Privacy Protection for Customer Financial Information

M. Maureen Murphy
Legislative Attorney

January 12, 2012

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

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Implementation of P.L. 111-203, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), may prompt legislative committees to review the federal regime that addresses how financial institutions protect confidential customer information. The major federal statutes which specify conditions under which customer financial information may be shared by financial institutions are Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA, P.L. 106-102) and the Fair Credit Reporting Act (FCRA). The Consumer Financial Protection Act of 2010 (CFPA), Title X of Dodd-Frank, transfers much of the federal agency rulemaking and enforcement authority under these statutes to the newly created Consumer Financial Protection Bureau (CFPB). Originally, rulemaking and enforcement power was distributed among the federal banking and security regulators, the Federal Trade Commission (FTC), and state insurance regulators. Possible topics for congressional oversight include (1) the transition of power from the financial institution prudential regulators and the FTC to the CFPB; (2) the interaction between the federal regulators and state enforcement efforts; and (3) the CFPB's success at issuing rules that adequately protect consumers without unreasonably increasing the regulatory burden on financial institutions.

GLBA prohibits financial institutions from sharing nonpublic personally identifiable customer information with non-affiliated third parties without providing customers an opportunity to opt out and mandates various privacy policy notices. It requires financial institutions to safeguard the security and confidentiality of customer information. FCRA regulates the credit reporting industry by prescribing standards that address information collected by businesses that provide data used to determine eligibility of consumers for credit, insurance, or employment and limits purposes for which such information may be disseminated. One of its provisions, which became permanent with the enactment of P.L. 108-159, permits affiliated companies to share non-public personal information with one another provided the customer does not choose to opt out.

CFPA alters the regulatory landscape for these laws. The newly created CFPB has responsibility for issuing rules under these privacy provisions. It has primary enforcement authority over non-depository institutions (subject to certain exceptions) and over depository institutions with more than $10 billion in assets. For depository institutions with assets of $10 billion or less, the CFPB's rules apply but enforcement authority remains with the banking regulators, subject to certain prerogatives of the CFPB.

In the 112th Congress, there is at least one measure, H.R. 653, that is aimed at amending GLBA's privacy provisions. There are also several general financial privacy or data breach bills that include proposals to provide safe harbors for entities subject to GLBA rules. Among the latter are H.R. 1707, H.R. 1841, H.R. 2577, S. 1151, S. 1207, S. 1408, and S. 1535, three of which, S. 1151, S. 1408, and S. 1535, were reported by the Senate Committee on the Judiciary during the first session of the 112th Congress.

This report will be updated to reflect action on major legislation. For further information, see CRS Report R41338, *The Dodd-Frank Wall Street Reform and Consumer Protection Act: Title X, The Consumer Financial Protection Bureau*, by David H. Carpenter; CRS Report R41839, *Limitations on the Secretary of the Treasury's Authority to Exercise the Powers of the Bureau of Consumer Financial Protection*, by David H. Carpenter; and, CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities*, by Margaret Mikyung Lee.

Contents

Background 1
Federal Laws Governing Consumer Financial Information Held by Financial Companies 1
Gramm-Leach-Bliley's Privacy Provisions 2
Public and Industry Reaction 3
The European Union Data Directive 4
The Role of the CFPB and the 112th Congress 4
Legislation in the 112th Congress 5

Contacts

Author Contact Information 7

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 enhance customer service by tailoring services and communications to customer preferences, but they can benefit from sharing that information with affiliated companies and 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 U.S. 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. At the federal level, the Right to Financial Privacy Act, 12 U.S.C. §§3401-3422, provides a measure of privacy protection by setting procedures for federal government access to customer financial records held by financial institutions.

Federal Laws Governing Consumer Financial Information Held by Financial Companies

There is no general federal regime covering how non-public personal information held in the private sector may be disclosed or must be secured. The major law which deals with this subject with respect to financial companies is Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA, P.L. 106-102),[1] which is discussed in a separate section of this report. The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§1681 to 1681x, predates GLBA. It 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. Another law, which predates GLBA, is the Electronic Funds Transfer Act, 15 U.S.C. §§1693a to 1693r, which describes the rights and liabilities of consumers using electronic funds transfer systems. These rights include the ability of consumers to have financial institutions identify 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 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."

[1] P.L. 106-102, Tit. V, 113 Stat. 1338, 1436. 15 U.S.C. §§6801 - 6809.

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 Congress every three years.

Gramm-Leach-Bliley's Privacy Provisions

Title V of the Gramm-Leach-Bliley Act (GLBA, P.L. 106-102)[2] contains the privacy provisions enacted in conjunction with 1999 financial modernization legislation. The Consumer Financial Protection Act of 2010, Title X of P.L. 111-203, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank),[3] makes the newly created Consumer Financial Protection Bureau (CFPB), which is located within the Federal Reserve System, the major rulemaking and enforcement authority for federal consumer protection laws, including the GLBA privacy provisions.[4] As originally enacted, GLBA allocated rulemaking and enforcement authority to an array of federal and state financial regulators.[5] GLBA requires that federal regulators issue rules that call for financial institutions to establish standards to insure the security and confidentiality of customer records.[6] It prohibits financial institutions[7] 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

[2] P.L. 106-102, Tit. V, 113 Stat. 1338, 1436. 15 U.S.C. §§6801 - 6809.

[3] P.L. 111-203, 124 Stat. 1376, 1955.

[4] P.L. 111-203, §1022, 124 Stat. 1376, 1980, 12 U.S.C. §5512.

[5] GLBA delegated authority to 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 is 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 was provided authority to issue rules implementing the privacy provisions of GLBA. 15 U.S.C. §6805(a)(7).

[6] Interagency Guidelines Establishing Standards for Customer Information were published by the federal banking regulators on February 1, 2001 (66 *Fed. Reg.* 8616). Under section 1093 of P.L. 111-203, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), 224 Stat. 1376, 2095, amending 15 U.S.C. §6804(a), the CFPB does not have authority to prescribe regulations with regard to safeguarding the security and confidentiality of customer records.

[7] 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.

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 Regulatory Relief Act of 2006, P.L. 109-351, the federal functional regulators were required to propose model forms for GLBA privacy notices. On March 29, 2007,[8] the agencies issued a notice proposing a model form. They subsequently published final amendments to their regulations incorporating a model privacy form which financial institutions may use to disclose their privacy policies.[9]

In general, regulations implementing GLBA's privacy requirements are the product of joint rulemaking and are found in various sections of the *Code of Federal Regulations*.[10] The banking regulators published their regulations in the *Federal Register* on June 1, 2000; the Federal Trade Commission (FTC) on May 24, 2000; and the Securities and Exchange Commission (SEC), on June 29, 2000 (65 *Fed. Reg.* 35162, 33646, and 40334).[11] They became effective on November 13, 2000.[12] Consumers may opt out at any time. Identity theft and pretext calling guidelines were issued to banks on April 6, 2001.[13] 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.[14]

These privacy provisions preempt state law except to the extent that the state law provides greater protection to consumers. The CFPB is to make the determination as to whether or not a state law is preempted.[15]

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.[16] These rules would have imposed precisely detailed requirements on banks and other financial

[8] 72 *Fed. Reg*. 14940.

[9] 74 Fed. Reg. 62890 (December 1, 2009). See text at http://www.occ.treas.gov/ftp/release/2009-142a.pdf.

[10] 12 C.F.R., Parts 40 (Office of the Comptroller of the Currency); 216 (Federal Reserve System); 332 (Federal Deposit Insurance Corporation); and 572 (Office of Thrift Supervision); 716 (National Credit Union Administration); 16 C.F.R., Part (Federal Trade Commission); and 17 C.F.R., Part 248 (Securities and Exchange Commission). The Commodities Futures Commission issued its implementing regulations, 17 C.F.R., Part 160, on April 27, 2001, 66 Fed. Reg. 21236; they became effective on June 21, 2001.

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

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

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

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

[15] Originally, GLBA delegated this authority to the FTC (in conjunction with the other federal regulators), section 1041(a)(2) of P.L. 111-203, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 124 Stat. 1376, 2011, delegated this authority to the CFPB exclusively. 12 U.S.C. §5551(a)(2).

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

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 had been increasingly promoting 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.[17] 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, does not entirely preempt state law; its preemption runs only to the extent of affiliate sharing of consumer report information.[18] GLBA also leaves room for more protective state laws.[19]

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.[20]

The Role of the CFPB and the 112th Congress

On July 21, 2011,[21] the CFPB began operations, assuming, among other things, authority to issue regulations[22] and take enforcement actions under enumerated federal consumer protection laws, including both FCRA and GLBA. The CFPB has primary enforcement authority over non-depository institutions (subject to certain exceptions) and over depository institutions with more than $10 billion in assets.[23] Although depository institutions with assets of $10 billion or less are

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

[18] See American Bankers Association v. Lockyer, 541 F.3d. 1214 (9th Cir. 2008), *cert. denied sub nom.* American Bankers Association v. Brown, ___ U.S. ___, 129 S. Ct. 2893 (2009).

[19] Under GLBA, inconsistent state statutes, regulations, orders, or interpretations, are preempted, to the extent of their inconsistency, and a state law is not inconsistent "if the protection such statute, regulation, order, or interpretation affords any person is greater" than is provided by GLBA. 15 U.S.C. §6807.

[20] 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).

[21] 75 Fed. Reg. 57252 (September 20, 2010).

[22] Under Dodd-Frank, the SEC, CFTC, and state insurance regulators retain their rulemaking authority; the FTC has authority to issue regulations covering motor vehicle leasing; all are required to coordinate for the sake of consistency. 15 U.S.C. §§6804(1) and (2), as added by P.L. 111-203, §1093, 124 Stat. 1376, 2095.

[23] P.L. 111-203, §§1024 and 1025, 124 Stat. 1376, 1987 and 1990, 12 U.S.C. §§5514-5515.

now subject to the CFPB's rules, enforcement remains with the "prudential regulators,"[24] subject to certain prerogatives of the CFPB.[25]

In general, as the impact of Dodd-Frank, the establishment of the CFPB and the President's recess appointment[26] of Richard Cordray as head of that agency draw increased congressional attention to oversight of the CFPB[27] in the second session of the 112th Congress, the GLBA and FCRA financial privacy regimes may command some focus on such issues as (1) identifying any problems arising in the transfer of regulatory power from the financial institution prudential regulators and the FTC to the CFPB; (2) monitoring the CFPB's rulemaking efforts to determine whether any newly issued rules unreasonably increase the regulatory burden on struggling institutions; (3) evaluating any effect on financial institutions operating nationwide stemming from application of non-preempted state laws; and examining issues that may arise in connection with programs that banks are increasingly offering to induce customers to combine banking activity with social media.[28]

Legislation in the 112th Congress

The 112th Congress has before it both legislation aimed at amending GLBA's privacy provisions and general financial privacy legislation or data breach legislation that includes proposals to provide a safe harbor for entities subject to GLBA rules.

H.R. 653 would amend GLBA, subject to certain exceptions, to require customer opt-in for financial institutions to share non-public personal information with nonaffiliated third parties and opt-out for disclosures to affiliates. It would prohibit financial institutions from discriminating against customers who choose to exercise these prerogatives and set forth requirements for model disclosure forms.

H.R. 1707 would require the FTC to issue regulations requiring anyone engaged in interstate commerce possessing personal information to establish information security procedures and to

[24] Under P.L. 111-203, §1002(24), 124 Stat. 1376, 1962, 12 U.S.C. §5481(24), "prudential regulator" is defined to cover the federal banking regulators and the National Credit Union Administration, that is, the federal regulators of depository institutions.

[25] P.L. 111-203, §1026, 224 Stat. 1376, 1993, 12 U.S.C. §5516. This provision requires coordination between the prudential regulators and the CFPB and authorizes the CFPB to have examiners join prudential regulator examinations on a sampling basis.

[26] See, Laura Meckler and Victoria McGrane, "Obama Picks Nominee Fight," Wall Street Journal (January 5, 2012), http://global.factiva.com/ha/default.aspx, and Helene Cooper and Jennifer Steinhauer, "Bucking Senate, Obama Appoints Consumer Chief," N. Y. Times (January 4, 2012), http://www.nytimes.com/2012/01/05/us/politics/richard-cordray-named-consumer-chief-in-recess-appointment.html.

[27] Legislation of this sort may develop on the basis of some studies of commercial privacy policy now under way at the Department of Commerce. On December 21, 2010, the department sought public comments in connection with its December 16, 2010, release of a report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf. Among the questions posed by the department was whether "baseline commercial data privacy principles … [should] be enacted by statute or other means, to address how current privacy law is enforced." 75 Fed. Reg. 80042, 80043 (December 21, 2010).

[28] See, e.g. Jeremy Quittner, "Citi's Facebook App Exposes the Perils and Rewards of Social Media," American Banker (January 3, 2012), http://www.americanbanker.com/issues/176_253/citi-citibank-facebook-app-privacy-rewards-security-thankyou-1045383-1.html.

comply with breach notification procedures. It would impose special requirements on information brokers who must establish procedures to maximize accuracy and provide a means for annual access by customers to the personal information maintained by the information broker. There would be a safe harbor for entities covered by GLBA's privacy requirements, provided the FTC determines that the GLBA requirements "provide protections substantially similar to, or greater than, those required"[29] under the legislation.

H.R. 1841 would require the FTC to issue regulations requiring any person engaged in interstate commerce that possesses or maintains through a third party data in electronic form containing personal information to establish and implement information security policies and procedures to protect personal information. It imposes a breach notification requirement and includes a means for the FTC to grant a safe harbor for financial institutions subject to GLBA. It also requires the FTC to study the feasibility of mandating standards for disposing of obsolete personal information held in non-electronic form. It would impose special requirements on information brokers, including verification of the accuracy of personal information maintained by the information broker and opportunity, at least annually, for each individual to review personal data.

H.R. 2577 would require the FTC to issue regulations requiring any entity engaged in interstate commerce to establish and implement information security policies and procedures to protect personal information, including minimizing the personal data being maintained. It imposes a breach notification requirement and includes a safe harbor for financial institutions subject to GLBA.

S. 1151, as reported by the Senate Committee on the Judiciary,[30] would impose data breach notice requirements and require business entities to comply with regulations which the FTC is to issue setting requirements for personal data privacy and security programs. It includes a specific exemption from these requirements for financial entities subject to GLBA (and for entities subject to the requirement of the Health Insurance Portability and Accountability Act (HIPPA Act).[31] The bill also includes various criminal provisions including one which would provide criminal penalties for intentional and willful concealment of a data security breach for which notification is required under this legislation.

S. 1207 would require the FTC to issue regulations requiring any person engaged in interstate commerce that possesses or maintains through a third party data in electronic form containing personal information to establish and implement information security policies and procedures to protect personal information. It imposes a breach notification requirement and includes a means for THE FTC to grant a safe harbor for financial institutions subject to GLBA. It would impose special requirements on information brokers, including verification of the accuracy of personal information maintained by the information broker and opportunity, at least annually, for each individual to review personal data.

S. 1408[32] would impose date breach notification requirements on federal agencies, with certain exceptions, and businesses engaged in interstate commerce that possess sensitive personally

[29] H.R. 1707, sec. 2(a)(3), 112th Cong., 1st Sess. (2011).

[30] S.Rept. 112-91, 112 Cong., 1st Sess. (2011).

[31] P.L. 104-191, 110 Stat. 1998, 104th Cong., 2d Sess. (1996).

[32] S. 1151, S. 1408, and S. 1535 were reported by the Senate Committee on the Judiciary without a written report. See, Rachel Bade and Katherine Tully-McManus, "Data Breach Bills Approved Amid Partisan Division," CQ Markup a& Vote Coverage, Senate Judiciary Committee Markup (September 22, 2011). http://www.cq.com/doc/committees-
(continued...)

identifiable data. It provides no general exception for financial institutions complying with GLBA.

S. 1535 would require businesses engaging in interstate commerce that have sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons to comply with rules that THE FTC is to issue mandating personal data privacy and security programs. It imposes data breach notice requirements and exempts financial institutions subject to GLBA's privacy regime provided that they are subject to a data breach notice requirement issued by their GLBA privacy regime regulator. The legislation also includes various criminal provisions including one that would provide criminal penalties for intentional and willful concealment of a data security breach for which notification is required under this legislation, provided there is knowledge of the notice requirement. Also included is a requirement that federal agencies contracting with data brokers for access to sensitive personally identifiable information databases must prepare a privacy impact assessment. They must also adopt regulations governing the standards applicable to the agencies with respect to access to these databases and require data brokers with whom they have contracts to comply with the requirements of this legislation.

Author Contact Information

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

(...continued)

2011092200290255?wr=RDlYTlRja3lSajZIaFQ2VjVNbmU4Zw.