. Maureen Murphy.

as S. 1332, S. 1408, S. 1789, H.R. 1263, and H.R. 4127, covered GLBA-regulated financial institutions along with all other businesses, in requirements for customer notification when data breaches occur.