GRAMM-LEACH-BLILEY: TIP OF THE PRIVACY ICEBERG

By
Andrea Lee Negroni
and
John P. Kromer
Goodwin Procter LLP
1717 Pennsylvania Avenue, N.W.
Washington DC 20006

Introduction

In a somewhat piecemeal fashion, state privacy laws protect consumers from unrestricted distribution of their personal financial information. Following enactment of the Gramm-Leach-Bliley Act (“GLBA”) however, federal law more comprehensively addresses the distribution of consumer information by financial institutions. With the mandatory compliance date of July 1, 2001 having passed, most financial institutions or their attorneys or compliance personnel are aware of GLBA’s requirement for notice to consumers of the institution’s information-sharing policies. Far fewer may be aware of the important state privacy laws whose effect continues unimpeded by GLBA.

1 Note: This article summarizes aspects of “State Privacy Laws Affecting Financial Institutions,” dated July 1, 2001 by the Washington office of the law firm of Goodwin Procter LLP (http://www.goodwinprocter.com/). The complete 50-state survey is available from John P. Kromer, Esq. (mailto:jkromer@goodwinprocter.com) or Andrea Lee Negroni, Esq. (mailto:alnegroni@goodwinprocter.com), who may also be reached by phone at 202-974-1000.

2 Andrea Lee Negroni is a partner in the Washington office of Goodwin Procter LLP, where her practice concentrates on compliance with state and federal laws and regulations governing mortgage lenders, consumer creditors and online financial service providers. She is the author of several books on state mortgage regulation including Pratt’s State Regulation of Second Mortgages and Home Equity Loans (© A.S. Pratt & Sons) and Residential Mortgage Lending: State Regulation Manual (© West Group). Ms. Negroni is a member of the bars of the District of Columbia and Florida.

3 John P. Kromer is a partner in the Washington office of Goodwin Procter LLP, where his practice concentrates on representing financial institutions on compliance with state and federal consumer protection and lending regulations. He is co-author of Pratt’s State Regulation of Second Mortgages and Home Equity Loans (© A.S. Pratt & Sons) and Residential Mortgage Lending: State Regulation Manual (© West Group). Mr. Kromer is a member of the bars of the District of Columbia and Virginia and is a member of the Advisory Counsel to the American Association of Residential Mortgage Regulators.

The principal privacy provisions of the GLBA not only require financial institutions to provide notice of their information-sharing policies to consumers, but restrict them from sharing information with unaffiliated parties unless the consumer has an “opt out” opportunity, i.e., is given a chance to request his information not be shared.

The subject of this article, however, is not the GLBA, but state privacy laws which may offer consumers more protection in the financial privacy arena than does the GLBA. The baseline privacy provisions of the GLBA are discussed here in order to draw the distinction between the different ways in which financial privacy is protected by federal and state law.

While the GLBA has a preemption provision,⁵ and preemption ordinarily leads to the conclusion that federal law displaces state laws, GLBA privacy provisions do not preempt state laws that are consistent with it; the preemption, if applicable, extends only to the inconsistency.⁶ The fact that a state law has more consumer protections against unauthorized information-sharing than does GLBA does not make the state law inconsistent with GLBA. The determination whether a state law is more protective of consumers is made by the Federal Trade Commission⁷ (“FTC”). The FTC may make this determination in response to a request of an interested party.⁸ A state law, for purposes of determining preemption, includes statutes and regulations, as well as any interpretation of law such as court decisions.

Banks and other financial institutions must therefore review state laws applicable to the states where they do business or have customers, to ensure compliance with the privacy laws of those states as well as with the GLBA. State financial privacy laws follow certain patterns as

---


⁷ 15 U.S.C. § 6807(b). The FTC has indicated that few state laws will be considered inconsistent with the GLBA, based on a presumption that state laws are not preempted by the GLBA.

⁸ For example, on September 12, 2000, the State of North Dakota asked the FTC to determine whether its “Disclosure of Customer Information” statute, N.D. Cent. Code ch. 6-08.1, was incompatible with the GLBA and therefore preempted. The FTC responded that a state law would be inconsistent with and superseded by the GLBA only if it either: (i) “works at cross-purposes to or otherwise thwarts the objectives of the federal law;” or (ii) makes it impossible to comply with both the state and the federal law. [Letter to the Honorable Gary D. Preszler, Commissioner, Department of Banking and Financial Institutions, State of North Dakota (June 28, 2001), on the Internet at http://www.ftc.gov/opa/2001/06/nd.htm.]
described below, along with specific state examples. In evaluating state privacy laws and patterns among them, this article focuses on those most likely to affect depository institutions, mortgage lenders, mortgage brokers, consumer finance companies, and insurance companies.9

The enactment of the GLBA sounded a “starting gun” in state legislatures, many of which rushed to introduce and debate bills that would give consumers greater privacy rights than federal law. However, many states had financial privacy laws in place before the GLBA. With judicial decisions on consumer financial privacy taken into account, nearly every state has some type of legal limit on disclosure of financial information by financial institutions. While state laws typically do not cover as many types of financial institutions as the GLBA, they often limit information distribution by covered institutions more sharply than the GLBA. Under state privacy laws, banks and insurance companies are the types of financial institutions most often covered, with non-depository institutions, such as mortgage lenders, mortgage brokers, and consumer finance companies, less likely to be subject to privacy regulation.

I. TRENDS IN STATE FINANCIAL INFORMATION PRIVACY LAWS

Opt-In is More Favored in State Law. Unlike the GLBA, which establishes an “opt-out” standard for third-party information sharing, state financial privacy laws often require financial institutions to obtain the affirmative consent of a customer (“opt-in”) before sharing nonpublic personal information with others. On the other hand, unlike the GLBA, most state privacy laws10 do not require financial institutions to notify consumers of their privacy policies, although notice may be required in connection with the opt-in.

The predominant rule of most state privacy laws is that a covered financial institution is restricted from disclosing information about its customers without the customer’s affirmative

---

9 This article does not consider state financial privacy laws affecting securities firms, certain other types of financial providers, or medical or health privacy laws affecting insurance companies.
10 Except for states that adopted the 1982 model Insurance Information and Privacy Protection Act of the National Association of Insurance Commissioners (NAIC).
consent; all but a handful of states\textsuperscript{11} have at least one statute, regulation, or judicial precedent that requires the customer of a covered financial institution to affirmatively consent to disclosure of nonpublic personal information.

Even though states are more likely to have opt-in formats, compliance with the GLBA is emerging as an alternative to state opt-in laws. In the 2001 legislative sessions, several states with opt-in financial privacy laws passed laws that essentially incorporate by reference the privacy provisions of the GLBA. Louisiana, North Dakota and Tennessee are examples. Two other states, Missouri and Maine, passed laws making a violation of the GLBA a violation of state law for financial institutions generally.

II. COVERAGE OF STATE FINANCIAL PRIVACY LAWS

A. Among Financial Institutions, Depository Institutions Are Most Likely To Be Restricted by Law from Disclosing Customer Financial Information. More than two thirds of the states have statutory or common law restrictions on the information sharing practices of depository institutions. Generally speaking, these laws prohibit the sharing of nonpublic personal information by banks, savings and loan associations, credit unions and other depository institutions without the affirmative consent of the customer. Some state financial privacy statutes cover only specific types of depository institutions, such as savings and loan associations, which are covered by the financial privacy laws of Kentucky, Minnesota, Mississippi, Missouri, New Jersey, New Mexico, Utah, and Wisconsin.

Examples of the restrictions applicable to a bank’s sharing of customer account information are found not only in statutes, but also in case law. New Jersey recognizes that a bank has a general duty of confidentiality to its customers. In \textit{Twiss v. State}, 591 A. 2d 913 (N.J.

\textsuperscript{11} Except Delaware, the District of Columbia, Nebraska, Nevada, South Dakota, Tennessee, and Wyoming. Of these, all but the District and Nevada restrict disclosures of financial information subject to a consumer’s right to opt out.
1991), the court observed that New Jersey recognizes a bank’s duty to keep confidential the bank records of a customer.¹²

New Jersey case law discusses this general duty of confidentiality in the context of a bank-depositor relationship and therefore, it does not appear that this duty of confidentiality would extend to other types of financial institutions. See Roth v. First Nat’l State Bank, 404 A. 2d 1182, 1184 (N.J. App. 1979) (“It must be conceded that there is a generally recognized obligation of confidentiality in respect of a depositor’s financial relationship with a bank.”); see also Brex v. Smith, 146 A. 34, 36 (N.J. Ch. 1929) (holding that information contained in bank records is a property right and therefore, there is an implied obligation on the part of the bank to keep such information confidential unless compelled by court order to do otherwise.)

Pennsylvania courts have reached a similar result. It has been held that a bank and its employees have an implied contractual duty to keep a customer’s bank account information confidential. McGuire v. Shubert, 722 A. 2d 1087, 1091 (Pa. Super. Ct. 1998). This decision appears applicable to all depository financial institutions, but only in their depository capacity. As far as depository institutions are concerned, however, the duty of confidentiality is unbounded, extending without explicit limitation to all account information. This rule is consistent with long-standing Pennsylvania criminal case law establishing that a bank “customer” has a reasonable expectation of privacy in “records pertaining to [his] affairs kept at the bank.” Commonwealth v. DeJohn, 403 A. 2d 1283, 1291 (Pa. 1979).¹³

In other states, where courts have held that financial institutions have a legal duty not to disclose information about the depositor’s account, certain exceptions have been articulated. For example, in Milohnich v. First National Bank of Miami Springs, 224 So. 2d 759, 762 (Fla. App. 1969), the Court cites with approval a purported summary of the formulation of Tournier v. National Provincial Bank, 1 K.B. 461 (1925) that a bank’s duty of confidentiality to the

¹² The Twiss court used the term ‘customer’ interchangeably with the term ‘depositor,’ leading to ambiguity about whether the duty of confidentiality extends only to depository account holders.

¹³ The Pennsylvania Supreme Court has recently been invited to limit the DeJohn decision by affirming a lower court holding that a bank customer does not have a reasonable expectation of privacy in his name and address. See Commonwealth v. Duncan, 752 A.2d 404, 412 (Pa. Super. Ct. 2000), appeal allowed, 762 A.2d 1082 (Pa. 2000). Unless and until the Pennsylvania Supreme Court affirms Duncan, however, it appears to be good law in Pennsylvania that an implied contractual duty of confidentiality applies to all deposit account information.
depositor does not extend to situations in which: (1) the disclosure is required by law, (2) there is a duty to the public to disclose the information, (3) the interests of the bank require disclosure, or (4) the disclosure is made with the express or implied consent of the customer. Milohnich, 224 So. 2d at 761.

B. Insurance Companies Are Subject To Comprehensive Privacy Rules In Many States. Fifteen states\(^{14}\) have enacted privacy laws based on the NAIC’s 1982 model Insurance Information and Privacy Protection Act, which establishes standards for the collection, use, and disclosure of personal and privileged information, including medical information, by insurance companies. The model law restricts the disclosure of a consumer’s personal or privileged information, except in specified circumstances, and imposes notice obligations on insurance companies. As adopted in many states, it also provides for a private right of action for violations.

Georgia’s Insurance Information and Privacy Protection Act\(^{15}\) is illustrative. Insurance institutions may not disclose personal or privileged information concerning an individual that was collected or received in connection with an insurance transaction. An exception to the rule of non-disclosure is available with written customer authorization. If the customer’s authorization is provided by another insurance institution, agent or insurance-support organization, the disclosure authorization form must comply with Ga. Code Ann. § 33-39-7, and if submitted by any other person it must be dated, signed by the individual, and obtained 1 year or less prior to

\(^{14}\) Arizona, California, Connecticut, Georgia, Illinois, Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, and Virginia.

\(^{15}\) The Georgia law defines “insurance institutions” as “any corporation, association, partnership, reciprocal exchange, interinsurer, Lloyd’s insurer, fraternal benefit society or other person engaged in the business of insurance, including health care plans, health maintenance organizations, medical service corporations, hospital service corporations, but not agents or insurance-support organizations. Ga. Code Ann. § 33-39-3(12). The Georgia law also applies to “agents,” defined as any agent, broker, subagent, counselor, adjustor, solicitor, or service representative, and to insurance-support organizations, defined as any person who regularly engages in assembling or collecting information on natural persons for the primary purpose of providing such information to an insurance institution or agent for insurance transactions, including the furnishing of consumer reports or investigative consumer reports and the collection of personal information for the purpose of detecting or preventing fraud and other misrepresentations in relation to insurance underwriting and insurance claim activity. Insurance-support organizations do not include agents, government institutions, insurance institutions, medical care institutions and medical care professionals. Ga. Code Ann. §§ 33-39-3(3), 33-39-3(13).
the date the disclosure is sought. There are also limited exceptions for disclosure to affiliates of the affected insurance institution, for disclosures to providers of services to the affected insurance institution, and for disclosures required in order to process or service a requested transaction. The making of a determination of eligibility for an applied-for insurance benefit would justify a disclosure under this latter exception.

Information that does not specifically identify individuals or their information is less closely protected under the insurance information and privacy protection law. Disclosure of personal and privileged information may be made for the purpose of conducting actuarial or research studies, if no individual is identified in the resulting report. Disclosure of personal or privileged information may also be made to the following parties under specified circumstances:

a. To medical-care institutions or medical professionals;
b. To an insurance regulatory authority;
c. To a law enforcement or other governmental authority;
d. As otherwise permitted or required by law;
e. In response to an administrative or judicial order (i.e. search warrant or subpoena);
f. To a party or representative of a party to a proposed or consummated sale, transfer, merger, or consolidation of all or part of the business of the insurance institution, agent or insurance-support organization;
g. To group policyholders to report claims experience or conduct an audit;
h. To a professional peer review organization;
i. To governmental authorities to determine an individual’s eligibility for health benefits for which government may be liable;
j. To a certificateholder or policyholder to provide information regarding the status of a transaction;

k. To a lienholder, mortgagee, assignee, lessor or other person shown on record to have a legal or beneficial interest in the insurance policy; or

l. By a consumer reporting agency, if the disclosure is to a person other than an insurance institution or agent.


C. Mortgage And Consumer Lenders Are Not Subject To Extensive Privacy Regulation at the State Level. Only a handful of states expressly regulate the information sharing practices of mortgage companies, including mortgage lenders, mortgage brokers, mortgage servicers and consumer lenders. Those that do include Louisiana, North Dakota, Tennessee, and Vermont. However, mortgage companies that are subsidiaries or affiliates of depository institutions may be subject to privacy restrictions in other states, particularly with respect to information used in connection with insurance sales.

Vermont is an example of the minority rule for financial information privacy governing mortgage companies. With limited exceptions, the Vermont Financial Privacy Act prohibits any financial institution from disclosing customer financial information to any person. This law applies to “financial institutions,” which include national and state financial institutions, credit unions, subsidiaries of financial institutions, licensed lenders, mortgage brokers and sales finance companies organized or regulated under the laws of the United States or any state.

---

16 Exceptions are available for disclosures made pursuant to consumer authorization (“opt in”) and disclosures made to those affiliates who have duties or responsibilities to the financial institution.


The law covers “financial information relating to a customer,” which is any information or information derived from the following as it relates to a customer:

1. A document that grants signature authority over a deposit or share account;

2. A statement, ledger card or other record of a deposit or share account that shows transactions in or with respect to that deposit or account;

3. A check, clear draft or money order that is drawn on a financial institution or issued and payable by or through a financial institution;

4. Any item, other than an institutional or periodic charge, that is made under an agreement between a financial institution and another person’s deposit or share account;

5. Any information that relates to a loan account or an application for a loan; or

6. Evidence of a transaction conducted by electronic or telephonic means.


As is the case with other state financial privacy laws, there are exceptions for disclosures with the customer’s consent, for disclosures that do not identify specific consumers or their transactions, and for disclosures to affiliates or those that are engaged in providing services to the financial institution.

Even if a state does not have a financial privacy law in place, it may attempt to enforce federal privacy law, or examine non-depository financial institutions, such as mortgage lenders, for compliance with federal law. 19

---

19 The Massachusetts Division of Banks has advised non-bank licensees under its jurisdiction that it will be examining them for compliance with the FTC privacy regulations issued under the Gramm-Leach-Bliley Act. All
D. Financial Privacy Protection May Be Limited to Certain Types of Transactions Under State Law. The laws of several states limit the disclosure of nonpublic personal information when specific transactions are involved, such as electronic funds transfer transactions. These privacy protections are found in the electronic funds transfer acts which restrict disclosure of customer or transaction-related information. States with such laws include Colorado, Iowa, Massachusetts, Michigan, Minnesota, Montana, and New Jersey. Other state laws address financial privacy for use of computerized banking terminals (i.e., ATMs) or other communications facilities.

For example, This Massachusetts Electronic Funds Transfer Act 20 which applies to any “person,” covers any information related to an account or electronic funds transfer. The general rule on information distribution is that a person may not disclose information regarding any account or electronic funds transfer to any other person. There are exceptions, of course, including disclosures with the consent of the consumer, and disclosures made in connection with the processing or servicing of a requested transaction. However, there are no exceptions in the law for disclosures to affiliates of the affected institution, or to providers of services to the institution.

III. OTHER SOURCES OF LAW, AND REMEDIES PROTECTING CONSUMERS’ FINANCIAL PRIVACY

A. Common Law, Interpreted by State Courts Also Protects Consumer Financial Privacy. As indicated above, in about one-third of the states, restriction on information sharing by a depository institution is based on common law theories, such as an implied contractual duty of confidentiality or, to a lesser extent, a tort of invasion of privacy. For example, the Ninth Circuit Court of Appeals, considering whether a cause of action for breach of an implied contract of customer privacy exists in Montana, stated that “it is unclear whether such a cause of action

licenses were asked to complete a Privacy Awareness Survey by June 15, 2001, or face an on-site privacy visitation to ensure compliance with the privacy regulations.

exists in Montana. Indeed, we agree with the district court that Mann Farms’ theory of liability seems more akin to a tort claim for breach of the implied covenant of good faith and fair dealing than to an invasion of privacy claim.” *Traders State Bank of Poplar v. Northeast Montana Bank Shares, Inc.*, 1992 U.S. App. LEXIS 28087 (9th Cir. 1992).

B. **State-Adopted Fair Credit Reporting Acts Are An Important Source Of Privacy Law.** More than a dozen states,21 have adopted laws that regulate collection and dissemination of consumer reports. While many of these laws closely mirror the federal Fair Credit Reporting Act, there are a number of state provisions that are unique or more restrictive than federal law. In general, these laws restrict users from obtaining consumer reports, except under specified conditions, and limit subsequent disclosures of consumer report information.

Violation of a state’s fair credit reporting act may be subject to specific sanctions not contemplated in federal law; an example is Nevada’s Fair Credit Reporting Act22 which makes a user of information in a consumer report liable for actual damages, punitive damages and attorney’s fees and costs for willful noncompliance with this law, which restricts the resale or redisclosure of consumer reports without disclosure to the provider of the identity of the intended user and the purposes for which the information will be used.

C. **Violations Of State Privacy Laws Are Typically Subject To Private Rights Of Action.** Unlike the GLBA, which does not expressly provide a private right of action for violation of its privacy provisions, many state financial privacy laws allow consumers whose personal information has been wrongfully disclosed to bring an action in court. Typical remedies include recovery of actual damages, attorney’s fees and costs. In addition, most state financial privacy laws authorize a regulatory agency to enforce the law. The regulator is typically the general regulator of the covered financial institution, such as the banking department or insurance commissioner, for state-chartered banks, and insurance companies, respectively. Regulatory agencies also have other sanctions at their disposal, such as the ability to withdraw an

---

21 Arizona, California, Kansas, Maine, Maryland, Massachusetts, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, Rhode Island, Vermont, and Washington.

22 Nev. Rev. Stat. § 598C.
III. REGULATORY ACTIONS

The regulators of the financial industry, including federal agencies such as the Federal Trade Commission and the Consumer Financial Protection Bureau, possess the authority to grant or refuse occupational license, or to issue cease and desist orders preventing unlawful disclosures. The combination of possible consumer lawsuits and regulatory action by the government creates a powerful incentive to compliance with state privacy laws.

IV. CONCLUSION

Despite the national attention being focused on compliance with the Gramm-Leach-Bliley Act, financial institutions, particularly those with multi-state operations and customer bases, cannot afford to overlook the myriad of state laws, rules and cases that further define their responsibilities in dealing with consumers’ financial information. The miscellaneous provisions of state laws are frequently more protective of consumers than federal law, and the remedies for non-compliance are likewise more varied.

The need for close review of state privacy laws is also recommended in light of the potentially greater likelihood of state scrutiny and enforcement. GLBA is new, but many of the state laws on privacy are of long standing. As GLBA is gaining its legs, consumer grievances and lawsuits on financial privacy issues may surface first in state forums, where courts protective of their citizens may be most sympathetic to privacy violations.

Finally, a financial institution’s compliance program for protecting consumers’ privacy must incorporate periodic review and updating of state privacy laws and court decisions. State laws are always subject to change, but with increased public and media attention to consumer privacy (including related topics such as identity theft) state legislators are likely to be more active in this area in the future than in the past.