Order Code RS20185
Updated April 18, 2005

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, H.Rept. 106-434) 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. 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. GLBA, which deals with information sharing among non-affiliated third parties, is not directly addressed. In the 109th Congress, S. 116 includes some modification of GLBA privacy provisions. 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*, CRS Report RL31758, *Financial Privacy: The Economics of Opt-In vs Opt-Out*; CRS Report RL31847, *The Role of Information in Lending: The Cost of Privacy Restrictions*; CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law;* and, CRS Report RL32535, *Implementation of the Fair and Accurate Transactions (FACT) Act of 2003.*

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. 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. Some 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 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 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.[1]

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)[2] contains the privacy provisions enacted in conjunction with financial modernization legislation. In addition to strengthening the prohibitions on identity fraud

---

[1] Local ordinances in San Mateo County and Daly City, California requiring customer affirmative permission for a financial institution to share personal data are the subject of a lawsuit brought by Wells Fargo Co. and Bank of America Corp. in September 2002.

[2] 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.

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.

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.[3] 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/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.[5]

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.[6] 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 Gramm-Leach-Bliley, depository institutions and their regulators have increasingly promoted industry self-regulation as a means of instilling consumer confidence and

---

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

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

[5] See CRS Report RL32626, "*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.

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

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.[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, in *New York State Bar Association v. FTC*,[10] it was held that GLBA's privacy provisions did not cover lawyers.

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

---

[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] 276 F. Supp. 2d 110 (D.D.C. 2003).

transfer is to a country having privacy laws affording similar protection as does Europe.

Legislation. The 107th 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. Various proposals to amend Gramm-Leach-Bliley were considered, some of which would broaden protection for consumer financial information by requiring an affirmative opt-in for disclosures of specified sensitive information. There were also measures to preempt state law and, thereby, prevent states from establishing more protections than are offered under federal law.

The 108th 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 109th Congress, S. 116 (Feinstein) generally requires businesses to provide notice and an opt-out to a consumer before selling or marketing personally identifiable information to affiliates; affirmative consent is required in the case of non-affiliated third parties. It also includes a prohibition and civil and criminal sanctions for the display, sale, or purchase of Social Security numbers without consent. It contains provisions aimed at curtailing the sale of individually identifiable health information and a section on driver's license privacy.

S. 751/H.R. 1069 (Feinstein/Bean) would amend GLBA to require financial institutions to provide timely notice to customers when there has been breach of data security that results in or reasonably could result in unauthorized loss or acquisition of "personal information" of the customer. "Personal information" is defined to mean last name and one of the following: (1) social security number; (2) driver's license number or other officially recognized form of identification; or (3) credit card number, debit card number, or any required security code, access code, or password that would permit access to financial account information relating to the customer.

S. 768 (Schumer) would establish an Office of Identity Theft in the FTC, which would have civil jurisdiction over covered commercial entities that collect, maintain, sell, or transfer sensitive personal information. Under the bill, the FTC would be required to issue regulations governing the sale, maintenance, collection, or transfer of sensitive personal information by covered commercial entities, including requirements to prevent unauthorized access. Data merchants would be required to register with the Office of Identity Theft and would be subjected to regulations FTC is to promulgate to govern the sale or transfer of sensitive personal information, including specifics as to providing consumers with reports on data collected and third party access thereto. Other provisions include requiring covered entities to provide individuals with notice regarding information breaches and prohibitions on unnecessary solicitation of social security numbers, display of personal identification numbers on employee identification tags, inmate access to social

security account numbers, and sale or display of the social security number in the private sector. Enforcement authority includes civil penalties of up to $1,000 per individual record per violation and civil actions by the FTC or a state attorney general, The bill also would create a National Cybersecurity Office in the Department of Homeland Security, prohibit covered persons from posting in a document that is publically accessible online an individual's financial account number with the person's name. It would require the FTC to provide Congress with a report on the use and publication of social security numbers by federal, state, and local governments and recommend policy modifications designed to reduce or prevent identity theft.