Order Code RS20185
Updated August 6, 2002

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 (P.L. 106-102, H.Rept. 106-434) requires financial institutions to provide their customers with notice of their privacy policies. It prohibits financial institutions from sharing nonpublic personally identifiable customer information with non-affiliated third parties without giving consumers an opportunity to opt out and prohibits financial institutions from providing account numbers to non-affiliated third parties for marketing purposes. 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. The legislation includes prohibitions on "pretext calling," obtaining financial institution customer information by false pretenses. Legislation has been offered in the 107th Congress to amend these provisions. This report will be updated on the basis of floor action involving privacy protection for financial institution customer information.

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 their preferences, but they can profit from sharing that information with others willing to pay for customer lists or targeted marketing compilations.[1] 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. Individuals are particularly interested in controls on 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

[1] This report addresses financial privacy issues. For more general information on privacy issues see: CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*, by Harold C. Relyea. Also see CRS Issue Brief IB98002, *Medical Records Confidentiality*.

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 government agent to obtain such records as a person's own copies of canceled checks, credit card charges and receipts, loan applications, and stock transfer 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.

Gramm-Leach-Bliley's Privacy Provisions. Title V of the Gramm-Leach Bliley Act[2] 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. It prohibits financial institutions 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.

Rules implementing these privacy provisions 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 on May 24, and by the SEC on June 29. 65 *Fed. Reg.* 35162, 33646, and

---

[2] Pub. 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.

40334.[3] They became effective on November 13, 2000. Compliance was optional until July 1, 2001, meaning that information may be shared after that date provided the necessary steps have been taken by the financial institutions. See FTC regulations at http://www.ftc.gov/privacy/glbact/index.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/sr0111.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.[4]

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. The Conference Committee rejected amendments that would have required customers to opt in, i.e., consent, before financial institutions could share customer financial information with either affiliates or third parties.

Privacy issues were discussed at each stage of the legislative process in the House consideration of financial modernization legislation. The House Banking Committee markup of the legislation (H.R. 10, 106th Cong.) included the rejection of an amendment, offered by Representative Inslee, that would have permitted bank customers to preclude sharing their information with third parties. What was accepted instead and included in the bill as reported by the House Banking Committee (H.Rept. 106-74)were provisions that would: require institutions to disclose their privacy policies, mandate a federal privacy study, and prohibit the sharing health information derived from insurance activities. As reported by the House Commerce Committee, H.R. 10's prohibition against sharing individually identified health information derived from insurance activities would have been extended to include genetic information; customers would have been given the opportunity to opt out of information sharing by their financial institutions; and consumers would have been able to examine, upon request, nonpublic personal information before their financial institution shares or sells such information for consideration to nonaffiliated persons or entities.

Public and Industry Reaction. Prior to enactment of Gramm-Leach-Bliley, there were various indicators of the public's interest in financial privacy as well as industry's efforts to address those concerns. 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.[5] 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

---

[3] *Federal Register* online at [http://www.access.gpo.gov/su_docs/aces/aces140.html].

[4] [http://www.naic.org/1news/releases]

[5] See CRS Report RS20026, *Banking's Proposed 'Know Your Customer' Rules*.

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. The American Bankers Association, for example, promulgates eight privacy principles for the banking industry,[6] and one of the federal banking regulators, the Office of Comptroller of the Currency, issued an advisory letter regarding information sharing.[7]

The regulatory scheme set in place by Gramm-Leach-Bliley became operative on July 1, 2001. In a certain sense, the debate as to whether information sharing by financial institutions with third parties–outside of their corporate families–should require actual consent rather than an opportunity to opt out continues. Both the FCRA and Gramm-Leach-Bliley contain provisions permitting limited and particularized state preemption of federal standards when state laws provide more protection for consumers. The year 2000 saw activity in some state legislatures considering ways to enhance the protections of Gramm-Leach-Bliley, including requiring actual consent–or opt in–before information sharing Only one state, California, enacted more protective legislation.[8] Industry sources view having to comply with multiple and inconsistent state regimes as posing excessive regulatory costs, litigation prospects, and liability potential. The validity of their claims may be reflected in a position taken by Robert Pitofsky, former Chairman of the Federal Trade Commission, in December 2000, when he went on record as potentially favoring legislation geared towards a nationwide financial privacy standard. In the same speech, however, he indicated that he would also consider enactment of legislation that the industry has resisted: requiring financial services providers to obtain customer consent before sharing data, i.e., an opt-in requirement rather than the current opt-out standard.[9]

A potential issue is the extent of coverage of Gramm-Leach-Bliley. It covers "financial institutions" within the meaning of the Bank Holding Company Act. Many commercial entities that sell or perform services for consumers are not included; some lawyers and accountants may be included because they perform services designated as "financial in nature" either by the BHCA, itself, or by the regulators under authority of that legislation as amended by Gramm-Leach-Bliley. On April 8, 2002, the FTC determined that lawyers were covered and that it had no authority to grant them an exemption; subsequently the New York State Bar Association filed suit.[10]

---

[6] See "Financial Privacy in America: A Review of Consumer Financial Issues," (June 1998). [http://www.aba.com].

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

[8] California enacted legislation that requires credit card issuers to provide consumers an opportunity to opt out of information sharing for marketing purposes, includes information sharing with affiliates for marketing purposes, and requires provision of a toll-free telephone number for exercising this right to opt out. 2000 Cal. Stat., ch. 977; 2000 Cal. Adv.Leg. Serv. 977 (Deering).

[9] "FTC Head Favors Federal Action on Privacy, Says Argument for Preemption Now Stronger," 6 *Electronic Commerce & Law Report* 7 (January 3, 2001).

[10] [http://www.nysba.org/Content/ContentGroups/News1/Release_attachments/nysbavftc.pdf] The American Bar Association had also requested an exemption for attorneys on the grounds that they are subject to stricter confidential requirements under their Code of Professional Responsibility and because having to send out Gramm-Leach-Bliley privacy notices could

(continued...)

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. The Department of Commerce has negotiated an agreement with the European Union that offers a framework under which US companies may be certified by the Department of Commerce and obtain a safe harbor, thereby continuing data transfers.[11] To date, the banking industry has not availed itself of this safe harbor, nor has the EU accepted Gramm-Leach-Bliley as one of the safe harbors meeting the Data Directive's requirements. U.S. entities with a presence in Europe, including some of the large bank holding companies, have chosen to draft guidelines and codes of conduct to meet the European standard and to satisfy that standard through separate negotiations. U.S. companies also have the option of adopting a standard contract approved in June 2001 by the European Commission, despite U.S. objections, for foreign companies to use to comply with the EU Data Directive.

Legislation. In the 107th Congress, Title III of P.L. 107-56, the USA PATRIOT Act, 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. S. 420, the Bankruptcy Reform Act of 2001, as reported and as passed by the Senate, includes a provision for the appointment of a privacy ombudsman in a bankruptcy proceeding to provide the court with information about the privacy policy of a debtor and its implication in any sale of the debtor's customer lists.

S. 2201 (Sen. Hollings) apples to online businesses; requires notice, affirmative consent (opt-in) for sensitive personally identifiable information, and an opt-out for other personally identifiable information; and includes a consumer right to correct information and judicial remedies for violations. H.R. 4678 (Rep. Stearns) applies to businesses in general, requires notice, includes an opt-out and a program of self-regulation administered by the FTC. Both bills would preempt state law. Other legislation includes : S. 30 (Sen. Sarbanes), amending Gramm-Leach-Bliley to require consumer consent for disclosure by financial institutions of certain data, extend the opt-out requirements to data sharing among affiliates, and authorize consumer access and correction of information; S. 324 (Sen. Shelby), specifying that Social Security numbers are non-public personal information for Gramm-Leach-Bliley privacy purposes; S. 450 (Sen. Nelson), requiring opt-in for sharing of health information, opt-out for sharing information with affiliates, and enhancing enforcement mechanisms; S. 536 (Sen. Shelby), requiring an opt-in for sharing profiling or marketing information; S. 1055 (Sen. Feinstein), requiring an opt-out for commercial entities' sale of personally identifiable information to non-affiliated third parties, amending Gramm-Leach-Bliley to require an opt-in in instances of disclosure for marketing purposes or sale of non-public personally identifiable information and to limit the exceptions to its nondisclosure provision, limiting the use

---

[10] (...continued)
confuse their clients as to that confidentiality. [http://www.abanet.org/poladv/letters/exec/privacy071001.html].

[11] See Department of Commerce website: [http://www.ita.doc.gov/].

of social security numbers, adding protections for driver's license information, and limiting disclosure of certain health information; H.R. 583 (Reps. Hutchinson and Moran), establishing a privacy commission; H.R. 1478 (Rep. Kleczka), prohibiting unconsented use of social security numbers; H.R. 2036 (Rep. Shaw), restricting the use of the social security number in public and private sectors; H.R. 2135 (Rep. Sawyer), requiring and opt-in for sharing consumer information; H.R. 2720 (Markey), requiring consumer consent (opt-in) for disclosure or unrelated use–even to affiliates–of nonpublic personal information collected by a financial institution in connection with any consumer transaction, prohibiting financial institutions from denying service to consumers who fail to provide such consent, providing consumers with a right to examine their data, prohibiting the disclosure of account numbers to affiliates or consumer reporting agencies for marketing purposes, authorizing the chief law enforcement officer of each state to bring a civil enforcement action in federal court, allowing each functional regulator to rule on state preemption issues, broadening the definition of "financial institution," and requiring states to elect as to whether to establish privacy rules for insurance industry; H.R. 2730 (Rep. Sessions), preempting states from imposing requirements or prohibitions on financial institutions other than those found in Gramm-Leach-Bliley's substantive privacy provisions and the regulations pertaining thereto, and making permanent the FCRA's current preemption–scheduled to end January 1, 2004–of state laws restricting sharing of credit report information among affiliates; and, H.R. 3068 (Rep. Ney), establishing a commission on financial privacy and national security.

House Energy and Commerce Committee hearings included such diverse topics as: the EU Data Protection Directive: Implications in the U.S. Privacy Debate; Privacy in the Commercial World; and Existing Federal Statutes Addressing Information Privacy [http://energycommerce.house.gov/107/action/action.htm].

The FCRA provisions on affiliate sharing of information preempt state law until January 1, 2004. Subsection (b)(2) of section 624, 15 U.S.C. § 1681t(b)(2), provides a general exception to the FCRA's general rule on preemption. Under that rule, FCRA does not preempt state law, unless the state law is inconsistent, and then it is preempted only to the extent of the inconsistency.[12] An exception to this rule applies to sharing of information among affiliates.[13] States may override this exception after January 1, 2004, by implementing or enacting laws providing greater protection to consumers with respect to information sharing among affiliates.[14] Gramm-Leach-Bliley, on the other hand, preempts state laws to the extent that they are inconsistent but provides that "a State statute, regulation, order, or interpretation is not inconsistent ... if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection under this subtitle as determined by the Federal Trade Commission...."[15] States may provide greater protection to consumers than Gramm-Leach-Bliley at any time. The FCRA moratorium ends on January 1, 2004.

---

[12] 15 U.S.C. § 1681t(a).

[13] 15 U.S.C. § 1681t(b)(2).

[14] 15 U.S.C. § 1681t(d)(2).

[15] 15 U.S.C. §§ 6824(b), Pub. L. 106-102, § 524(b), 113 *Stat.* 1448.