

Congressional Research Service
Informing the legislative debate since 1914

Privacy Protection for Customer Financial Information

M. Maureen Murphy
Legislative Attorney

July 14, 2014

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

One of the functions transferred to the Consumer Financial Protection Bureau (CFPB) under P.L. 111-203, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), is authority to issue regulations and take enforcement actions under the two major federal statutes that specify conditions under which customer financial information may be shared by financial institutions: Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA, P.L. 106-102) and the Fair Credit Reporting Act (FCRA). Possible topics for congressional oversight in the 113th Congress include (1) the transition of power from the financial institution prudential regulators and the Federal Trade Commission to the CFPB; (2) CFPB's interaction with other federal regulators and coordination with 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. The creation of CFPB alters the regulatory landscape for these laws. 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 first session of the 113th Congress, the House passed H.R. 749, which would eliminate the GLBA requirement for an annual privacy notice if the financial institution has not changed its policies and practice with respect to sharing nonpublic personal information since its last disclosure. A similar bill, S. 635, would require that any financial institution eliminating its annual privacy notice must provide electronic access to its privacy policies. Several bills that require data breach notifications, H.R. 3990, S. 1193, S. 1897, and S. 1995, provide exemptions for financial institutions covered by the GLBA privacy provisions.

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; 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 113th Congress 5
Legislation in the 113th Congress 6

Contacts

Author Contact Information 6

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. Sections 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. Sections 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. Sections 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, Section 2419, 110 Stat. 3009-452, adding 15 U.S.C. Section 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 GLBA (P.L. 106-102)[2] contains the privacy provisions enacted in conjunction with 1999 financial modernization legislation. These privacy provisions preempt state law except to the extent that the state law provides greater protection to consumers.[3] 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),[4] 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.[5] As originally enacted, GLBA allocated rulemaking and enforcement authority to an array of federal and state financial regulators.[6] GLBA requires that federal regulators issue rules that call for financial institutions to establish standards to insure the security and confidentiality of customer records.[7] It prohibits financial institutions[8] from disclosing

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

[3] The Consumer Financial Protection Bureau (CFPB) is to make the determination as to whether or not a state law is preempted. 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).

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

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

[6] 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).

[7] Interagency Guidelines Establishing Standards for Customer Information were published by the federal banking regulators on February 1, 2001 (66 *Federal Register* 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.

[8] 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.

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 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,[9] 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.[10]

Initially, regulations implementing GLBA's privacy requirements were the product of joint rulemaking and were found in various sections of the *Code of Federal Regulations*.[11] They became effective on November 13, 2000.[12] 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]

The establishment of the CFPB as authorized by Dodd-Frank has meant the transfer from the other federal agencies of much of the rulemaking authority for GLBA's privacy provisions.[15] The CFPB promulgated an interim final rule.[16]

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

[9] 72 *Federal Register* 14940.

[10] 74 *Federal Register* 62890 (December 1, 2009). See text at http://www.occ.treas.gov/ftp/release/2009-142a.pdf.

[11] 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 *Federal Register* 21236; they became effective on June 21, 2001. 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 *Federal Register* 35162, 33646, and 40334). *Federal Register* at http://www.gpoaccess.gov/fr/index.html.

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

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

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

[15] Dodd-Frank did not transfer to the CFPB the rulemaking authority delegated to the SEC or the CFTC under the Gramm-Leach-Bliley privacy provisions. The FTC retains rulemaking authority over "any motor vehicle dealer that is predominantly engaged in the sale and servicing of motor vehicles, the leasing and servicing of motor vehicles, or both." 12 U.S.C. §5519(a).

[16] 12 C.F.R., Part 1016 (CFPB's Regulation P). 76 *Federal Register* 79025 (December 21, 2011).

aborted attempt by the federal banking regulators to promulgate "Know Your Customer" rules.[17] 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 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.[18] 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.[19] GLBA also leaves room for more protective state laws.[20]

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.[21] Revision of European Union data protection law may be on the near horizon. In January 2012, the European Commission released a draft legislative proposal for consideration by the European Parliament and the Council of the European Union. It is aimed at updating the legal protection the European Union affords to personal data in view of challenges accompanying advances in technology and arising in the increasing pervasiveness of online environments.[22] U.S. companies operating in Europe are likely to be monitoring the progress of any changes to the European data protection regime. The U.S. Chamber Institute for Legal Reform (Institute) is already on record as having "deep concerns" about one aspect of the Commission's Draft Regulation, its authorization of third parties to bring litigation to seek remedies and damages to protect the rights of others. To the Institute, this is analogous to what it deems to be the faults of class action

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

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

[19] 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).

[20] 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.

[21] 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).

[22] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). See http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

lawsuits in the United States, encouraging plaintiff's attorneys to initiate and promote costly and abusive litigation that does not serve the ends of justice.[23]

The Role of the CFPB and the 113th Congress

On July 21, 2011,[24] the CFPB began operations, assuming, among other things, authority to issue regulations[25] 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.[26] Although depository institutions with assets of $10 billion or less are now subject to the CFPB's rules, enforcement remains with the "prudential regulators,"[27] subject to certain prerogatives of the CFPB.[28]

Given the CFPB's predominant role in implementing the GLBA privacy regime and increasing attention to the problem of Internet data security,[29] Congress is likely to scrutinize how the CFPB implements such programs by (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 (4) examining issues that may arise in connection with the increasing use by banks of social media both to communicate with customers and for marketing purposes.[30]

---

[23] Lisa A. Rickard, U.S. Chamber Institute, Letter to Viviane Reding, Vice-President of the European Commission (January 29, 2013). The Institute is concerned about "[t]he possibility of third party representatives seeking damages; [t]he criteria to be met by third party representatives; [t]he absence of consent on the part of data subjects; and [m]echanisms to safeguard recoveries for claimants to prevent abuse." See http://www.instituteforlegalreform.com/global/european-union.

[24] 75 *Federal Register* 57252 (September 20, 2010).

[25] 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.

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

[27] 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.

[28] 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.

[29] 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 *Federal Register* 80042, 80043 (December 21, 2010).

[30] 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.

Recently, the CFPB announced[31] that it was proposing to amend Regulation P, Privacy of Consumer Financial Information,[32] to permit financial institutions to satisfy GLBA's annual privacy notice requirement in situations in which customers would not need the notice to avail themselves of an opt-out right. Under the proposal, financial institutions could satisfy the requirement for an annual notice without a separate mailing. They would be required to post the notice separately and continuously on a website page and to include it, at least once a year, in other communications with customers. Moreover, the proposal would require covered businesses choosing not to send annual privacy notices to use a model privacy disclosure form and to provide a dedicated telephone number for customers to call to request mailed copies of the privacy policy.

Legislation in the 113th Congress

The 113th Congress has two bills that would eliminate GLBA's requirement for an annual privacy notice under certain circumstances.

H.R. 749 would eliminate the annual notice requirements for financial institutions if their privacy policies have not changed from their last disclosure notice and they share nonpublic personal information only pursuant to certain permissible exceptions to GLBA's prohibitions.

S. 635 would eliminate the annual notice requirements for financial institutions if their privacy policies have not changed from their last disclosure notice and they share nonpublic personal information only pursuant to certain permissible exceptions to GLBA's prohibitions and otherwise provide customers access to their most recent disclosure in electronic or other form.

Other bills, H.R. 3990, S. 1193, S. 1897, and S. 1995, would require commercial concerns to secure personal information and to provide notification of data breaches. Exemptions are provided for financial institutions covered by the GLBA privacy provisions.

Author Contact Information

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

[31] Consumer Financial Protection Bureau, "CFPB Proposes Rule to Promote More Effective Privacy Disclosures" (May 6, 2014). http://www.consumerfinance.gov/newsroom/cfpb-proposes-rule-to-promote-more-effective-privacy-disclosures/. 75 *Fed. Reg*. 30485 (May 14, 2014). https://www.federalregister.gov/articles/2014/05/28/2014-12148/amendment-to-the-annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p.

[32] 12 C.F.R., Part 1016.