Privacy Year in Review: Recent Developments in the Gramm-Leach Bliley Act, Fair Credit Reporting Act, and Other Acts Affecting Financial Privacy

STEVEN ROBERT ROACH & WILLIAM R. SCHUERMAN, JR.*

ABSTRACT

This article addresses current privacy issues that concern financial information. The Gramm-Leach Bliley Act ("GLB Act") is the most comprehensive federal financial privacy act. Federal case law in 2004 helped to define the meaning of "financial institution," "affiliate," and "notice" under the GLB Act, along with exploring whether it provides a private right of action. The interaction of the GLB Act with state laws is reviewed through examples from California, Vermont and Massachusetts. The European Union Directive is also discussed.

This article also explores the privacy issues arising under the Fair Credit Reporting Act ("FCRA") and accurate credit transaction acts. An introduction of these acts, including their interactions with one another, is provided. Issues discussed are: state laws and federal preemption, limitations on the usage of credit reports, obligations for the users of credit reports, and the difficulty of enforcing these acts. Further case law illustrates the expanding protections for consumers who attempt to correct credit errors by furnishers of credit information. These issues are analyzed through current laws and federal and state cases. The impacts on financial privacy of Section 326 of the Patriot Act and the Health Information Portability and Accountability Act ("HIPAA") are also discussed.

I. INTRODUCTION

Americans are becoming increasingly concerned with their privacy, and public opinion polls are nearly unanimous in finding strong support among Americans favoring legal protections that ensure the privacy of their personal information. A summary of recent public opinion polls on privacy by the Electronic Privacy Information Center identified several broad trends and reported consumer concerns including:

---

* The authors are J.D. candidates at The Ohio State University Moritz College of Law, class of 2006. Steven Robert Roach, B.A., High Honors, The University of Michigan, 2002. William R. Schuerman Jr., B.S., *cum laude*, Cornell University, 2003.

> Individuals should be in control of both initial collection of data and data sharing; individuals want accountability and security; individuals want comprehensive legislation, not self-regulation; individuals value anonymity; individuals object to web tracking, especially when personal information is linked to the profile; individuals do not trust companies to administer personal data and fear both private-sector and government abuses of privacy; individuals engage in privacy self-defense; individuals are unaware of prevalent tracking methods; [and individuals desire] notice.[1]

One important area in which these concerns manifest themselves is the area of financial privacy. Recent developments illustrate the tension between balancing information sharing to provide an efficient financial services industry and protecting the privacy of consumer information and the rights of consumers. Financial institutions are realizing that protecting privacy is good for a company's bottom line, and not protecting it is no longer an option. However, as Federal Reserve Board Chairman Alan Greenspan notes, "the free-flow of information allows the market to adjust to meet consumers' needs," and regulation in this area restricts the market's ability to respond to consumers' needs for privacy.[2] The free-flow of financial information that is essential for a market must be balanced with the public's concerns with excessive information sharing.

Federal financial laws have attempted to work within these two competing interests by supporting the sharing of information between institutions while protecting consumer information through disclosure and notice requirements in the Gramm-Leach-Bliley Act ("GLB Act"). The Fair and Accurate Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transaction Act ("FACT Act") attempt to protect the consumer against legitimate and growing harms such as identity theft. Section 326 of the USA PATRIOT Act was passed after September 11th and provides stricter mechanisms to combat money laundering domestically and abroad. Finally, financial institutions such as banks are among the many organizations that need to familiarize themselves with the new Health Information Portability and Accountability Act ("HIPAA") regulations developed to help

---

[1] Electronic Privacy Information Center, *Public Opinion on Privacy, available at* http://www.epic.org/privacy/survey/ (last visited March 17, 2005) (quoting headers).

[2] American Bar Association, *Greenspan on the Free Flow of Information, available at* http://www.aba.com/Industry+Issues/GR_PR_Greenspan.htm (last visited April 3, 2005).

promote a more economically efficient electronic claim process, and protect the privacy of individually identifiable health information. This paper will restrict its focus to these four primary areas and will address recent case law, regulations, and statutes that affect the financial privacy sector.

II. THE GRAMM-LEACH-BLILEY ACT

A. BACKGROUND

The Gramm-Leach-Bliley Act ("GLB Act"), signed into law by President Clinton on November 12, 1999, contains the most comprehensive financial privacy provisions of any federal legislation ever enacted.[3] The purpose of the GLB Act was "to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers."[4] The Act attempts to accomplish this purpose by eliminating barriers on affiliation between banks, securities firms, insurance companies, and other financial service providers.[5]

The relevant privacy provisions from the GLB Act are found in Title V (the Financial Privacy Law) and contain two separate privacy-related subtitles.[6] Subtitle A creates new substantive obligations relating to the disclosure of customers' nonpublic personal information by financial institutions to nonaffiliated third parties.[7] Under these obligations, a financial institution is required to provide each customer

---

[3] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in Titles 12 and 15 of the United States Code). For further discussion of the potential effects of GLBA, see generally Arthur E. Wilmarth, Jr., *The Transformation of the U.S. Financial Services Industry, 1975-2000: Competition, Consolidation and Increased Risks*, 2002 U. Ill. L. Rev. 215 (2002).

[4] *See* H.R. CONF. REP. NO. 106-434 (1999); *see also* Julia C. Schiller, *Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?*, 11 COMMLAW CONSPECTUS 349, 355 (2003).

[5] Kyle Thomas Sammin, *Any Port in a Storm: The Safe Harbor, The Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, 36 GEO. WASH. INT'L L. REV. 653, 666 (2004) (quoting JONATHAN R. MACEY ET AL., BANKING LAW AND REGULATION 34, 443, 460 (3d ed.) (2001)).

[6] *See* 15 U.S.C. §§ 6801-6827 (1999).

[7] *See* 15 U.S.C. §§ 6801-6809 (1999).

with a clear statement describing the institution's policies and practices with respect to the sharing of customer information with third parties, and their procedures for protecting the security and confidentiality of consumer information.[8] In addition, Subtitle A requires that each financial institution provides its customers and certain other consumers with notice offering a clear and conspicuous opportunity to "opt out" of the disclosure of certain information to nonaffiliated third parties prior to disclosure.[9] Subtitle B of Title V establishes new federal criminal penalties relating to the fraudulent obtainment of customer information from financial institutions.[10] Subtitle B was enacted by Congress in response to "information brokers" who purportedly obtain customer information by engaging in a variety of tactics with the purpose of defrauding customers and financial institutions.[11]

The above obligations of Subtitle A of Title V apply principally to "financial institutions," defined as any institution "the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956."[12] This broad definition, as added by section 103 of the GLB Act, includes any entity engaging in any of the activities identified as permissible for a financial holding company or its nonbank affiliates, regardless of the entity's traditional structural classification.[13] In addition, the GLB Act authorizes the Board of Governors of the Federal Reserve System ("FRB") to act as an "umbrella regulator" in defining permissible activities for a financial holding company or its nonbank affiliates.[14] Through this authority, the FRB has issued regulations for financial holding companies and nonbank affiliates that have expanded the definition of

---

[8] L. Richard Fischer, *Disclosure of Nonpublic Personal Information*, THE LAW OF FINANCIAL PRIVACY, ¶ 9.01 SUBTITLE A (A.S. Pratt & Sons 2004); *see* 15 U.S.C. §§ 6803(a), 6803(b)(1) (1999).

[9] Fischer, *supra* note 8, at ¶ 9.01 SUBTITLE A; *see* 15 U.S.C. § 6802(b)(1) (1999).

[10] Fischer, *supra* note 8, at ¶ 9.02; *see* 15 U.S.C. §§ 6821–6827 (1999).

[11] Fischer, *supra* note 8, at ¶ 9.02; *see also* H.R. REP. NO. 106-74, pt. 1, at 103 (1999).

[12] 12 U.S.C. § 1843(k)(4)(A)-(E) (2000); *see also* 12 U.S.C. §§ 1841–1850 (1956).

[13] *Id.*

[14] Sammin, *supra* note 5, at 667 (citing Lisa L. Broome & Jerry W. Markham, *Banking and Insurance: Before and After the Gramm-Leach-Bliley Act*, 25 J. CORP. L. 723, 762 (2000)); *see also* 12 U.S.C. § 1843(k)(5).

"financial institutions" to include many traditionally non-financial entities.[15]

The GLB Act operates by placing limits on financial institutions' ability to disclose "nonpublic personal information" of customers.[16] Section 509(4)(A) of the Financial Privacy Law defines "nonpublic personal information" as any personally identifiable financial information that is obtained by a financial institution from the customer, from the institution's own transactions with the customer, or through any third party source.[17] In defining proper disclosure, the GLB Act "adopted the basic rule of requiring an opt-out choice before personal data could be shared with nonaffiliated third parties."[18] The "opt-out provision" must: (1) be clear and conspicuous; (2) accurately explain the customer's right to "opt-out"; (3) inform the customer that the institution may disclose nonpublic financial information to nonaffiliated third parties; and (4) provide customers with reasonable means by which to exercise their right to "opt-out."[19] The Financial Privacy Law further complicates the Act by distinguishing between the terms "consumer" and "customer." A "consumer" is defined as an individual who obtains financial products or services for a personal, family, or household purpose from a financial institution.[20] A "customer" is defined as a consumer who has a continuing "customer relationship" with the financial institution.[21] This differentiation is important because a "customer" of a financial institution is always entitled to receive a copy of the financial institution's privacy policy, both at the time of establishing the customer relationship and annually thereafter. A "consumer," on the other hand, is not covered by section 503 of the Financial Privacy Law and will receive "opt-out" rights

---

[15] *See* Sammin, *supra* note 5, at 667 (providing examples of several non-traditional financial institutions).

[16] *See* 15 U.S.C. § 6809(4)(B) (1999).

[17] Fischer, *supra* note 8, at ¶ 9.01[1][B]; *see* 15 U.S.C. § 6809(4)(A) (1999).

[18] Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV., 1263, 1268 (2002).

[19] *See* 15 U.S.C. § 6809.

[20] 15 U.S.C. § 6809(9).

[21] *See* 12 C.F.R. § 40.3(i) (2000).

only if the institution intends to disclose information relating to that "consumer" to a nonaffiliated third party.[22]

The Gramm-Leach-Bliley Act is a congressional attempt to facilitate the efficient sharing of information throughout the financial services industry. Congress eliminated "the barriers on affiliation between banks, insurance, and securities industries," in an attempt to provide one-stop shopping for financial services, reducing costs, and creating more efficient operations.[23] The GLB Act balances these efficiencies with customers' rights to privacy by requiring financial institutions to comply with the notice and opt-out provisions discussed above. Through these requirements, the GLB Act attempts to create an efficient compromise between the benefits of information sharing and the personal privacy rights of customers. Although considered by many as a significant advance in financial privacy law, the Gramm-Leach-Bliley Act played a controversial role in 2004, with specific issues concerning: (1) the proper interpretation of so-called "terms of art" on the federal level; (2) the Act's notice requirement; (3) state preemption issues, especially pertaining to interaction with the Fair Credit Recording Act; (4) the proper enforcement of the Act; and (5) compliance with the European Union's Privacy Directive.

B. FEDERAL CASE LAW SUMMARY

During 2004, federal case law concerning the application and enforcement of the Gramm-Leach-Bliley Act under federal law focused on: (1) the proper interpretation of terms of art such as "financial institutions" and "affiliate;" (2) the notice requirement; (3) the availability of a private right of action under the GLB Act; and (4) state preemption issues concerning possible conflicts in law.

1. DEFINING A "FINANCIAL INSTITUTION"

Over the past year, federal courts have been asked to define further "financial institutions" under the GLB Act, and to rule explicitly on the status of several specific entities. After unsuccessfully attempting to obtain a statement from the Federal Trade Commission ("FTC"), two state bar associations challenged the FTC's determination that attorneys engaging in certain financial activities fall within the Act's

---

[22] Fischer, *supra* note 8, at ¶ 9.01[2]; *see* 15 U.S.C. §§ 6803(a), 6802(b).

[23] Schiller, *supra* note 4, at 355.

definition of financial institutions.[24] In New York State Bar Association v. FTC, the plaintiff bar association brought an action following "report[s] in the professional and trade regulation press" indicating that the FTC had decided that attorneys engaged in certain "financial activities" as part of their legal practice would be subject to the GLB Act.[25] In this action, the bar association was seeking a declaratory judgment that

> (1) the FTC's decision that attorneys engaged in certain "financial activities" as part of their practice of law are covered by the [GLB Act] is beyond the FTC's statutory authority; (2) the FTC's decision that attorneys engaged in certain "financial activities" as part of their practice of law are covered by the [GLB Act] is arbitrary and capricious agency action; and (3) the FTC's refusal to grant attorneys engaged in the practice of law an exemption from the [GLB Act] also constitutes arbitrary and capricious agency action.[26]

The D.C. district court granted summary judgment for the plaintiffs, citing the reasons set forth by the court in its August 11, 2003 Memorandum Opinion.[27] The district court, citing the 2003 memorandum opinion, found it was "unable to conclude as a matter of law that Congress intended for the [GLB Act's] privacy provisions to apply to attorneys who provide legal services in the fields of real estate settlement, tax-planning[,] and tax-preparation."[28] The court stated that the conclusion was "compelled by the plain language, the underlying purpose, and the legislative history of the [GLB Act], which all indicate that it does not appear that Congress intended for attorneys to be considered 'financial institutions.'"[29] As for the bar

---

[24] *See* N.Y. State Bar Ass'n v. FTC, 2004 U.S. Dist. LEXIS 7698 (D.D.C. Apr. 30, 2004); *see also* N.Y. State Bar Ass'n v. FTC, 276 F. Supp. 2d 110 (D.D.C. 2003).

[25] *N.Y. State Bar Ass'n*, 2004 U.S. Dist. LEXIS 7698, at *2 (citing N.Y. State Bar Ass'n Compl., at 37).

[26] *Id.* at *4, 5.

[27] *N.Y. State Bar Ass'n*, 276 F. Supp. 2d 110.

[28] *N.Y. State Bar Ass'n*, 2004 U.S. Dist. LEXIS 7698, at *7 (discussing *N.Y. State Bar*, 276 F. Supp. 2d at 136).

[29] *Id.* at *8.

association's "arbitrary and capricious" claims, the court again cited the 2003 memorandum opinion, concluding, "[t]here is nothing else in the record that indicates that the FTC engaged in any type of reasoned decisionmaking, confirming the Court's belief that the FTC acted in an 'arbitrary and capricious' manner"[30] and, pursuant to 5 U.S.C. § 706(2)(A), "the FTC's interpretation that attorneys are subject to the [GLB Act's] privacy provisions constitutes 'arbitrary and capricious' agency action."[31]

In Texas, the Federal District Court for the Northern District of Texas determined whether "financial institutions" include software companies.[32] Here, the defendants filed a motion to dismiss, contending that the plaintiff software company violated the GLB Act by including defendants' personal credit card numbers and signatures in exhibits to the original complaint.[33] The Texas district court looked to the Code of Federal Regulations for insight, finding:

> [F]inancial institutions include, but are not limited to[,] mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account services, check cashers, wire transferors, travel agencies operated in connection with financial services, collecting agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission.[34]

The court then compared these "financial activities" to the activities conducted by Lacerte, finding that the software company appears not to have "engaged in any of the activities above."[35] The court issued a narrow holding, however, stating only that "even if Lacerte were a financial institution, the Act does not provide a private right of action,"

---

[30] *Id.* at *11.

[31] *Id.* at *12.

[32] Lacerte Software Corp. v. Prof'l Tax Servs. L.L.C., 2004 WL 180321 (N.D. Tex. Jan. 6, 2004).

[33] *Id.* at *1.

[34] *Id.* (citing 16 C.F.R. § 313.1(b)).

[35] *Id.* at *2.

and did not go so far to hold that all software companies were not "financial institutions."[36]

In Maryland, the FTC sued AmeriDebt for violations of the GLB Act's disclosure requirements, alleging that AmeriDebt, while operating under the disguise of a non-profit credit counseling service, defrauded consumers through a debt repayment plan.[37] In response, AmeriDebt denied it was a "financial institution," claiming it was exempt from the Act's requirements.[38] The court found that the Act authorizes the FTC and other federal agencies to promote polices and issue regulations necessary to carry out the stated purpose of the GLB Act.[39] The court discovered that the preamble to the FTC's final rule on the privacy of customer financial information states that "the term 'financial institutions' is defined 'very broadly' under the [GLB Act] and includes several entities not traditionally recognized as financial institutions."[40] The court discussed the provision cited above in the *Lacerte* case, finding that the final rule explicitly includes a "credit counseling service" as an example of a financial institution.[41] In addition to citing AmeriDebt's practice as a self-described "credit counseling service," the court looked at AmeriDebt's specific practices, concluding AmeriDebt is a "financial institution" under the GLB Act.[42] The Maryland district court went a step further, citing *Chevron U.S.A., Inc. v. NRDC* and concluding, "insofar as there may be ambiguity in the term 'financial institution,' the Commission's interpretation of the definition to embrace credit counseling services is entitled to the Court's deference."[43]

---

[36] *Id.*

[37] FTC v. AmeriDebt, Inc., 343 F. Supp. 2d 451, 453 (D. Md. 2004).

[38] *Id.* at 465.

[39] *Id.* (citing 15 U.S.C. § 6804(a)(1)).

[40] *Id.* at 457 (discussing 65 Fed. Reg. 33646, 33647 & 33658 (May 24, 2000)).

[41] *Id.* at 458 (quoting 16 C.F.R. § 313.3(k)(2)(xii); "an investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in 4(k)(4)(C)" of the Bank Holding Company Act).

[42] *See* FTC v. AmeriDebt, Inc., 343 F. Supp. 2d, at 461-62 (practices include brokering consumer's credit with various creditors, collecting payments from consumer, and transferring payments received to end creditors).

[43] *Id.* at 462 (discussing Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837, 104 S. Ct. 2778 (1984)).

2. DEFINING "AFFILIATE"

The Gramm-Leach-Bliley Act defined the term "affiliate" to mean "any company that controls, is controlled by, or is under common control with another company."[44] The GLB Act operates to enhance the ability of affiliated companies to share information more efficiently and effectively for cross-marketing purposes.[45] Although "affiliates" clearly create operating efficiencies for financial institutions, there are privacy concerns inherent in granting an entity "affiliate" power and therefore, federal courts are asked to determine whether a subsidiary constitutes an "affiliate" under the GLB Act.

In *Wachovia Bank v. Burke*, the federal district court of Connecticut determined whether the National Bank Act[46] and regulations promulgated by the Office of the Comptroller of the Currency ("OCC") preempt Connecticut state licensing statutes.[47] Specifically, Wachovia Bank claimed that the National Bank Act created "a system by which so-called 'national' banks would receive a federal charter and would be free from state 'visitorial' power except as permitted by law or court order."[48] Commissioner Burke conceded that he could not enforce the statutes against Wachovia Bank itself, but asserted his authority to regulate Wachovia Mortgage on the ground that it is a subsidiary of a "national bank."[49] In determining whether Wachovia Mortgage was a subsidiary, the court turned to the language of the GLB Act, finding "Congress singled out only financial subsidiaries, not operating subsidiaries, for treatment as national bank affiliates."[50] From this language, the court concluded that because the GLB Act authorized financial subsidiaries to conduct certain non-national bank functions formally forbidden, Congress made a decision to treat these financial entities as "affiliates" subject to state regulation.[51] Essentially, the court stated that national banks were able

---

[44] 15 U.S.C. § 6809(6).

[45] *See* Fischer, *supra* note 8, at ¶9.01[1][C].

[46] National Bank Act, 12 U.S.C. § 21 *et. seq.*

[47] Wachovia Bank, N.A. v. Burke, 319 F. Supp. 2d 275, 277 (2004).

[48] *Id.* at 278; *see* 12 U.S.C. § 484.

[49] *See Wachovia Bank*, 319 F. Supp. 2d at 281.

[50] *Id.* at 284 (citing 12 U.S.C. § 371c(e)(2)).

to engage in previously forbidden, non-commercial bank functions through their affiliates, and that these "financial" affiliates could be subject to state regulation.[52]

3. THE "NOTICE" REQUIREMENT

The GLB Act imposes an obligation on financial institutions to disclose their privacy policies to customers, both "[a]t the time of establishing a customer relationship" and on an annual basis so long as that customer maintains a relationship with the institution.[53] The Act also requires that financial institutions provide customers with notice and the opportunity to opt-out of the sharing of information with nonaffiliated third parties.[54] Under section 503 of the Financial Privacy Law, privacy policy notices must "'convey information that is critical to [a person's] decision making' regarding his personal data."[55] Senator Gramm stated that Congress intended the disclosure requirement to enable consumers to make educated choices among financial institutions that offer different privacy policies or disclosure practices.[56] The GLB Act requires that these privacy notices and the disclosure of opt-out provisions be made "clearly and conspicuously."[57] Instead of being "clear and conspicuous," however, the typical privacy notice offered by financial institutions is difficult to understand and is written in a manner that makes it difficult to exercise the option to-opt out.[58] Explanations of how to opt-out typically appear at the end of the privacy notice and are often never read and executed by customers.[59]

---

[51] *Id.*

[52] *See id.*

[53] 15 U.S.C. § 6803(a).

[54] 15 U.S.C. § 6802.

[55] Sammin, *supra* note 5, at 663-64 (quoting Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1225 (2002)).

[56] 145 CONG. REC. S13785-13786 (daily ed. November 3, 1999) (Statement of Sen. Gramm).

[57] 15 U.S.C. § 6802(b)(1)(A).

[58] Schiller, *supra* note 4, at 362; *see* Janger, *supra* note 55, at 1230–32.

[59] *Id.*

In response to these concerns, the Securities and Exchange Commission ("SEC") issued an "interagency proposal to consider alternative forms of privacy notices under the Gramm-Leach-Bliley Act."[60] In this proposal, various agencies[61] requested comment on whether the regulations that implement sections 502 and 503 of the GLB Act should be amended to allow or require financial institutions to provide alternative types of privacy notices that would be easier for consumers to understand (short-form notices[62]).[63] In this proposal, the agencies applauded efforts already made by consumer advocates and financial institutions to formulate short, consumer-friendly notices that accompany the longer, legally mandated notices under the GLB Act.[64] The agencies believed that the best approach to addressing the "notice" problem was to solicit comments from financial institutions on the "wide range of issues associated with the format, elements, and language used in privacy notices."[65]

The agencies' proposal focuses on the possible need for a short privacy notice that will improve the readability and usefulness of privacy notices.[66] The proposal identifies five possible approaches to simplify privacy notices:

---

[60] Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. 75164 (proposed Dec. 30, 2003), *available at* http://www.sec.gov/rules/concept/34-48966.pdf (interagency proposal between the financial privacy law enforcement "Agencies": the Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Federal Trade Commission, Commodity Futures Trading Commission, and the Securities and Exchange Commission).

[61] "Agencies" include: Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Federal Trade Commission, Commodity Futures Trading Commission, and the Securities and Exchange Commission.

[62] For examples of "short-form" opt-out notices: *see Privacy Rights Clearinghouse, Addendum to Fact Sheet 24(a), Sample Opt-Out Letters, Short Form, available at* http://www.privacyrights.org/fs/fs24a-formletter.htm (last viewed February 15, 2005), *The University of Texas at Arlington, Notice of Privacy Practices (Short Form), available at* http://www.uta.edu/health_services/Notice%20of%20Privacy%20Practices.pdf (last viewed February 15, 2005).

[63] *See* Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. at 75164.

[64] *Id.* at 75166.

[65] *Id.*

[66] *Id.* at 75167.

> (1) the development of a specific format and standardized language for a short notice that highlights key elements of an institution's privacy policy;
>
> (2) the development of a short notice with a specific format and standardized language designed to address all of the relevant elements listed in the GLB Act and the privacy rule;
>
> (3) establishing a standardized format for notices, but still allowing financial institutions to provide their own descriptions of their privacy policies and practices;
>
> (4) prescribing standardized language that financial institutions would use to design their own, specific notice without a format specified by the privacy rule; or
>
> (5) focusing attention on the consumer's right to opt-out of disclosures available under the institution's privacy policies.[67]

Although each of the policies would require regulatory implementation by the agencies, the policies clearly differ as to the agencies' actual involvement in formulating each institution's specific "short form" policy. For example, the second approach requires that all institutions develop a specific format using standardized language that addresses all of the relevant elements of the GLB Act.[68] Under this approach, privacy notices from all institutions would be very similar and could be ill suited to meet each institution's actual privacy concerns. On the other hand, the fourth approach, which allows institutions to develop their own privacy policy within the boundaries created by standardized language, would allow each institution to formulate policies specifically suited for its organization, while still providing consumers with the ability to compare institutions through standardized language.[69]

---

[67] *Id.*

[68] Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. at 75167.

[69] *Id.*

During 2004, the agencies received numerous responses to their request for information concerning the wide range of issues associated with the format, elements, and language to use in future privacy notices.[70] The agencies have yet to enter a final rule stating the official changes to GLB Act privacy notices. However, the agencies clearly favor the implementation of consumer-friendly notice requirements that efficiently describe the institution's privacy policies in a simple fashion, while meeting all the legal requirements for notice.[71]

4. PRIVATE RIGHT OF ACTION

During 2004, courts again held that the Gramm-Leach-Bliley Act "does not provide a private right of action for a financial institution's violation of the [GLB Act's] privacy provisions,"[72] with the *Borninski* and *Lacerte* courts citing the New York district court case of *Menton v. Experian Corporation*[73] as authority. In *Menton*, the court found that 15 U.S.C. § 6805(a) clearly restricted the GLB Act to government action and did not provide for a private right of action.[74]

C. INTERACTION WITH STATE LAWS

Over the past year, developments in the interaction between the GLB Act and state laws focused on state law preemption issues and the judicial process exception to the disclosure of nonpublic personal

---

[70] *See* Comment #5, America's Health Insurance Plans (Mar. 26, 2004) *available at* http://www.ftc.gov/os/comments/glbaltprivacynotices/03-31992-0005.pdf (last viewed February 15, 2005); Comment #10 Mary J. Culnan, Ph.D., *Comments on Advance Notice of Proposed Rulemaking*, (Mar. 29, 2004) *available at* http://www.ftc.gov/os/comments/glbaltprivacynotices/03-31992-0010.pdf (last viewed February 16, 2005); Comment #11, Household Automotive Finance Corporation (Mar. 29, 2004) *available at* http://www.ftc.gov/os/comments/glbaltprivacynotices/03-31992-0011.pdf.

[71] *See* Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. at 75166.

[72] Borninski v. Williamson, 2004 WL 433746, at *3 (N.D. Tex. Mar. 1, 2004); *see also Lacerte Software Corp.*, 2004 WL 180321, at *2 (N.D. Tex. Jan. 6, 2004).

[73] Menton v. Experian Corp., 2003 WL 21692829, at *3 (S.D. N.Y. Jul. 21, 2003).

[74] *See id.* (quoting 15 U.S.C. § 6805(a))("This subchapter and the regulations prescribed thereunder shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to the financial institutions and other persons subject to their jurisdiction . . .").

information. State law preemption issues were raised in California,[75] Massachusetts,[76] and Vermont.[77] The judicial process exception was invoked by state courts in Alabama[78] and West Virginia[79] as a means of permitting state courts to require the disclosure of nonpublic personal information during the litigation process.

1. STATE PREEMPTION ISSUES – THE CALIFORNIA PRIVACY LAW

The California Information Privacy Act ("California Privacy Law") became operative on July 1, 2004.[80] The California Privacy Law affords Californians greater protection over their personal financial information than those provided by the GLB Act.[81] The California Privacy Law and the GLB Act do not share the same exceptions from disclosure restrictions, nor apply exceptions to the same entities.[82] Further complicating matters is the effect of the *Bank of America v. City of Daly City* decision,[83] holding that local California ordinances regarding affiliate sharing of nonpublic personal information are preempted by the Federal Fair Credit Reporting Act ("FCRA").[84] The *Bank of America* decision raised the question that the California Privacy Law may also be preempted by federal law.

---

[75] *See* Am. Bankers Ass'n v. Lockyer, 2004 WL 1490432 (E.D. Cal. June 30, 2004); *see also* Bank of Am. v. City of Daly City, Cal, 279 F. Supp. 2d 1118 (N.D. Cal. 2003).

[76] *See* Mass. Bankers Ass'n v. Bowler, U.S. Dist. LEXIS 348 (D. Mass. Jan. 10, 2005) (slip copy).

[77] *See* Am. Council of Life Insurers v. Vt. Dep't of Banking, 2004 WL 578737 (Vt. Super. Feb. 12, 2004).

[78] *See ex parte* Nat'l W. Life Ins. Co. v. Farmer, 2004 WL 2260308 (Ala. Oct. 8, 2004); *Ex parte* Mutual Sav. Life Ins. Co., 2004 Ala. LEXIS 262 (Ala. Oct. 8, 2004).

[79] *See* Martino v. Barnett, 215 W.Va. 123, 595 S.E.2d 65 (2004).

[80] CAL. FIN. CODE § 4060 (West 2004).

[81] Elizabeth A. Huber & Elena A. Lovoy, *Update on State Consumer Financial Privacy Legislation and Regulation*, 59 BUS. LAW. 1227, 1228 (2004).

[82] *Id.*

[83] *See Am. Bankers Ass'n*, 2004 WL 1490432, at *5 (stating that the *Bank of America* decision has been vacated by the Ninth Circuit and lacks precedential authority); *see generally* Bank of Am., 279 F. Supp. 2d 1118.

[84] *Bank of Am.*, 279 F. Supp. 2d at 1128–29.

In response to the *Bank of America* holding, three financial services trade associations brought a collective action, asking the court to declare the affiliate sharing provision of the California Privacy Law void and unenforceable. The trade associations claimed it was expressly preempted by the FCRA.[85] In particular, the plaintiffs sought to overturn the California Privacy Law's restrictions on the dissemination of personal financial information between affiliated business institutions.[86] In its defense, the state of California contended that passage of the California Privacy Law was proper "[b]ecause § 6807(b) of the [GLB Act] expressly allows states to enact consumer protection statutes providing greater privacy protection."[87] In addressing the issue, the California district court looked at the stated purpose of the FCRA and concluded that the "only reasonable reading of the FCRA preemption provision is that it prevents states from enacting laws that prohibit or restrict the sharing of consumer reports among affiliates."[88] The court rejected the plaintiffs' argument that the FCRA preemption provision broadly preempted all state laws regulating information sharing by affiliates.[89] The California district court then looked to the GLB Act for support, finding that the Act encompassed the general sharing of consumer information between affiliates.[90] In applying the GLB Act to the "affiliate sharing provisions," the court first examined the legislative history of the Act, finding that Congress intended to allow more rigorous state regulation.[91] Based on this finding, the California district court held that Congress clearly "intended that states to be afforded the right to regulate consumer financial privacy on behalf of their citizens in adopting statutes more protective in that regard than the provisions of the [GLB Act]."[92]

---

[85] *Am. Bankers Ass'n*, 2004 WL 1490432, at *1.

[86] *Id.*

[87] *Id.* at *2.

[88] *Id.* at *4.

[89] *Id.*

[90] *Am. Bankers Ass'n*, 2004 WL 1490432, at *5.

[91] *See id.* (citing a Conference Report that confirms under the GLB Act, "States can continue to enact legislation of a higher standard than the Federal standard"; 145 CONG. REC. S13915 (Nov. 4, 1999)).

[92] *Id.*

On June 30, 2004, the California district court held that the California Privacy Law was not preempted by the FCRA because the limitations on the sharing of personal financial information were specifically discussed in the GLB Act, which "allow[ed] states to enact more stringent privacy regulations."[93] Plaintiffs immediately appealed the decision to the United States Court of Appeals for the Ninth Circuit. In response to the appeal, numerous financial institutions and privacy groups submitted briefs to the Ninth Circuit in support of both parties. On August 11, 2004, the federal agencies ("Agencies") responsible for enforcing federal financial privacy laws[94] filed an *amicus curiae* brief in support of American Bankers Association.[95] The Agencies' brief looked to the language of the FCRA, as amended by the Fair and Accurate Credit Transaction ("FACT") Act, and argued that "[n]othing in the text of FCRA preemption provision at issue even hints that its scope is limited only to state laws regulating consumer reports."[96] The Agencies' brief also highlighted the language and legislative history of the FACT Act, arguing that it unambiguously supported the conclusion that the FCRA preemption provision, as amended by the FACT Act, was intended to preempt state laws limiting the sharing of information among all affiliates, not just state laws dealing with "consumer reports."[97]

The appellees, the State of California, *et al*, continued to argue that the FCRA is limited to "consumer reports" as defined by section 1681a(d)(1) of the statute.[98] In support, the state presented specific textual evidence it claimed establishes that neither the FCRA nor the

---

[93] *Id.* at *6.

[94] Agencies include: Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Federal Trade Commission, Commodity Futures Trading Commission, and the Securities and Exchange Commission.

[95] Amicus Curiae Brief of Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Federal Trade Commission, Commodity Futures Trading Commission, and the Securities and Exchange Commission in Support of Appellants American Bankers Association, et al., (filed Aug. 11, 2004), *available at* http://www.ftc.gov/ogc/briefs/lockyer.pdf.

[96] *Id.* at 19.

[97] *Id.* at 20.

[98] Brief of Appellees California Attorney General Bill Lockyer et al., Am. Bankers Ass'n v. Lockyer, 2004 WL 2606248, at 39 (9th Cir. Oct. 13, 2004)(Nos. 04-16334, 04-16560).

FACT Act demonstrated that Congress intended to establish uniform national standards with respect to all affiliate sharing.[99] Specifically, California cited the strong presumption against preemption where a state exercised its historic police power to protect consumers, while also pointing to the FCRA exclusion clause in the GLB Act for supportive textual evidence.[100] The state urged that the court look to the "clear and unequivocal expression of congressional intent" found in the GLB Act, where "Congress explicitly preserved the right of states to enact more protective laws."[101]

While the Ninth Circuit has yet to hear the case on appeal, these "affirmative consent" rules are in place in a number of states, and many more states are considering adding similar requirements.[102] The first courts to address federal challenges to state privacy legislation have upheld the opt-in requirement as permissible.[103] All courts, including the Ninth Circuit, have recognized that the GLB Act allows for states to enact privacy legislation of a higher standard than the federal standard.[104] Therefore, it appears the Ninth Circuit's decision will focus on the proper interpretation of the FCRA's preemption provision and whether the provision is intended to preempt state laws limiting the sharing of information among all affiliates, or only affiliates dealing with consumer reports.

2. STATE PREEMPTION ISSUES – MASSACHUSETTS AND VERMONT

In May 2000, the Massachusetts Bankers Association, Inc. ("MBA") requested the opinion of the Office of the Comptroller of the Currency ("OCC"), the primary regulator of federally chartered banks, on whether the GLB Act preempted certain provisions of the Massachusetts Consumer Protection Act Relative to the Sale of

---

[99] *Id.* at 34.

[100] *Id.*

[101] *Id.* at 70-71.

[102] Christopher Wolf, *The Gramm-Leach-Bliley Act: Current Developments 2004*, 789 PLI/PAT 715, 727 (2004).

[103] Am. Council of Life Insurers v. Vt. Dep't of Banking, 2004 WL 578737 (Vt. Super. Feb. 12, 2004).

[104] *See Am. Bankers Ass'n, supra* note 75.

Insurance by Banks.[105] The OCC responded that the provisions were preempted by federal law.[106] Thereafter, pursuant to 15 U.S.C. § 6714(a), the Massachusetts Commissioners of Insurance and Banks and the Commonwealth of Massachusetts sought review in the First Circuit Court of Appeals of the "regulatory conflict" resulting from the OCC opinion.[107] After review, the First Circuit dismissed the case for lack of jurisdiction because the court found there was no regulatory conflict.[108]

In response to this ruling, MBA and other Massachusetts banks brought a collective action challenging four provisions of Massachusetts law, which they labeled as the Referral Prohibition,[109] the Referral Fee Prohibition,[110] the Waiting Period Restriction,[111] and the Separation Restriction.[112] MBA argued that the four challenged provisions were preempted by the GLB Act, pointing specifically to section 6701(d)(2)(A) of Title 15 of the United States Code, which states: "no State may, by statute, regulation, order, interpretation, or other action, prevent or significantly interfere . . . with an affiliate or other person, in any insurance sales, solicitation, or cross marketing activity."[113] Upon review, the court stated that the determinative issue was "whether any of the challenged provisions 'prevent or

---

[105] Mass. Bankers Ass'n v. Bowler, 2005 U.S. Dist. LEXIS 348, at *2 (D. Mass. Jan. 10, 2005) (slip copy).

[106] *Id.* at *3.

[107] *Id.*

[108] Bowler v. Hawke, 320 F.3d 59, 64 (1st Cir. 2003).

[109] *See Mass.Bankers Ass'n*, 2005 U.S. Dist. LEXIS 348, at *4 (the Referral Provision "allows officers, tellers, and other bank employees who are not licensed insurances agents to refer a bank customer to a licensed insurance agent only when the customer inquires about insurance").

[110] *See id.* at *5 (the Referral Fee Prohibition "forbids banks from paying their employees from making the referrals to their insurance agents").

[111] *See id.* (restriction which allows banks to solicit insurance sales to loan applicants only after the application for the extension of credit is approved and all necessary disclosures are communicated to and acknowledged by applicant in writing).

[112] *See id.* (requires that insurance solicitations be conducted in a physically separate area of bank).

[113] *Id.* at *6, 7 (quoting 15 U.S.C. § 6701(d)(2)(A)).

significantly interfere' with the ability of banks to sell, solicit, or cross market insurance."[114] Applying this standard, the court found that each of the Massachusetts laws challenged seriously "impedes plaintiffs' [Massachusetts banks] ability to solicit, cross market and sell insurance products" and are preempted by the GLB Act.[115] In a final statement, the court also concluded that its decision was based on deference to the GLB Act and not the 2000 OCC opinion.[116]

In November 2001, the Vermont Department of Banking, Insurance, Securities, and Healthcare Administration ("BISHCA") created an "opt-in" system for the disclosure of nonpublic financial and health information by licensees.[117] In response to this regulation, five insurance trade organizations subject to the new Vermont Regulation sought a declaratory judgment invalidating the Regulation, arguing that it fell outside BISHCA's statutory authority and violated constitutional protections.[118] The court looked to the GLB Act for guidance, finding that the GLB Act's opt-out and related privacy provisions set a floor for consumer protection, superceding state laws except insofar as they provide greater protection.[119] In applying the GLB Act in light of the Vermont Regulation, the court found that the opt-in provision of the Regulation and the opt-out provision of the GLB Act both served the same substantial interests of protecting consumer's privacy.[120] The court held that because the Vermont Regulation provided greater privacy protection than the parallel GLB provision, the Regulation was not superceded and was therefore

---

[114] *Mass. Bankers Ass'n*, 2005 U.S. Dist. LEXIS 348, at *7, 8.

[115] *Id.* at *12, 13.

[116] *Id.* at *13.

[117] *See* Am. Council of Life Insurers v. Vt. Dep't of Banking, 2004 WL 578737, at *1 (Vt. Super., Feb. 12, 2004); *see also* William A. Darr, Commissioner of Illinois Office of Banks and Real Estate, *letter to FTC* (July 16, 2001); *available at* http://www.ftc.gov/privacy/glbact/illinoispetition.pdf (letter seeking preemption determination on a Illinois statute that provides customers with an "opt-in" provision, no response as of Feb. 15, 2005).

[118] *Am. Council of Life Insurers*, 2004 WL 578737, at *1.

[119] *Id.* at *2.

[120] *Id.* at *6.

enforceable so long as the opt-in strategy did not violate plaintiffs' constitutional rights.[121]

3. THE JUDICIAL PROCESS EXCEPTION

During 2004, several states addressed the issue of whether the disclosure of "nonpublic personal financial" information by financial institutions during the discovery process was a violation of the GLB Act. In both Alabama and West Virginia, state supreme courts held that the GLB Act permited financial institutions to disclose a customer's nonpublic personal financial information to comply with a discovery request in a state action.

In *Ex parte Mutual Savings Life Insurance Company*, the Supreme Court of Alabama held that the trial court was correct in ordering Mutual Savings to "disclose its customers' nonpublic personal information without providing notice to those customers engaging in the opt-out requirement."[122] The court found Congress created an exception applicable to situations where "the trial court orders the disclosure of a customer's nonpublic personal information during discovery in a civil action."[123] The court concluded by stating that courts "should also issue a comprehensive protective order to guard the customers' privacy."[124]

In a similar case, the Supreme Court of Appeals of West Virginia concluded that "the [GLB Act] and the Privacy Rule [FTC's final rule] allow the use of any judicial process expressly authorized by statute or court rule, whether by way of discovery or for any other purpose expressly authorized by law," to obtain relevant information.[125] The court chose to extend the "judicial process exception" past

---

[121] *See id.* at *6–7 (court finds that the Regulation's opt-in strategy does not violate Plaintiffs' commercial speech rights).

[122] *Ex parte* Mutual Savings Life Ins. Co., 2004 Ala. LEXIS 262, at *14–15 (Ala., Oct. 8, 2004); *see also Ex parte* Nat'l W. Life Ins. Co., 2004 WL 2260308 (Ala., Oct. 8, 2004).

[123] *Ex parte Mutual Savings Life Ins. Co.*, 2004 Ala. LEXIS 262, at *14 (The court bases its decision on a finding that a plain reading of the GLB Act revealed that "the phrase 'to respond to judicial process' is independent from the phrase 'to respond to . . . government regulatory authorities. . .'" Through this finding, the court concluded that the "to respond to judicial process" provision provides an exception for situations where a party discloses information pursuant to a court order).

[124] *Id.* at *15–16.

[125] *See Martino*, 595 S.E. 2d at 72.

"discovery," stating "no such limitation to application of the term 'judicial process' appears in the [GLB Act] exception."[126] Although the West Virginia Court seemingly extended the exception to all parts of the trial process, the court remained mindful of the purposes of the GLB Act, instructing that it was important to balance the strong interests involved in protecting the privacy of consumers' financial information against the importance of full disclosure of any matter that is relevant to the claim or defense of any party.[127] To this end, the West Virginia Court stated that trial courts have a duty to balance these interests and issue protective orders which "limit access to necessary information."[128]

Over the past year, state courts have interpreted the language of the GLB Act to provide an explicit "judicial process" exception that provides state courts with the authority to order financial institutions to disclose customers' nonpublic personal financial information, in order to comply with discovery requests in state actions. However, these decisions also recognized the importance of the GLB Act's privacy protection provisions and have generally required that courts issue comprehensive protective orders to guard against abuse and misuse of customers' private information.

D. HOT TOPICS CONCERNING GLB ACT

1. STATE PREEMPTION ISSUES – CALIFORNIA PRIVACY LAW

The Ninth Circuit has yet to hear the *American Bankers Association* case on appeal from the eastern district of California holding that the California Privacy Law was not preempted by the Fair Credit Recording Act. In this case, the California district court concluded that the FCRA's regulatory power was limited to affiliates dealing with "consumer reports" and that the limitations on the sharing of personal financial information found in the Gramm-Leach-Bliley Act allowed states to enact more stringent privacy regulations.[129]

These types of "affirmative consent" rules are already in place in a handful of states with many more considering adding similar

---

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Am. Bankers Ass'n*, 2004 WL 1490432, at *6.

requirements.[130] The first courts to address federal challenges to state privacy legislation have upheld the opt-in requirements as permissible under both the FCRA and the GLB Act.[131] All jurisdictions, including the Ninth Circuit, recognize that the GLB Act allows for states to enact privacy legislation of a higher standard than the federal standard.[132] Therefore, it appears the Ninth Circuit's decision will focus on the proper interpretation of the FCRA's preemption provision and whether the provision is intended preempt state laws limiting the sharing of information among all affiliates, or just affiliates dealing with consumer reports.

2. THE EUROPEAN UNION'S PRIVACY DIRECTIVE

The United States and the European Union devised a Safe Harbor Agreement[133] to facilitate trade between the groups while not compromising on data privacy following the enactment of the European Union's Privacy Directive in 1998.[134] The E.U. deemed the GLB Act insufficient to meet the requirements of the Safe Harbor Agreement, citing a lack of customer "access" and "opt-in" provisions.[135] Negotiations are at a standstill, with U.S. negotiators arguing that Europeans should accept the GLB Act as adequate protection, and E.U. negotiators stating that their position is "not something to be negotiated."[136] This refusal to compromise has left financial services under a standstill agreement where no enforcement

---

[130] Christopher Wolf, *The Gramm-Leach-Bliley Act: Current Developments 2004*, 789 PLI/PAT 715, 727 (2004); *see also* Mark E. Budnitz, *Consumer Privacy in Electronic Commerce: As the Millennium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 821, 883 (2000).

[131] *Am. Council of Life Insurers*, 2004 WL 578737 (Vt. Super. Feb. 12, 2004).

[132] *See Am. Bankers Ass'n*, 2004 WL 1490432, at *5 (citing a Conference Report that confirms under the GLB Act, "States can continue to enact legislation of a higher standard than the Federal standard;" 145 Cong. Rec. S13914 (Nov. 4, 1999)).

[133] The Safe Harbor Agreement is a comprehensive data sharing privacy policy that focuses on seven principles: (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement; *see* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,667-45,668 (July 24, 2000).

[134] Sammin, *supra* note 5.

[135] *Id.* at 654, 664.

[136] *Id.* at 654.

action will be taken so long as "the U.S. and E.U. officials continue their 'good faith' negotiations."[137]

The recent judicial enforcement of state statutes and regulations that supercede the minimum requirements of the GLB Act may help strengthen the United States' position in arguing that the GLB Act meets the requirements of the Safe Harbor Provision. For example, states such as California[138] and Vermont,[139] have enacted state legislation increasing privacy restrictions for affiliate sharing and providing customers with the opportunity to "opt-in" to disclosure notices. These statutes appear to meet many of the E.U.'s "sticking points" with the GLB Act and may help the E.U. and the U.S. work toward a compromise.

E. GRAMM-LEACH BLILEY ACT AND THE FUTURE

Under current trends, the continued enactment of privacy statutes by state legislatures and subsequent certification by federal courts will lead to an erosion of the foundations of the GLB Act. However, this erosion may be necessary to ensure the protection of American citizens' nonpublic personal information. The Gramm-Leach-Bliley Act was a congressional attempt to facilitate the efficient and open sharing of consumer information throughout the financial services industry. In eliminating "the barriers on affiliation between banks, insurance, and securities industries," Congress hoped that "one-stop" shopping for financial services could generate efficiencies in the industry, thereby reducing transaction costs for institutions and increasing profitability.[140] The GLB Act attempts to balance these efficiencies with customers' rights to privacy by requiring financial institutions to comply with the notice and opt-out disclosure provisions. The "affiliate sharing" and "opt-out" provisions are essential to cost-efficient sharing of information among integrated

---

[137] *Id.* (citing Kerry A. Kearney & P. Gavin Eastgate, *Financial Services Should Meet Privacy Standards*, LEGAmedia, Nov. 2000 (inaccessible website)).

[138] *See* CAL. FIN. CODE § 4060 (West 2004) (affords Californian's greater protection over their personal financial information than those provided by the GLB Act).

[139] Vermont Department of Banking, Insurance, Securities, and Healthcare Administration Regulation IH-2001-01, Nov. 17, 2001 (creating an "opt-in" system for the disclosure of nonpublic financial and health information); *see also Am. Council of Life Insurers*, 2004 WL 578737 at *1.

[140] Schiller, *supra* note 4, at 355.

financial services companies, and have generated the most controversy in states attempting to provide greater protection. Under the GLB Act, nonpublic personal information may be shared among all affiliates, once the consumer has received notice indicating such information may be disclosed and has chosen not to opt for nondisclosure. Citing to the GLB Act's provision that expressly allows states to enact consumer protections statutes providing greater privacy protection, states have responded by enacting provisions that require "opt-in" disclosure and place greater restrictions on affiliate sharing.

State "affiliate sharing" restrictions and "opt-in" disclosure requirements are in clear conflict with the GLB Act's overarching goal of facilitating the efficient and open sharing of consumer information throughout the financial services industry. Proponents of these state statutes argue that the statutes operate effectively to supplement the GLB Act, by providing consumers with greater privacy protections and a better understanding of the actual purpose of notice and disclosure requirements.[141] Opponents, on the other hand, argue that Congress expressly chose to use "opt-out" language to provide for an effective sharing of more information.

The United States' financial privacy framework will continue to evolve in response to external forces throughout the world. Although the United States plainly values the free flow of information and the rewards that come from these open channels, it remains unclear how far states will go in restricting that flow of information out of the necessity to protect their citizens' personal financial privacy.

III. THE FAIR CREDIT REPORTING ACT & FAIR AND ACCURATE CREDIT TRANSACTION ACTS

A. INTRODUCTION

The Fair Credit Reporting Act ("FCRA") was enacted in 1970[142] and was the first significant effort to address personal privacy on the federal level. It provides consumers with protection from incorrect and inappropriate disclosures of personal information from consumer reporting agencies.[143] Congress's goal in passing the FCRA was to

---

[141] *Id.* at 367.

[142] Fair Credit Reporting Act, Pub. L. No. 91-508, § 601, 84 Stat. 1114, 1128 - 1136 (1970) (codified at 15 U.S.C. §§ 1681 - 1681t).

[143] Partnership to Protect Consumer Credit, *Fair Credit Reporting Act Summary, at* http://www.protectconsumercredit.org/legislative/updates.asp (last visited Feb. 19, 2005).

require credit bureaus and similar organizations to adopt reasonable procedures that balance the need for information in the commercial context with the necessity of protecting consumer privacy.[144] Specifically, the congressional purpose in passing the FCRA was "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[145] The primary focus of the FCRA is to ensure fair and accurate information in credit and other reports on consumers. Credit reporting agencies ("CRAs") collect information on consumers' creditworthiness based on public records, information from financial institutions, and other sources that total over two billion transactions per month.[146] Millions of businesses rely on the reports from these agencies to provide services and products to more than 180 million consumers.[147]

The FCRA requires CRAs to disclose personal credit information under limited circumstances and to follow reasonable procedures for the collection and maintenance of credit and similar data,[148] and gives customers the right to correct inaccurate information in their files.[149] It also allows consumers to have summaries of their disputes with these agencies and updated information included with their credit reports.[150] However, "in exchange for these rights and obligations, the FCRA restricts the rights of consumers to sue under state law governing defamation, negligence, and invasion of privacy for inaccuracies in these reports and in information that organizations provide to credit bureaus and other consumer reporting agencies."[151]

In 1996 the Act was substantially modified to clarify obligations of reporting agencies, and to create new obligations on existing

---

[144] 15 U.S.C. § 1681(b).

[145] 15 U.S.C. § 1681(a)(4).

[146] Partnership to Protect Consumer Credit, *supra* note 143.

[147] *Id.*

[148] 15 U.S.C. §§ 1681b, 1681c, 1681e(b), 1681k, 1681ll, 1681m.

[149] 15 U.S.C. §§ 1681li, 1681s-2.

[150] 15 U.S.C. § 1681li(b).

[151] L. Richard Fischer, *Fair Credit Reporting Act*, THE LAW OF FINANCIAL PRIVACY, ¶ 1.01 (A.S. Pratt & Sons 2004); *see* 15 U.S.C. § 1681h(e).

organizations that furnish information to these agencies.[152] The revision also established the FCRA as the uniform national standard and preempted all applicable corresponding state laws.[153] In summary, the FCRA restricts dissemination of consumer reports for certain "permissible purposes," as defined in 15 U.S.C. § 1681b, and otherwise prohibits disclosure of consumer information by consumer reporting agencies, and attempts to prevent the distribution of information that may be either obsolete or inaccurate.[154] The 1996 Amendments also included a sunset provision "to prompt Congressional review of the impact of the... amendments after such time that the full range of their effects on credit markets could be comprehensively evaluated."[155] The sunset provision expired on January 1, 2004.[156]

Partially in response to the expiration of the 1996 Amendment provisions, the Fair and Accurate Credit Transactions Act of 2003, ("FACT Act"), was signed into law on December 4, 2003.[157] It permanently reauthorized the national uniformity provisions of the FCRA and strengthened the national credit reporting system, in an effort to protect consumers and financial institutions against identity theft. The FACT Act's purpose was to create a uniform national standard to enhance and govern the development of a national recording system.[158] President Bush's office proclaimed, "the legislation will provide consumers, companies, consumer reporting agencies, and regulators with important new tools that expand access to credit and other financial services for all Americans, enhance the accuracy of consumers' financial information, and help fight identity theft."[159] Specifically, "the overwhelming votes by which the House and Senate bills and the final FACT Act was passed, combined with

---

[152] Pub. L. No. 104-208, §§ 1401-1420, 110 Stat. 3009, 3009-426-3009-454 (1996).

[153] 15 U.S.C. § 1681t.

[154] 15 U.S.C. §§ 1681c, 1681e(b).

[155] S. REP. No. 108-166 at 6 (2003).

[156] 15 U.S.C. § 1681t(d)(2)(A).

[157] Pub. L. No. 108-159, 117 Stat. 1952 (2003).

[158] S. REP. No. 108-166 at 6 (2003).

[159] *Fact Sheet: President Bush Signs the Fair and Accurate Credit Transaction Act of 2003, available at* http://www.whitehouse.gov/news/releases/2003/12/print/20031204-3.html (last visited Feb. 19, 2005).

the significant support that each bill received by both parties in Congress, was demonstrative of a legislative process characterized by a 'bipartisan, bicameral effort' and was reflective of the priority and the urgency that Congress placed on amending the FCRA."[160] Ultimately, the support for the FACT Act has been wide-ranging.[161]

The FCRA was designed to help prevent identity theft, and to that end Congress looked at several widely reported surveys including a September 2003 report by the FTC, which estimated that nearly ten million people were victims of identity theft in 2002.[162] The FACT Act allows for free annual consumer credit reports,[163] an improved accuracy standard for information that is furnished to credit reporting agencies,[164] and access to credit scores from credit reporting agencies for a reasonable fee.[165] The statute includes multiple measures to prevent identity theft, including a duty of creditors to take precautionary steps if a fraud alert is in a credit file or accompanies a credit score before granting credit.[166] Commentators note, however, that while Congress responded to the prevalence of identity theft and the importance of accuracy of consumer credit files with the FACT Act, it is not a comprehensive solution to identity theft, and "Congress left much work for states to do."[167] States have found it challenging to

---

[160] Fischer, *supra* note 151, at ¶ 1.01.

[161] *See* Jill Schachner Chanen, *Consumer Complaints*, A.B.A. J., Dec. 2004, 51.

[162] Federal Trade Commission, *Identity Theft Survey Report, September 2003, available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited Feb. 29, 2005). The survey found that 27.3 million Americans have been victims of identity theft from 1998-2002, including 9.91 million people or 4.6% of the population in 2002 and that 52% of all ID theft victims, approximately 5 million people in 2002, discovered that they were victims of identity theft by monitoring their accounts. On January 26, 2005, the Better Business Bureau released its Identity Theft Survey as an update to the FTC 2003 report. *Available at* http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html (last visited Feb. 19, 2005). It found that in 2004, 9.3 million Americans were victims of identity theft and that the total annual identity fraud when adjusted for inflation remains essentially unchanged.

[163] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 211, 117 Stat. 1952 (2003).

[164] *Id.*

[165] Fair and Accurate Credit Transaction Act § 212(e).

[166] Fair and Accurate Credit Transaction Act § 111.

[167] Hillebrand, Gail. *After the FACTA: State Power to Prevent Identity Theft.* 17 LOY. CONSUMER L. REV. 53, 58 (2004).

reconcile the provisions in the FACT Act with their own protection statutes.

B. FCRA, THE FACT ACT, AND PREEMPTION FOR IDENTITY THEFT

The general rule under the FCRA favors non-preemption in the absence of inconsistencies with provisions of the federal Act.[168] To clarify the general language in the FCRA, the FACT Act qualifies preemption as pertaining to laws "for the prevention or mitigation of identity theft."[169] As such, state laws regarding identity theft are preempted by the FCRA only when they are inconsistent with a provision of the FCRA. The legislative history is clear on this issue, and the Oxley-Bachus[170] legislative history notes that "no state or local jurisdiction, may add to, alter or affect the rules established by statute or regulations thereunder in any of these...areas," and explicitly states that the federal preemption provision regarding identity theft is governed "solely by federal law and any State action that attempts to impose requirements or prohibitions in these areas would be preempted."[171] Although the FACT Act permanently extends the seven areas of preemption that were added in the 1996 Amendments,[172] "national consumer organizations have called this a

---

[168] Fair Credit Reporting Act § 625(a).

[169] Fair and Accurate Credit Transactions Act § 711(1) (amending 15 U.S.C. § 1681t(a) (2004)).

[170] The "Section-by-Section Summary of H.R. 2622" submitted by Representative Michael Oxley, Chairman of the House Financial Services Committee, and Representative Spenser Bachus, Chairman of the Subcommittee on Financial Institutions and Consumer Credit is refered to as the Oxley-Bachus report or the Oxley-Bachus legislative history. *See* The Fact Act Compliance Manual, *available at* http://www.sheshunoff.com/store/media/pdf/h87_htu.pdf (last visited May 14, 2005).

[171] Fischer, *supra* note 161, at ¶ 1.10[2][c]; *see* 149 CONG. REC. E2519 (daily ed. Dec. 8, 2003).

[172] Six of the seven of these preemptions apply "with respect to any subject matter regulated under" listed sections or subsections. Fair and Accurate Credit Transactions Act § 711(3) (amending 15 U.S.C. § 1681t(b)(1) (2004)). These are § 1681b (prescreening of consumer reports), § 1681i (how long a consumer reporting agency must take action related to disputed information in a customer's file), § 1681m(a,b) (duties of a person who takes adverse action with a consumer), § 1681m(d) (duties of those who use consumer reports in connection with credit or insurance transactions not initiated by consumer that result in a firm offer of credit or insurance), § 1681c (information contained in consumer reports), § 1681s-2 (responsibilities of persons who furnish information to credit reporting agencies). The seventh, FCRA

major loss for consumers because federal preemption systems stymie the development of new consumer protections to respond to both old and new credit related problems."[173] Additionally, the FACT Act adds three sections to the "subject matter regulated under" form of the FCRA preemption.[174]

The first is § 609(a), which requires a business that provided an identity thief credit, products, or services, to provide the victim of the identity theft with copies of an application and the reasonably available business transaction records within its control.[175] In the absence of support from law enforcement agencies, which are often unresponsive to these frequently low-dollar amount claims, those who have fallen victim to identity theft must often investigate themselves, and one can use the information provided under this provision to help stop the identity thieves. Because § 609(a) falls under the "subject matter regulated under" preemption provision, states are limited in their ability to enact laws in this area. "For example, state laws that shorten the 30 day time period or provide for an alternative way to trigger the right to receive this information are highly likely to be preempted."[176] But, state laws that provide greater consumer protections are not likely to be preempted.[177]

Secondly, the FACT Act adds § 624 to the FCRA, which states that unless a consumer is given a chance to opt-out, the exchange and use of a consumer's information to make a solicitation for marketing purposes is prohibited.[178] But, the "subject matter regulated under" preemption describes the subject matter as "relating to the exchange and use of information to make a solicitation for marketing purposes,"[179] and the description is broader than the subject matter of

---

§ 624(b)(2), renumbered § 625(b)(2), is not included under the "subject matter regulated under" language.

[173] Hillebrand, *supra* note 167, at 59.

[174] Fair and Accurate Credit Transactions Act § 151(a)(2) (amending 15 U.S.C. § 1681t(b)(1)(G)-(I) (2004)) (citing Fair and Accurate Credit Transactions Act §§ 214(c)(2), 311(b)).

[175] Fair and Accurate Credit Transactions Act § 151(a) (amending 15 U.S.C. § 1681t (2004).

[176] Hillebrand, *supra* note 167, at 63.

[177] *Id.* at 81-82.

[178] Fair and Accurate Credit Transactions Act § 214. The language only regulates use of information for marketing purposes, but does not regulate the sharing of information.

[179] *Id.*

the section, resulting in some confusion. "Such preemption should extend, at the most, to state laws imposing conditions or restrictions on the use of personal financial information obtained from an affiliate for marketing solicitations and not for other purposes, such as credit or insurance underwriting."[180] Ultimately, the scope of any new preemption of state affiliate sharing laws is not entirely clear.

The third portion of the FCRA that was added to the "subject matter regulated under" preemptions is § 615(h), which relates "to the duties of users to provide notice with respect to terms in certain credit transactions."[181] This section requires notice to the consumer when, based on a consumer report, the terms offered are materially less favorable than the most favorable terms available to a "substantial proportion" of consumers via that lender or broker.[182] This part was included because information in a consumer's credit file could lead to the consumer being offered less favorable credit terms, yet lenders claimed that they were not obligated to give a notice of adverse action. "The risk-based pricing notice is essentially a counterpart to the notice of adverse action, a type of notice for which state laws were already preempted under FCRA."[183] As such, applying the "subject matter regulated under" preemption to the risk-based pricing notice preempts state law in an area where the 1996 amendments have effectively prevented the states from acting.[184]

C. THE FACT ACT STANDALONE PREEMPTION SECTIONS: CREDIT SCORE DISCLOSURE & ANNUAL FREE REPORTS

Having good credit is increasingly important to Americans, but a 2004 study from the Consumer Federation of America found that "most consumers do not understand the meaning of credit scores, their importance, how to obtain them, and how to improve them."[185]

---

[180] Hillebrand, *supra* note 167, at 64.

[181] Fair and Accurate Credit Transactions Act § 311(a).

[182] Fair and Accurate Credit Transactions Act § 311.

[183] Hillebrand, *supra* note 167, at 66.

[184] *Id.*

[185] Consumer Federation of America, *Most Consumers do not Understand Credit Scores According to a New Comprehensive Survey*, *available at* http://www.consumerfed.org/092104creditscores.PDF (last visited Feb. 19, 2005).

Specifically, only about 34% understand that credit scores indicate the risk of not repaying a loan as opposed to factors such as financial resources or consumer credit knowledge.[186] The study found that few consumers even know what constitutes a good score, and many have no clear idea of how they can improve their score.[187] The credit score preemption under the FACT Act is narrow and applies to disclosures under § 609(b), which addresses consumer reporting agency disclosure of credit scores for credit granting purposes, and under § 609(g), which addresses mortgage lenders and brokers.[188] The preexisting state credit score disclosure laws in California[189] and Colorado[190] are expressly exempted from preemption. States should remain free to regulate disclosure of credit scores from non-home secured lenders and with respect to issues other than disclosure.[191] "States can regulate credit score disclosure by consumer reporting agencies when credit scores are generated or used for purposes other than credit granting purposes."[192] The FACT Act explicitly gives states authority over insurance scoring.[193]

To promote further the availability of credit reports to individuals interested in monitoring unauthorized activity that may be the result of identity theft, the FACT Act added § 612(a) which provides for a free annual credit report.[194] A 2004 report from the National Association of State Public Interest Research Groups ("PIRGs") studied the three major credit bureaus – Experian, Equifax, and Trans Union, which maintain files on nearly 90% of all American adults.[195] The study

---

[186] *Id.*

[187] *Id.*

[188] Fair and Accurate Credit Transactions Act § 212(b) (amending 15 U.S.C. § 1681t(b)(3) (2004)).

[189] CAL. CIV. CODE § 1785.10, 1785.15-1785.15.2, 1785.16, 1785.20 (West 2003).

[190] COLO. REV. STAT. § 5-3-106(2), 212-14.3-104.3 (2003).

[191] Hillebrand, *supra* note 167, at 69.

[192] *Id.*

[193] Fair and Accurate Credit Transactions Act § 212(b).

[194] Fair Credit Reporting Act § 612(a) (current version at 15 U.S.C. § 1681j(a) (2004)).

[195] National Association of State PIRGs, *Mistakes Do Happen: A Look at Errors in Consumer Credit Reports, available at* http://uspirg.org/reports/MistakesDoHappen2004.pdf (last visited Feb. 19, 2005).

found that "25% of the credit reports surveyed contained serious errors that could result in the denial of credit, such as false delinquencies or accounts that did not belong to the consumer" and that altogether "79% of the credit reports surveyed contained either serious errors or other mistakes of some kind."[196] Although preexisting laws in the seven states that provide for free annual credit reports are exempt from the standalone preemption in FCRA, § 625(b)(4), these laws are not included in the "conduct required" preemption in § 625(b)(5).[197] "This suggests that the inclusion of the free annual report section on the list of provisions which preempt as to the conduct they require is simply an error."[198] The effect on states is uncertain and "states could impose a similar free annual report requirement on regional consumer reporting agencies and regional specialty agencies such as a regional landlord-tenant database, from which § 612(a) does not require a free annual report."[199]

D. STATE LAWS AND FEDERAL PREEMPTION

In terms of fair credit reporting laws, there is an intersection between state statutes, common law, constitutional provisions, and federal statutes that require financial institutions to be careful when structuring their relationship with customers and credit reporting agencies. "Financial institutions should be cognizant of fair credit reporting obligations under both federal and state law whenever they implement information interchange policies, structure their relationships with customers or credit reporting agencies, or consider the consequences of the interchange of information with unaffiliated

---

[196] National Association of State PIRGs, *Mistakes Do Happen: A Look at Errors in Consumer Credit Reports Executive Summary*, *available at* http://uspirg.org/uspirg.asp?id2=13649&id3=USPIRG&#notes (last visited Feb. 19, 2005).

[197] *See* COLO. REV. STAT. § 12-14.3-105(1)(d) (2003); GA. CODE ANN. § 10-1-393(29)(C) (2004); ME. REV. STAT. ANN. tit. 10, § 316.2 (West 2003); MD. CODE ANN., COM. LAW I § 14-1209(a)(1), § 14-1209(b)(1)(i) (2004); MASS. GEN. LAWS ch. 93, § 59(d)-59(e) (2004); N.J. REV. STAT. ANN. § 56:11-37.10(a)(1) (West 2004); VT. STAT. ANN. tit. 9, § 2480c(a)(1) (2004). The Oxley-Bachus legislative history notes that only the identified state laws governing credit score disclosure, credit-based insurance score disclosure, and the frequency of consumer report disclosure are grandfathered. 149 CONG. REC. E2514 (daily ed. Dec 8, 2003).

[198] Hillebrand, *supra* note 167, at 71.

[199] Hillebrand, Gail. *After the FACT Act: What States Can Still Do to Prevent Identity Theft*, *available at* http://www.consumersunion.org/pdf/FACT-0104.pdf (last visited Feb. 19, 2005).

businesses."[200] Again, while there is a general deference to state laws consistent with the governing principals of the FCRA, FTC commentary indicates that a state law is preempted by the FCRA "only when compliance with inconsistent state law would result in violation of the FCRA."[201] However,

> [a]s a practical matter, the uncertainty engendered by piecemeal preemption under the nebulous standard of inconsistency may require financial institutions to comply with both state and federal law unless compliance with both is impracticable or there is a specific federal preemption provision, or an administrative interpretation or judicial decision, clearly applicable to a specific case.[202]

Recent cases continue in the trajectory of broad FCRA preemption in specific areas that are inside the areas covered by the statute and federal agency regulations.

The California case *American Bankers Association v. Lockyer*, discussed in the GLB Act context, *supra*, held that "[n]o requirement or prohibition may be imposed under the laws of any State...with respect to the exchange of information among persons affiliated by common ownership or common corporate control."[203] The court held that the FCRA only covered the sharing of information that constitutes consumer reports, and explained that the "FCRA preemption provision [did] not broadly preempt all state laws regarding sharing by affiliates, whatever the purpose or context."[204] This case rejected the frequently held view by large financial institutions with hundreds and often thousands of affiliates, that the FCRA preempts affiliate information sharing for non-marketing solicitation purposes.[205]

The FCRA does not preempt all state law rights. The Minnesota case, *Davenport v. Farmers Ins. Group*, held that the notice provisions required under the Minnesota Insurance Fair Information Reporting

---

[200] Fischer, *supra* note 151, at ¶ 1.10[1].

[201] Fischer, *supra* note 151, at ¶ 1.10[2][a] (citing 16 C.F.R. pt. 600, App., ¶ 622-1).

[202] *Id.*

[203] *Am. Bankers Ass'n*, 2004 WL 1490432, at *6.

[204] *Id.* at *13.

[205] Hillebrand, *supra* note 167, at 64 - 65.

Act ("MIFIRA") were not preempted by the FCRA.[206] The plaintiffs claimed on behalf of themselves and others similarly situated that Farmers Insurance Group and others violated the MIFIRA by collecting and disclosing personal information without first providing notice and securing written authorization. In finding that the FCRA did not preempt the MIFIRA, the court said, "the FCRA makes clear that it is not intended to occupy the entire regulatory field with regard to consumer disputes," and that "the statute plainly limits its preemption of state regulations 'only to the extent of the inconsistency' with those regulations."[207] The court then cited FTC commentary that emphasized that the FCRA was not intended to preempt the entire field of consumer report law, stating, "state law is pre-empted by the FCRA only when compliance with inconsistent state law would result in violation of the FCRA."[208] The Eighth Circuit held that the MIFIRA requirement that insurance companies notify consumers before obtaining their personal information does not conflict with the FCRA, and that the FCRA does not preempt all state law rights.

In a Michigan case, *Nelski v. Ameritech, Ameritech Services*,[209] the plaintiff was a victim of identity theft and sued defendants alleging defamation and violation of the FCRA.. The court held that because the plaintiff had sufficiently alleged a cause of action for common-law defamation under § 1681h(e), the trial court erred in dismissing the claim for failure to state a cause of action.[210] After the plaintiff's FCRA claims were removed to the federal court and resolved, the trial court granted defendants summary disposition of the plaintiff's state law claim.[211] The court concluded that the defendants were furnishers of information under the FCRA and that the FCRA applied to this case and preempted the plaintiff's state law claim.[212]

---

[206] Davenport v. Farmers Ins. Group, 378 F.3d 839 (8th Cir. 2004).

[207] *Id.* at 7 (citing 15 U.S.C. § 1681t(a)).

[208] *Id.* at 8 (citing 16 C.F.R. Pt. 600, App. § 622).

[209] Nelski v. Ameritech, Ameritech Servs., Inc., No. 244644, 2004 Mich. App. LEXIS 1798 (Mich. App. June 29, 2004).

[210] *Id.* at *18.

[211] *Id.* at *1.

[212] *Id.*

The court cited § 1618h(e), stating that it provided qualified immunity to furnishers of information, including the defendants, "except as to false information furnished with malice or willful intent to injure such consumer."[213] The plaintiff alleged that the "[d]efendants acted in a libelous, slanderous[,] and defamatory manner in terms of reporting and/or publishing false financial records."[214] She further alleged that she "was declined credit from two separate companies due to negligent reporting/publishing and/or willful and wanton disregard as to reporting/publishing by Defendants of Plaintiff's financial record."[215] The Court held that the plaintiff sufficiently alleged a cause of action for common-law defamation under § 1681h(e).[216] However, Judge White in a concurring opinion said that "on this record, it is unclear plaintiff can sustain an action under 15 U.S.C. § 1681(h)" and noted that the parties should address the issue on remand.[217]

Although no federal court of appeals has addressed the issue of preemption of state law tort claims accompanying a claim under the FCRA, the court in *Malm v. Household Bank* attempted to reconcile what it saw as two overlapping sections that restricted state law claims against furnishers.[218] The original FCRA preemption, § 1681h(e), limited liability for defamation, invasion of privacy, and negligence to instances where "false information [was] furnished with malice or willful intent to injure...[the] consumer." Plaintiffs who show that information was provided with "knowledge that it was false or with reckless disregard of whether it was false or not" could bring claims under it.[219]

At the same time, the second preemption requirement in the 1996 amendments stated "no requirement of prohibition may be imposed under the laws of any State with respect to any subject matter regulated under...section 1681s-2 of this title, relating to the

---

[213] *Id.* at *18 (citing § 1681h(e)).

[214] *Nelski*, Mich. App. LEXIS 1798, at *18.

[215] *Id.*

[216] *Id.*

[217] *Id.* at *19 (White, J., dissenting).

[218] Malm v. Household Bank, N.A., Civil No. 03-4340, 2004 U.S. Dist. LEXIS 12981, at *15 (D. Minn., 2004).

[219] *Id.* at *16 (citing 15 U.S.C. § 1681h(e)).

responsibilities of persons who furnish information to consumer reporting agencies."[220] The *Malm* court held that, "because § 1681t(b)(1)(F) precludes imposition of any state law on matters regulated under § 1681s-2, the FCRA preempts state tort actions premised on a furnisher's post-notice conduct."[221] The Minnesota court regarded § 1681t(b)(1)(F), which was added to the FCRA after § 1681g, as completely subsuming § 1681h(e).

In contrast, a second approach, as represented by the Alabama case *McCloud v. Homeside Lending*, is that § 1681t(b)(1)(F) does not preempt common law tort claims and that it applies to state statutes only, with § 1681h(3) pertaining to common law torts.[222] This is referred to as the "minority view,"[223] although the distinction between the minority and majority view is somewhat precarious since "the most recent cases appear to indicate that the so-called minority rule is on the verge of gaining majority status."[224] Courts are reluctant to adopt a single majority or minority view, preferring instead to look at the reasoning of the various options.[225]

A third approach is called the temporal approach. Under this approach,

> there are two distinct time frames that are relevant to an analysis under the FCRA with respect to furnisher liability under state common law: (1) before the furnisher is notified of a dispute by the consumer reporting agency; and (2) after notification. In the first time period, according to these courts, § 1681h(e) applies and a plaintiff may bring any claims for defamation or negligence so long as the furnisher had 'malice or willful intent to injure.' In the second time period, after the furnisher has been notified of a complaint

---

[220] *Id.* at * 17 (citing 15 U.S.C. § 1681t(b)(1)(F)).

[221] *Id.* at *22.

[222] McCloud v. Homeside Lending, 309 F. Supp. 2d 1335, 1341-42 (N.D. Ala. 2004).

[223] Carriere v. Proponent Federal Credit Union, 2004 U.S. Dist. LEXIS 14095 (D. La. 2004).

[224] *McCloud*, 309 F. Supp. 2d at 1342.

[225] *Id.*

> by the consumer reporting agency, § 1681t(b)(1)(F) serves as a total bar to state-law claims.[226]

This approach seems to be the most widely used at present.[227]

In a Louisiana case, *Carriere v. Proponent Federal Credit Union*, the plaintiff suggested a fourth approach that combined the elements of the second and third approaches, urging that § 1681t(b)(1)(F) preempts all state law claims arising after a furnisher receives notice of a dispute from a credit reporting agency.[228] The *Carriere* court rejected creating a fourth standard, because it was unclear whether the actions complained of arose before or after the plaintiff received notice from the credit reporting agency.[229] Ultimately the court used the temporal approach and recommended that the motion to dismiss for preemption be denied, because discovery had not yet been conducted.[230]

E. LIMITATIONS ON THE USAGE OF CONSUMER REPORTS

The 2003 case *Hasburn v. County of Los Angeles* dealt with obtaining a consumer report to collect child support payments. The court held that "under the FCRA, a child support enforcement agency may obtain the consumer credit report of a person owing or potentially owing child support."[231] The plaintiff, a delinquent child support obligor, claimed that the Bureau of Family Support Operations obtained the plaintiff's credit report in violation of the FCRA, and that

---

[226] Carlson v. Trans Union, LLC, 259 F. Supp. 2d 517, 521 (N.D. Tex. 2003) (citing Vazquez-Garcia v. Trans Union De P.R., Inc., 222 F. Supp. 2d 150 (D.P.R., 2002) & Aklagi v. Nationscredit Fin. Servs. Corp., 196 F. Supp. 2d 1186 (D. Kan., 2002)); *see also Carriere*, 2004 U.S. Dist. LEXIS 14095 at *13; *see* Bank One, N.A. v. Colley, 294 F. Supp. 2d 864, 868 (N.D. La. 2003).

[227] *See* Jeffery v. Trans Union, LLC, 273 F. Supp. 2d 725, 726 (D. Va. 2003); Woltersdorf v. Pentagon Fed. Credit Union, 320 F. Supp. 2d 1222, 1225-27 & nn.5-6 (N.D. Ala. 2004); Harrison v. Ford Motor Credit Co., 2005 U.S. Dist. LEXIS *3 (D. Conn., 2005).

[228] *Carriere*, 2004 U.S. Dist. LEXIS 14095, at *14; *see* Stafford v. Cross Country Bank, 262 F. Supp. 2d 776, 786-788 (W.D. Ky. 2003).

[229] *Carriere*, 2004 U.S. Dist. LEXIS 14095, at *17.

[230] *Carriere*, 2004 U.S. Dist. LEXIS 14095, at *17; *see* Woltersdorf v. Pentagon Federal Credit Union, CIV-03-H-2820-S, 2004 WL 1252689, at *4 (N.D. Ala. April 2, 2004) (holding that defendant could move forward with a motion for summary judgment once it could produce evidence supporting its preemption argument.).

[231] Hasburn v. County of Los Angeles, 323 F.3d 801, 805 (9th Cir. 2003).

the child protection agency failed to comply with certification requirements, as required by 15 U.S.C. § 1681b(a)(4).[232] The court held that when requesting a consumer credit report to establish one's ability to pay support or to determine the appropriate amount, the child support enforcement agency must comply with § 1681b(1)(4).[233] However, when the agency seeks to enforce an existing order of child support, the certification requirements of § 1681b(a)(4) are inapplicable.[234] Cases like this show the breadth of the FCRA and how the 1996 Amendments expand the permissible purposes under which one can obtain a consumer report.

An additional issue is what constitutes a firm offer of credit.[235] In 2003, a Louisiana case, *Kennedy v. Chase Manhattan Bank*, held that because the "FCRA ha[d] been manipulated such that a 'firm offer' really means a 'firm offer if you meet certain criteria,' plaintiffs allegations [sic] do not amount to a violation of the FCRA, but merely evidence a dissatisfaction with this prescreening process."[236] The plaintiff received a pre-qualified offer for a credit card from the defendant bank, and believing that she was pre-approved for credit, she accepted the offer and returned the application.[237] Upon receiving the application, the bank obtained her credit report and notified her that she could not open an account based on the information contained in her credit report.[238] The plaintiff alleged that the bank had obtained her credit report without her consent or knowledge, and that the bank had an obligation to make a firm offer of credit and honor that offer.[239] The bank argued that it had a legal right to decline credit to a

---

[232] *Id.* at 802.

[233] *Id.*

[234] *Id.*

[235] The FCRA defines "firm offer of credit or insurance" as "any offer of credit or insurance to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer...." 15 U.S.C. § 1681a(l).

[236] Kennedy v. Chase Manhattan Bank, Civil Action No. 03-0050 Section M, 2003 U.S. Dist. LEXIS 8454, at *6 (E.D. La. May 20, 2003).

[237] *Id.* at *2.

[238] *Id.*

[239] *Id.* at *3.

consumer who did not satisfy its credit criteria.[240] The district court held that a firm offer may "be conditioned on the consumer being determined to meet specific criteria bearing on credit worthiness that is established before selection of the consumer and for the purpose of determining whether to extend credit."[241] The Louisiana court held that to the extent the plaintiff had alleged violations of state laws, those laws were expressly preempted by § 1681t(a) of the FCRA and her case was dismissed.[242]

On appeal, the plaintiff maintained that her complaint stated a cause of action, and that the district court was incorrect in dismissing it. The plaintiff argued that the FCRA

> [p]ermits a bank to obtain a consumer credit report for the purpose of extending a firm offer of credit, but may decline credit for only three reasons: (1) because of information contained in the consumer's credit application, (2) because of verification of the information used to select the consumer for the offer, and/or (3) because the consumer fails to provide collateral.[243]

The plaintiff insisted that the bank used other criteria when declining her credit. The appeals court noted that because the plaintiff responded to the pre-approved credit offer, the creditor was allowed to access the credit report to determine whether the plaintiff still satisfied the previously-established credit worthiness criteria.[244]

Additionally, the plaintiff argued that the bank violated sections 1681a(l) and 1681b(c) by declining to extend credit after extending firm offers of credit.[245] The court said in response that the FCRA "allows a creditor to use information in a consumer report to verify a consumer's credit worthiness, and to withdraw a firm offer of credit if the consumer does not meet the creditor's previously-established

---

[240] *Id.* at *4.

[241] *Kennedy*, 2003 U.S. Dist. LEXIS 8454, at *5.

[242] *Id.* at *6.

[243] Kennedy v. Chase Manhattan Bank U.S., NA, 369 F.3d 833, 839 (5th Cir. 2004).

[244] *Id.* at 838.

[245] *Id.* at 841.

criteria for extending credit."[246] The plaintiff authorized the banks to obtain a consumer report for issuing a credit card account, and the bank could withdraw the offer if the plaintiff was not credit worthy based on the consumer reports.

The plaintiff also argued that the bank violated the FCRA by obtaining credit information under false pretenses, in violation of FCRA § 1681q, which provides a cause of action for obtaining credit information under false pretenses.[247] The court dismissed this cause of action, because the bank fully apprised the plaintiff that it would review her credit history prior to determining whether to extend the offered credit.[248] When the plaintiff signed the pre-approved certificates, she agreed to the terms of the offers and authorized the bank to access her credit information.[249] The Fifth Circuit held that the district court did not err, and that in absence of an allegation of inaccurate information there was no claim.[250] On November 15, 2004 a petition for writ of certiorari to the United States Court of Appeals for the Fifth Circuit was denied by the Supreme Court.[251]

F. OBLIGATIONS OF USERS OF CONSUMER REPORTS

A Pennsylvania case, *Crane v. American Home Mortgage Corp.*, addressed the obligations of those who use the credit information contained in consumer reports. The plaintiff alleged that the defendant was using consumer credit information in violation of the FCRA, and brought the action on behalf of himself and others who sought mortgage loans from the defendant bank and were approved subject to payment of higher interest rates, fees, or other unfavorable terms.[252] The plaintiff believed that the denial of pre-qualification at the defendant's prime rate was an adverse action under the FCRA §

---

[246] *Id.* at 841-42; *see* 15 U.S.C. § 1681a(l)(2).

[247] *Kennedy*, 369 F.3d at 842; *see* 15 U.S.C. § 1681q.

[248] *Kennedy*, 369 F.3d at 844.

[249] *Id.* at 843.

[250] *Id.*

[251] Kennedy v. Chase Manhattan Bank, USA, NA, 125 S. Ct. 508 (2004).

[252] Crane v. American Home Mortgage, Corp., No. 03-5784, 2004 U.S. Dist. LEXIS 12770, at *1 (E.D. Pa. July 1, 2004).

1681n, and the defendant was required to comply with the FCRA's notice provisions.[253] The defendant moved for summary judgment, claiming that he had not taken an adverse action against the plaintiff because the plaintiff initiated the pre-qualification process without following up on his initial inquiry.[254] The defendant further argued that a formal credit application was required to trigger consumer protections under the FCRA, while the plaintiff argued that the transaction was enough, because the FCRA does not require a formal application for credit.[255]

The court looked to the definition of adverse action in the Equal Credit Opportunity Act ("ECOA") and defined adverse action as "a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested."[256] The court held that the language of the FCRA provision was clear and that Congress intended a broader definition of "adverse action" in the FCRA than in the ECOA.[257] "The FCRA notice requirements are intended to cover adverse actions 'made in connection with an application' or 'a transaction that was initiated by ... any consumer.'"[258] After considering that the FCRA was enacted to protect consumers from transmission of inaccurate consumer information, the Pennsylvania court found it unlikely that Congress intended pre-qualification processes to fall outside of the Act's protection, and read a broad definition of "adverse action" in the FCRA.[259]

---

[253] *Id.* at *8.

[254] *Id.* at *12.

[255] *Id.*

[256] *Id.* at *14 (citing 15 U.S.C. § 1691(d)(6)); *see* ECOA 12 C.F.R. § 202.2(c)(1)(i)(2004).

[257] *Crane*, 2004 U.S. Dist. LEXIS 12770, at *17.

[258] *Id.* The Court also cited several other 2004 cases to support that "the FCRA defines 'adverse action' more broadly than does the ECOA," Treadway v. Gateway Chevrolet Oldsmobile, Inc., 362 F.3d 971, 982-83 (7th Cir. 2004); *see also* Payne v. Ken Diepholz Ford Mercury, No. 02-C-1329, 2004 U.S. Dist. LEXIS 19, at *18 (N.D. Ill. Jan 6, 2004) (applying the catch-all provision to auto financing transactions).

[259] *Id.* at *21.

G. CASES IN INVOLVING THE CORRECTION OF ERRORS

Several recent cases have helped bolster the protections that consumers receive under the FCRA. *Nelson v. Chase Manhattan Mortgage Corp* held that the FCRA gave consumers a private cause of action against providers of credit information, because the primary purpose of the FCRA was to protect consumers against inaccurate and incomplete credit reporting.[260] A recent article notes that post-*Nelson*, "the liability has ratcheted way up...it used to be only the credit bureaus... now the liability is anyone involved in the loop between the credit bureaus – the information furnishers and anyone else obtaining the information."[261] A recent key case was *Johnson v. MBNA*, which held that those who furnish credit information had a duty to investigate consumer complaints about incorrect information.[262] The plaintiff sued a credit card issuer to challenge its contention that she was responsible for the balance on a credit card that was in the name of her former husband.[263] She claimed that she had no knowledge of the card, had not applied for it as a co-obligor, and had not used it.[264] The Fourth Circuit used the balancing test employed by the district court and held that "weighing the cost of verifying disputed information against the possible harm to the consumer – logically applies in determining whether the steps taken (and not taken) by a creditor in investigating a dispute constitute a reasonable investigation."[265] This test toughens the standard and credit information furnishers may need to consult underlying documents such as account applications, rather than simply relying on data in computerized customer information systems.[266] Courts are forcing credit providers to become more diligent in following up on consumer complaints.[267]

---

[260] Nelson v. Chase Manhattan Mortg. Corp., 282 F.3d 1057, 1060 (9th Cir. 2002).

[261] Chanen, *supra* note 161, at 53.

[262] Johnson v. MBNA America Bank, 357 F.3d 426, 433 (4th Cir. 2004).

[263] *Id.* at 428–29.

[264] *Id.*

[265] *Id.* at 432-33.

[266] *Id.* at 431.

[267] The Chanen article quotes Leonard Bennett, who represented the plaintiff at the trial court level, stating "almost all creditors that investigate what they report to credit bureaus do a very superficial computer check...*Johnson* held that the creditors have to go back to the original

By holding that § 1681-2(b)(1) compels furnishers "to conduct a reasonable investigation of their records to determine whether the disputed information can be verified" only after adequate notice, the *Johnson* decision forced credit providers to do a more thorough job in researching complaints.[268] *Malm v. Household Bank*, the Minnesota case discussed earlier in the State Laws and Federal Preemption section, clarified the *Johnson* standard and held that an unclear form did not notify Sherman Financial Group that additional inquiry was necessary; Sherman had not reviewed the actual application.[269] The court held, "while specific notice of Plaintiff's concerns could have compelled Sherman to conduct a more thorough review, thus creating an issue of 'reasonableness' for the jury, a more rigorous investigation was not required here based on the superficial notice that Trans Union provided."[270] While there is a duty to investigate, that duty has limitations.

H. ENFORCEMENT ISSUES

Courts typically review the actions of the employer and not the employee when making decisions regarding liability under the FCRA, and one issue is whether an employer can be held liable under the FCRA when an employee, acting outside of the scope of his employment, obtains a credit report for his own personal purposes. While an employee is liable when he or she obtains a consumer report under false pretenses,[271] it is less clear if an employer should also be exposed to liability. In Mississippi, *Smith v. Sears Roebuck* focused on the actions of the employer rather than the employee and held that

> [d]espite an employer's best efforts to ensure compliance with the FCRA, the employer is subject to liability for the actions of any rouge [sic] employee who might manage to obtain a credit report for his own personal reasons – which is

---

documents. It seems somewhat self-evident, but that was not what the practice was." Chanen, *supra* note 161, at 53.

[268] Johnson v. MBNA America Bank, 357 F.3d at 431.

[269] Malm v. Household Bank, N.A., Civil No. 03-4340, 2004 U.S. Dist. LEXIS 12981, at *15 (D. Minn. July 7, 2004).

[270] *Id.* (citing 15 U.S.C. § 1681s-2(b)(1)).

[271] 15 U.S.C. § 1681q.

> to say, short of implementing foolproof compliance procedures, there is nothing an employer can do to avoid liability.[272]

The plaintiff in this case sued his ex-wife's employer for not preventing her from accessing his credit report. The court explained that the FCRA does not impose strict liability for consumer reporting agencies and that users such as the defendant should not be held to a higher standard than the reporting agencies themselves.[273]

Several 2004 cases applied the *Sears* decision, including the Pennsylvania decision *Lukens v. Dunphry Nissan,* which found a dealership to be a "person" as defined by § 1681a(b) and as such subject to liability under the FCRA.[274] The court cited *Smith* and applied agency principles to the plaintiff's FCRA claims.[275] The combined elements of the defendant's disregard for Williams' relevant criminal history, the access to consumer credit information that the defendant provided to a known identity thief, and the eventual leak of the plaintiff's information invoked employer liability.[276] Additionally, the Kansas case *Cole v. American Family Insurance* struggled with the issues of agency and relation, and concluded that the rule had not been fully developed either in Kansas or within the Tenth Circuit, except in Title VII employment discrimination cases.[277] The court held that the issue of vicarious liability could not be properly considered in a motion to dismiss, and that it should be raised in a summary judgment where the "the parties should address whether apparent authority or aided-in-the-agency-relation rule is the correct theory of agency liability in this case; whether an affirmative defense exists to the chosen vicarious liability theory; and, whether the affirmative defense is applicable in this context."[278] These cases illustrate the difficulty

---

[272] Smith v. Sears Roebuck & Co., Civil No. 3:01-CV-675LN, 2003 U.S. Dist. LEXIS 14189, at *17 (S.D. Miss. May 30, 2003).

[273] *Id.* at *18.

[274] Lukens v. Dunphy Nissan, Inc., 2004 U.S. Dist. LEXIS 14528 (D. Pa. July 23, 2004).

[275] *Id.* at *12.

[276] *Id.* at *13.

[277] Cole v. Am. Family Mut. Ins. Co., 333 F. Supp. 2d 1038, 1046 (D. Kan. 2004).

[278] *Id.* at 1046-47.

that courts have when fashioning standards for vicarious liability under the FCRA.

I. FCRA, FACT, AND THE FUTURE

While implementation may require some work and operational adjustments from parties such as lenders, the new consumer protection requirements within the FCRA are overall extremely positive for the financial services sector. By giving the federal government permanent preemption over FCRA-type rules at the state level, the FACT Act establishes minimum uniform consumer protection standards at the national level. This protection is valuable because, "without that, industry entities might be forced to deal with a patchwork quilt of various laws across states, cost of credit would rise, and consumers might have fewer credit products to choose from."[279] The free credit reports provision, which allows a free credit report annually from the major CRAs, has been widely publicized and is perhaps the most visible portion of the FACT Act.

State laws addressing identity theft are preempted by the FCRA only when they are inconsistent with a provision of the FCRA, and state laws that provide greater consumer protections are not likely to be prohibited. Case law confirms a pattern of broad FCRA preemption in specific areas addressed by statute and federal agency regulations, while state laws that provide greater protections are being upheld. The FCRA covers broad territory, and future cases will continue to expand and define the permissible purposes of obtaining a consumer report and who can obtain them. Future developments will also focus on defining a firm offer of credit within the FCRA.

Another area that will be developed involves the correction of errors on reports and establishing the limitations on the protections that consumers receive under the FCRA. One trend is expanding liability to include more information furnishers, and generally holding those who furnish credit information responsible for investigating consumer complaints regarding incorrect information. Courts are looking to the consumer protection theme of the FCRA and are forcing credit providers to be more diligent in addressing consumer complaints. However, courts are currently struggling with creating standards for vicarious liability under the FCRA and defining when an employer should be exposed to liability due to the actions of its employee.

---

[279] Karlene Bowen, *FACTA: Pointing the Industry in a Good Direction, available at* http://www.fairisaac.com/Fairisaac/News/ViewPoints/200405/FACTA+Pointing+the+industry+in+a+good+direction.htm (last visited April 3, 2005).

IV. MONEY LAUNDERING AND SECTION 326 OF THE USA PATRIOT ACT

A. BACKGROUND

In an immediate response to the terrorists' attacks on September 11, 2001, the U.S. Congress passed the USA PATRIOT Act.[280] The USA PATRIOT Act gives U.S. federal officials greater authority to track and intercept communications, and vests regulatory powers in the U.S. Secretary of the Treasury to combat money laundering domestically and abroad.[281] Section 326 specifically states that the Secretary of the Treasury has the power to issue regulations for financial institutions and to recommend means to verify effectively the identification of foreign customers.[282] Section 326 requires that financial institutions adopt formal anti-money laundering policies with a focus on aggressive "know your customer" standards and effective record-keeping.[283]

B. IMPLEMENTATION

During 2003 and throughout 2004, the Department of the Treasury and the Department of Justice focused on three overarching goals in implementing the USA PATRIOT Act: (1) safeguarding the international financial system from money laundering and terrorist financing; (2) enhancing the U.S. government's ability to identify, investigate, and prosecute major money laundering organizations; and (3) ensuring effective regulation.[284] Acting on its goals, the

---

[280] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[281] *See* Raymond L. Moss, et. al, *The U.S. Patriot Act and Related Domestic and International Anti-Money Laundering Regulations, with a Special Focus on Switzerland: Legal and Business Implications*, 1440 PLI/CORP 801, 805 (2004).

[282] *See id.* at 808 (citing 31 U.S.C. § 5318(j) (2001)).

[283] *See id.* at 809 (citing Security and Exchange Commission, Release No. 34-47752, File No. S7-25-02 (effective June 9, 2003), *available at* http://www.sec.gov/rules/final/34-47752.htm (last viewed Feb. 16, 2005)).

[284] Edward J. Krauland and Aaron R. Hutman, *International Legal Developments in Review: 2003: Public International Law*, 38 INT'L LAW 509, 510 (2004) (citing United States Department of Treasury and United States Department of Justice, *2003 National Money Laundering Strategy*, (2003), *available at* http://www.treas.gov/press/releases/reports/js10102.pdf (last viewed Feb. 16, 2005)); *see also* United States Department of the Treasury,

Department of the Treasury, through the Financial Crimes Enforcement Network ("FinCEN") and the SEC, jointly adopted a final rule to implement § 326 of the USA PATRIOT Act.[285] The final rule requires that brokers or dealers

> implement reasonable procedures to "verify the identity of any person seeking to open an account, to the extent reasonable and practicable; to maintain records of the information used to verify the person's identity; and to determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency."[286]

The final rule also requires that the Secretary of the Treasury and the Securities and Exchange Commission prescribe further regulations for enforcing the USA PATRIOT Act.[287]

C. ENFORCEMENT

1. ENFORCEMENT AGENCIES

There are numerous governmental agencies and organizations involved in enforcing regulations throughout the world. Three important organizations operate through the U.S. Department of the Treasury: (1) FinCEN, which works with other U.S. law enforcement agencies to enforce federal statutes; (2) the Office of Foreign Assets Control, which works to disrupt and freeze global terrorist financing; and (3) "Operation Green Quest," an inter-agency enforcement group.[288] In the international community, the Financial Action Task

---

FY 2004 Performance and Accountability Report, at 65-77 (2004), *available at* http://www.treas.gov/offices/management/dcfo/accountability-reports/2004reports/part2.pdf?IMAGE.X=0\&IMAGE.Y=0 (last viewed Feb. 16, 2005).

[285] Security and Exchange Commission, Release No. 34-47752, File No. S7-25-02 (effective June 9, 2003).

[286] *Id.*

[287] *Id.*; *see also* 31 U.S.C. § 5318(1) (2001) (provides an initial framework for Secretary's powers under Act).

[288] Walter Perkel, *Money Laundering and Terrorism: Informal Value Transfer Systems*, 41 AM. CRIM. L. REV. 183, 186 (Winter 2004) (citing *The Administration's National Money Laundering Strategy for 2002, Testimony before the Senate Comm. on Banking, Housing, and*

Force ("FATF"),[289] is tackling international money laundering by requiring nations to enact legislation that imitates U.S. money laundering regulations. Internationally, the U.S. is also working with the United Nations, the World Bank/IMF, and the Egmont Group.[290]

Section 311 of the USA PATRIOT Act grants the Secretary of the Treasury (through FinCEN) specific authority to find that a "foreign jurisdiction, institution, class of transactions, or type of account is of 'primary money laundering concern' and to require domestic financial institutions and financial agencies to take certain 'special measures' against the primary money laundering concerns."291 The statute provides procedures for selecting the imposition of specific special measures against these institutions.292 Before declaring a foreign financial institution as a primary money laundering concern, the Secretary is required to consult with both the Secretary of State and the U.S. Attorney General.293 Following a final determination that a foreign financial institution is of "primary money laundering concern," FinCEN may impose special measures that include: (1) record keeping obligations and reporting requirements; (2) collection of information relating to beneficial ownership; (3) collection of information relating to corresponding accounts; (4) collection of information relating to certain payable-through accounts; and (5) prohibition or conditions on the opening or maintaining of correspondent or payable-through accounts.294 As for the effect of the measures on those operating in the United States, FinCEN typically requires that all U.S. persons,

---

Urban Affairs, 108th Cong. (2002) (Statement of Kenneth W. Dam, Deputy of Treasury, U.S. Dep't of Treasury)).

[289] *See id.* (FATF is an international organization created by the members of G-8 and is the investigative branch of the Organization for Economic Cooperation and Development).

[290] *Id.* at 187.

[291] Federal Crimes Enforcement Network, 69 Fed. Reg. 28098 (May 18, 2004), *available at* http://www.fincen.gov/311syrianprm.pdf (codified at 31 C.F.R. pt. 103).

[292] *Id.*

[293] *See id.* (during these discussions relevant factors for consideration include: (1) extent to which financial institution is used to facilitate money laundering, (2) extent to which financial institution is used for legitimate business purposes, and (3) extent to which classifying the institution as a "primary concern" is sufficient to ensure that the purposes of the Bank Secrecy Act is fulfilled).

[294] *Id.* (citing 31 U.S.C. § 5318A(b)(1)-(5)).

including U.S. institutions, exercise a higher level of due diligence in complying with the various sanction programs.[295]

2. SPECIFIC ENFORCEMENT IN 2004

FinCEN imposed "special measures" on five separate incidents during 2004. By imposing special measures, FinCEN labeled certain countries and organizations as "institutions of primary money laundering concern." These institutions were then placed on a "blacklist" that was circulated throughout the U.S. financial industry. Specific enforcement in 2004 includes:

> 1) Imposition of Special Measures against Myanmar Mayflower Bank and Asia Wealth Bank (April 12, 2004).[296]
>
> 2) Imposition of a Special Measure against Commercial Bank of Syria, including its subsidiary, Syrian Lebanese Commercial Bank, as a Financial Institution of Primary Money Laundering Concern (May 18, 2004).[297]
>
> 3) Imposition of Special Measures against Burma (September 30, 2004).[298]
>
> 4) Imposition of Special Measure against Infobank as a Financial Institution of Primary Money Laundering Concern (September 30, 2004).[299]
>
> 5) Imposition of Special Measure Against First Merchant Bank OSH Ltd, Including Its Subsidiaries, FMB Finance

---

[295] *Id.*; *see also* Krauland, *supra* note 284, at 513 (discussing reporting requirements for suspicious information).

[296] *See* Financial Crimes Enforcement Network, 69 Fed. Reg. 19098 (Apr. 12, 2004), *available at* http://www.fincen.gov/mayflowerbank.pdf (codified at 31 C.F.R. pt. 103).

[297] *See* Financial Crimes Enforcement Network, 69 Fed. Reg. 28098 (May 18, 2004), *available at* http://www.fincen.gov/311syrianprm.pdf (codified at 31 C.F.R. pt. 103).

[298] *See* Financial Crimes Enforcement Network, 69 Fed. Reg. 19093 (Apr. 12, 2004), *available at* http://www.fincen.gov/burma.pdf (codified at 31 C.F.R. pt. 103).

[299] *See* Financial Crimes Enforcement Network, 69 Fed. Reg. 58375 (Sep. 30, 2004), *available at* http://www.fincen.gov/311infobankextension.pdf (codified at 31 C.F.R. pt. 103).

> Ltd, First Merchant International Inc, First Merchant Finance Ltd, and First Merchant Trust Ltd, as a Financial Institution of Primary Money Laundering Concern (September 30, 2004).[300]

Each specific enforcement action is unique and contains different requirements for financial institutions dealing with these "primary money laundering" institutions. Financial institutions must maintain an awareness of the current FinCEN "blacklist" and should implement procedures and policies to comply with FinCEN's due diligence requirements.

D. MONEY LAUNDERING, SECTION 326 OF THE PATRIOT ACT, AND THE FUTURE

The challenges facing the United States in preventing illegal financing are enormously complex and encompass numerous organizations throughout the world. Current U.S. statutes appear sufficient to regulate and monitor formal financial institutions in U.S. and Western Europe, but struggle to maintain the same control over the informal networks found elsewhere in the world.[301] International criminality and terrorist financing are a global problem and cannot be combated effectively by any one country alone.[302]

Looking into the future, U.S. financial institutions must continue to be vigilant in meeting the compliance and reporting obligations imposed under the USA PATRIOT Act. Both traditional and non-traditional financial institutions should continually be watchful for suspicious activity in order to protect the public and minimize their own exposure as conduits of illegal financing activities.[303] The U.S. must continue to strive to work with the international community to develop and implement international rules and regulations. It is crucial that all the financial leaders of the world continue coordinating

---

[300] *See* Financial Crimes Enforcement Network, 69 Fed. Reg. 58374 (Sept. 30, 2004), *available at* http://www.fincen.gov/311fmbextension.pdf (codified at 31 C.F.R. pt. 103).

[301] *See* Perkel, *supra* note 288, at 210 (discussing the problems inherent in monitoring informal value transfer systems).

[302] Moss et. al, *supra* note 281, at 830.

[303] *Id.*

their efforts and resources to help defeat global criminality and terrorist financing.[304]

V. HIPAA AND FINANCIAL INSTITUTIONS

In 1996 Congress passed the Health Information Portability and Accountability Act ("HIPAA"),[305] which went into effect on April 14, 2003.[306] It was developed to help promote a more economically efficient electronic claim process and to protect the privacy of individually identifiable health information. While the goals of HIPAA are to increase privacy while decreasing costs, the rules created by the Department of Health and Human Services pursuant to HIPAA may in fact increase health care costs, because companies now have more stringent standardization requirements for electronic transactions.[307] Failure to meet HIPAA regulations can result in penalties as much as $25,000 per year and per violation.[308] Banks are among the many institutions that need to familiarize themselves with the new HIPPA regulations.

A banking organization may be subject to HIPAA if it is considered either a "health care clearinghouse,"[309] or a "business associate" of a "covered entity."[310] A bank may also find itself subject to HIPPA regulation if it plays an active role in a payment system that typically originates from insurance carriers, or payments through the

---

[304] *See id.* (discussing the importance of continual cooperation among all nations).

[305] Health Information Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified at 42 U.S.C. § 1320d (2000)).

[306] 66 Fed. Reg. 41315, 41341 (Aug. 7, 2001) (to be codified at 42 C.F.R. pts. 412 & 413).

[307] Jessica M. Lewis. *Comment: New Regulations Affecting the Banking Industry: HIPAA: Demystifying the Implications for Financial Institutions.* 8 N.C. BANKING INST. 141, 141-42 (April 2004).

[308] *Id.*

[309] A "health care clearinghouse" is defined as a: "Public or private entity...that does either of the following functions: (1) Processes or facilitates the processing of health information...in a nonstandard format or containing nonstandard data content into standard date elements of a standard transaction. (2) Receives a standard transaction...and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity." Public Welfare, 45 C.F.R. § 160.103 (2003). A "standard transaction" complies with the standards adopted in 45 C.F.R. § 162.103 (2003).

[310] 45 C.F.R. § 160.508 (2003).

Automated Clearinghouse Network ("ACH"), which is an electronic funds transfer system widely used by financial institutions. While HIPAA requirements apply only to the health care components of the bank, the bank must be sure that it does not share protected health information used in the health care components with parts of the bank not subject to HIPAA compliance.[311]

Health care clearinghouses are intermediaries between health plans and health care providers. The clearinghouses process claims using a structure similar to that used by the credit card industry, although a health care claim must be processed in compliance with HIPAA.[312] Once a bank is termed a health care clearing house under HIPAA, it meets, at least partially, the covered entity and business associate labels, which subject the bank to some degree of HIPAA compliance.[313]

HIPAA establishes only minimum federal protections, and states can enact more stringent laws than the federal HIPAA rules on protected health information privacy, security, and health claims processing.[314] A state law that "relates to the privacy of individually identifiable health information" and is "contrary to and more stringent than the federal requirements" will control, as will state laws that the Secretary of Health and Human Services ("HHS") deems necessary.[315] A state law is more stringent than the rules when it provides "greater privacy protection for the individual who is the subject of the individually identifiable health information,"[316] while a contrary state law is defined by the HHS as one that would be "impossible to comply with" or that "stands as an obstacle" to the goals of the rules.[317] Although HIPPA rules preempt "contrary" state laws, several recent

---

[311] Lewis, *supra* note 303, at 153.

[312] *See* Richard D, Marks, *Surviving Standard Transaction: A HIPAA Roadmap*, 8 ELECTRONIC COM. & L. REP., (BNA), 559, 561 (Jun. 4, 2003).

[313] Lewis, *supra* note 307, at 153.

[314] AHIMA Policy and Government Relations Team, *Final Rule for HIPAA Security Standards, available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_017594.html (last visited Feb. 19, 2005).

[315] Robert Woody, *Health Information Privacy: The Rules Get Tougher*, 37 TORT & INS. L. J. 1051, 1055 (2002).

[316] Public Welfare, 45 C.F.R. § 160.202 (2003).

[317] *Id.*

cases have questioned whether a state law is more stringent than HIPAA. In Florida, *United States v. Diabetes Treatment Centers of America* held that because the state law governing medical privacy related to matters of individually identifiable health information and was more stringent than HIPAA, the Florida law was not preempted.[318]

When a financial institution processes health care payments, it may become subject to HIPAA standards. But there is still uncertainty as to where financial institutions fit under either the "health care clearinghouse" definition or the "business associate" definition that would render them accountable for compliance with HIPAA. While it seems to be clear that, when banks explicitly contract with covered entities to provide health care clearinghouse services, they are subjected to HIPAA regulations, "where banks inadvertently begin to deal with protected health information as more and more health care payments become processed electronically, banks may validly argue against having to increase their privacy and security standards for those transactions."[319] However, banks accept HIPAA's dual goals of automating and standardizing the processing of health insurance transactions and establishing privacy and security standards that safeguard the confidentiality of protected health information. In the words of one group, "the banking industry's unique capability to keep 'dollars and data together' - i.e., payment-related information flowing as addenda with the payment entry itself through the ACH Network - is consistent with HIPAA's objective to reduce costs and simplify administration."[320] While most large health care institutions have faced challenges with HIPAA, financial institutions need to recognize the privacy pressure that health care institutions face, and prepare a strategy that balances the needs of the health care entity with the necessity of operational flexibility on the part of the financial institution.[321]

---

[318] United States ex rel. Pogue v. Diabetes Treatment Ctrs. of Am., 2004 U.S. Dist. LEXIS 21830 (D.D.C. May 17, 2004); *see also* Nat'l Abortion Fed'n v. Ashcroft, 2004 U.S. Dist. LEXIS 1701 (D. Ill., 2004) (A government subpoena for medical records which contained a HIPAA order for disclosure was quashed. Illinois's nonparty patient privacy laws were more stringent and not preempted by HIPAA. Disclosure would have violated them).

[319] Lewis, *supra* note 307, at 162-63.

[320] The Banking Industry HIPAA Task Force, *HIPAA and the Banking Industry*, *available at* http://www.hipaabanking.org/default.html (last visited Feb. 19, 2005).

[321] Kirk J. Nahra, *Financial Institutions and the New HIPAA Rules*, WILEY, REIN, & FIELDING PRIVACY IN FOCUS, (Mar. 2004) *available at* http://www.wrf.com/docs/publications/11766.pdf.

VI. CONCLUSION

Financial privacy developments during 2004 generally focused on: (1) the proper interpretation and application of the Gramm-Leach-Bliley Act to federal, state, and international law; (2) the role and proper interpretation of the Fair and Accurate Credit Transactions Act of 2003 in supplementing the Fair Credit Recording Act; (3) protective statutes designed to shelter U.S. citizens domestically and abroad; and (4) the implementation and application of narrow statutes aimed at addressing specific privacy concerns, such as the Health Insurance Portability and Accountability Act of 1996. Central to the analysis of these developments was the overriding importance of maintaining a healthy balance between the need for free and open information sharing and the importance of protecting customers' privacy rights domestically and abroad. In balancing these competing interests, federal financial laws have helped generate efficiencies in the financial services industry by facilitating an open sharing of information created by the elimination of barriers between affiliates of financial institutions, while continuing to protect customers' privacy rights through disclosure and notice requirements. These laws have made the financial services industry more profitable, and have helped to educate and inform customers as to their personal financial privacy rights.

The financial privacy framework of the United States will continue to evolve in response to external forces throughout the world. Recent developments have tended to place a greater importance on the open sharing of information in order to expand the U.S. economy and protect the safety of American citizens, and appear to have eroded many of the general privacy rights of individuals.

Recent enactments, such as the USA PATRIOT Act and the GLB Act, have opened avenues for information sharing, creating more efficient financial services domestically and further regulating the flow of money throughout the world. On the other hand, industry-specific statutes have been used to place greater protection on specific privacy rights. Examples include the FACT Act, which created uniformed national standards for credit reporting to ensure accurate information and prevent identity theft, and HIPAA, which protects the privacy on individual health information. In addition to federal legislation, state legislatures have taken an active role in preventing the erosion of individual privacy rights by enacting statutes that provide greater protection than similar federal statutes, thereby creating preemption issues.

The challenges affecting the United States in allowing for the free flow of financial information, protecting the individual privacy rights of citizens, and preventing terrorist and other illegal financing, are complex. U.S. financial privacy law remains a liquid medium that continues to adapt and change in addressing these challenges. Although the United States plainly values the free flow of information and the rewards that come from these open channels, the future status of financial privacy laws remain unclear, as it has yet to be determined how effective state legislatures will be in restricting the flow of information. It is equally unclear what role the United States will play in the development of the world economy during the 21st century in creating uniform international privacy standards and combating terrorism.