Consumer Federation of America

CFA HANDBOOK
FEDERAL AND STATE LEGAL PROTECTIONS OF CONSUMERS' FINANCIAL INFORMATION PRIVACY AND SECURITY[1]

I. Introduction

The primary federal law intended to protect the privacy and security of consumers' financial information held by financial service providers is the Gramm-Leach-Bliley Act. The rules the U.S. Federal Trade Commission has promulgated to implement that Act reach a much broader swatch of credit providers than do the rules of the several other federal and state regulators which also enforce that law.

In addition, the Fair Credit Reporting Act, the Internal Revenue Code and a variety of state laws and regulations provide consumers with protection in the handling of their credit report and tax return information by financial service providers.

The Gramm-Leach-Bliley Act[2], also known as the Financial Services Modernization Act of 1999, was enacted by the Congress of the United States on November 12, 1999. The Act had multiple purposes, among which was to remove existing federal legal barriers[3] that prevented the integration of banking, stock brokerage, and insurance activities within a single business entity. There was a concern, however, that by combining two or all three of these activities, a single business would have access to a far greater range of sensitive information on any one consumer than it had under the then-existing separation requirements. Other abuses in the use of consumers' financial information contributed to the need for several legal provisions[4]. As a result, the Congress included in the Act a set

[1] The Handbook author is Mark Silbergeld, CFA Senior Fellow.

[2]Public Law 106-12, 15 U.S.C. § 6801 *et seq*., hereinafter sometimes referred to as "GLB" or "the Act." The names in the popular "GLB" title of this statute refer to three Members of Congress who were its instrumental sponsors, Senator Phil Gramm (R-TX), Chairman of the Senate Banking Committee; Representative Jim Leach (R-IA), Chairman of the House Banking Committee; and Representative Thomas Bliley (R-VA), Chairman of the House Commerce Committee. All "U.S.C." citations in this document were viewed at the Cornell University Law School website and are accessible via that site's U.S.C. home page, http://www4.law.cornell.edu/uscode/. Citations below to the Code of Federal Regulations ("C.F.R.") are accessible via the companion CFR home page, http://www.law.cornell.edu/cfr/ or the eCode of Federal Regulations as redirected to that resource from the Cornell website.

[3]These were contained in the Glass-Steagall Act of 1933, also known as the Banking Act, 48 Stat. 162, and the Bank Holding Company Act of 1956, 12 U.S.C. § 1841 *et seq*.

[4]See "The Gramm-Leach-Bliley Act," Electronic Privacy Information Center, http://epic.org/privacy/glba, accessed June 9, 2008, at pp. 2-3 for some examples.

of provisions establishing four basic consumer privacy rights[5] and the means for their enforcement[6].

These rights are:

- The consumer's right to know how a financial services provider ("financial institution," in the terms of the Act) will use his or her nonpublic personal financial information;

- The consumer's right, with exceptions, to opt out of having this information transferred to nonaffiliated third parties;

- The consumer's right to have the financial services provider securely safeguard and protect his or her nonpublic personal information against unauthorized access; and

- The consumer's right not to have this information obtained by third parties through the use of fraud or deception.

And, because the combined information could come into the hands of unrelated, "third party" businesses, these rights were more broadly applied to cover virtually all businesses engaged in consumer transactions relating to lending and other consumer financial matters, as well as to all parties seeking the information about a consumer from entities that possessed it. GLB limits the conditions under which a business can provide to another, unrelated business the data it has on any consumer. It also limits the basis on which any business can request such information from other businesses[7].

State consumer financial laws that are not inconsistent with GLB may exceed its requirements and GLB does not prevent state authorities from separately enforcing such state laws[8], whether equivalent to or more protective than GLB.

The privacy provisions of GLB fall into three main categories: (1) the requirements for a financial services provider to give notification to its consumers regarding its policies about the collection and sharing of consumer financial information; (2) the right of a

---

[5]Title V, Subchapter A, which is the subject of this report, also hereinafter referred to as "GBL" or "the Act," since the rest of the Act is beyond the scope of this report.

[6]Instead of giving the enforcement authority to a single agency, the Act provides for enforcement with respect to various categories of "financial institutions" by the various federal agencies that oversee these institutions. As has been the case in previous statutes regulating financial transaction practices, residual enforcement authority is given to the U.S. Federal Trade Commission. As discussed below, the agencies have coordinated their promulgation of rules under GLB. State insurance authorities have enforcement authority with regard to insurers and consultative status in the development of these rules, since most regulation of insurance is the exclusive jurisdiction of the states.

[7]These provisions are directed against the practice of "pretexting," which is the act of obtaining financial information under false pretenses.

[8]15 U.S.C. § 6807. 16 C.F.R. § 313.17. The Federal Trade Commission has the legal authority to determine the consistency or inconsistency of state laws vis-à-vis Gramm-Leach Bliley. *Id.*

consumer to opt out of having certain personal financial information shared by a financial services provider with an unaffiliated, third party; and (3) the requirements for protection by a financial services provider of covered consumer financial information in its possession. In addition, the Act codifies and makes enforceable by all GLB implementing Agencies the traditional trade practices law ban on pretexting, which is the practice of obtaining nonpublic personal consumer information under false pretenses.

II. Primary Privacy Protection Purposes of Gramm-Leach-Bliley

In Gramm-Leach-Bliley, Congress declares a policy of financial services provider responsibility with regard to consumer privacy:

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.[9]

To further this policy, the Congress charges each agency or authority responsible for administering GLB with establishing appropriate standards for the financial institutions. These standards relate to administrative, technical and physical safeguards, in order to achieve the purposes of the Act:

> (1) To insure the security and confidentiality of customer records and information;
>
> (2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[10]

These are the three basic principles of GLB. To effect these principles, the Act establishes legal requirements for each "financial institution" in its handling and disclosure of "nonpublic personal information" about a "consumer" or "customer," including disclosure to a "nonaffiliated third party." The meaning and scope of these terms is important to understanding Gramm-Leach-Bliley.

[9] 15 U.S.C. § 6801(a).
[10] 15 U.S.C. § 6802(b).

III. Important Definitions Under Gramm-Leach-Bliley

A. What entities are "financial institutions"?

Gramm-Leach-Bliley's requirements apply to "financial institutions"[11]; the Agency enforcement rules only apply to those financial institutions (financial service providers) that are "significantly engaged in"[12] any of the following activities:

- Lending[13], including mortgage lending[14], mortgage brokerage[15], payday lending[16] and lending by colleges and universities[17];
- Government provision of consumer financial services such as student loans or mortgages[18];
- Retail credit extension[19];
- Medical service provision that establishes for a significant number of the provider's patients long-term payment plans that involve interest charges[20];
- Automobile leasing for a period of at least 90 days, and lease financing[21];
- Leasing real or personal property on an initial lease term of at least 90 days[22];
- Check cashing[23];
- Check guaranty services[24];

---

[11] 15 U.S.C. § 6809(3)(A), referring to 12 U.S.C. 1843(k), the Bank Holding Company Act, Subparagraph (k)(4) of which contains the relevant language. This report uses the terms "financial institution," "financial services provider," and "provider" interchangeably.

[12] 16 C.F.R. § 313.3(k)(1). "Significantly engaged in" is a flexible standard that takes into account all the facts and circumstances. The F.T.C. specifically does not apply the Rules to, for example, retailers that accept third party credit cards but do not issue their own; to stores that allow customers to get cash back by writing a check for more than the amount of a purchase; to merchants that allow customers to run a tab; or to retailers that provide occasional layaway or deferred payment plans. 16 C.F.R. § 313.3(k)(4). "Gramm-Leach-Bliley Act, Privacy of Consumer Financial Information," FTC staff, http://www.ftc.gov/privacy/glbact/glboutline.htm , accessed September 8, 2008, hereinafter "FTC Staff Outline."

[13] 12 U.S.C. § 1843 (k)(4)(A); FTC Staff Outline p. 3.

[14] FTC Staff Outline p. 3.

[15] 16 C.F.R. § 313.3(k)(2)(xi). FTC Staff Outline p. 3.

[16] FTC Staff Outline p. 2.

[17] The F.T.C. has jurisdiction over colleges and universities for purposes of Gramm-Leach-Bliley, but will consider such an institution in compliance with GLB to the extent it is in compliance with the Federal Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. part 99, which govern the privacy of education records, including student financial aid records. 16 C.F.R. §313.1(b). See 65 Fed. Register No. 101, Wednesday, May 24, 2000 at p. 33648 for a discussion of this issue.

[18] FTC Staff Outline p. 3.

[19] 16 C.F.R. § 313.3(k)(2)(i). FTC Staff Outline p. 3.

[20] FTC Staff Outline p. 3.

[21] 16 C.F.R. §313.(k)(2)(iii). FTC Staff Outline p. 3.

[22] As determined by the Federal Reserve Board, 12 U.S.C. §1843(k)(4)(F), 12 C.F.R. §225.28. FTC Staff Outline p. 2.

[23] 16 C.F.R. §313.(k)(2)(vii); FTC Staff Outline, p. 3.

- Issuing cash to a consumer through an ATM not operated by a financial institution with which the consumer has a bank account and regardless of the frequency with which a consumer uses that ATM network[25];
- Sale of money orders, savings bonds or traveler's checks[26];
- Relocation services that assist individuals with financing for moving expenses and/or mortgages[27];
- Money wiring[28], money exchange and transfer services[29];
- Investment services[30];
- Financial, investment and economic advisory services[31];
- Credit counseling[32];
- Depository services[33];
- Sale of money orders, savings bonds or traveler's checks[34];
- Check printing services sold to consumers[35];
- Tax preparation, whether or not performed by an accountant[36];
- Insurance, insurance agency and insurance brokerage[37];
- Issuing or selling direct investment in a bank's directly held pooled assets[38];
- Underwriting, dealing in or making a market in securities[39];
- Real estate and personal property appraisal[40];
- Real estate settlement services[41];
- Servicing loans[42];
- Collection agency services,[43];
- Check guaranty services[44];
- Credit bureau services[45],

---

[24]FTC Staff Outline p. 2.
[25]FTC Staff Outline, p. 3.
[26]*Id.*
[27]*Id.*
[28]16 C.F.R. §313.(k)(2)(vi).
[29]FTC Staff Outline p. 4.
[30]FTC Staff Outline p. 2.
[31]12 U.S.C. § 1843(k)(4)(C). FTC Staff Outline p. 2.
[32]16 C.F.R. § 313.3(k)(2)(xii). FTC Staff Outline p. 2.
[33]FTC Staff Outline p. 2, "safeguarding money or securities."
[34]FTC Staff Outline p. 3.
[35]16 C.F.R. § 313.3(k)(2)(v).
[36]16 C.F.R. § 313.3(k)(2)(viii). However, a certified public accountant (CPA) is exempt under § 6803(d) of the Act from providing the otherwise required annual disclosure. See the discussion below of the Internal Revenue Service rules relating to tax preparer handling of consumer financial information.
[37]12 U.S.C. § 1843(k)(4)(B). FTC Staff Outline p. 2.
[38]12 U.S.C. § 1843(k)(4)(D).
[39]12 U.S.C. § 1843(k)(4)(E). FTC Staff Outline p. 2.
[40]16 C.F.R. § 313.3(k)(2)(ii). FTC Staff Outline p. 2.
[41]16 C.F.R. § 313.3(k)(2)(x). FTC Staff Outline p. 2.
[42]FTC Staff Outline p. 2.
[43]*Id.*
[44]*Id*.

- Operating a travel agency in connection with financial activities[46].

The Act expressly does *not* apply to certain financial transactions:

- Transactions with the Federal Agricultural Mortgage Corporation or any agency chartered and operating under the Farm Credit Act of 1971[47];

- Secondary market sale or securitization of the consumer's debt (including servicing rights) by institutions chartered by Congress specifically to engage in such transactions (including Fannie Mae and Freddie Mac), to the extent these institutions do not sell nonpublic personal information to a nonaffiliated third party [48].

Therefore, a business is not a "financial institution" under the GLB Act simply because it engages in one of those activities[49].

B. What is "nonpublic personal information"?

The Act only protects "nonpublic personal information." Financial information that is "personally identifiable[50]" to a specific consumer is "nonpublic personal information" if it is:

---

[45] *Id.*
[46] 12 U.S.C. § 1841 *et seq*. 16 C.F.R. §313.(k)(2)(ix). FTC Staff Outline p. 2.
[47] 6809 U.S.C. § (3)(C).
[48] 15 U.S.C. § 6809(D).
[49] The Act originally did not include commodity futures trading within the jurisdiction of the Commodity Futures Trading Commission. 15 U.S.C. § 6809(3)(B). However, this omission was eliminated with the enactment of the Commodity Futures Modernization Act of 2000 ("CFMA") on December 21, 2000. Under Section 124 of the CFMA, Congress amended the Commodity Exchange Act ("CEA") to add a new Section 5g to the CEA to include the CFTC and certain financial institutions subject to its jurisdiction within Title V of GLB. That section of the CFMA makes the CFTC a "federal functional regulator" and mandates that it promulgate privacy rules for certain entities subject to its jurisdiction. These entities are: (1) futures commission merchants, (2) CTAs, (3) CPOs, and (4) introducing brokers. However, institutions subject to the CFTC's GLB authority need only comply with the Act with regard to transactions involving consumers trading in commodity futures for personal, family, or household purposes; transactions involving institutional investors are not covered by GLB. See CFTC 01-70, July 6, 2001, http://www.cftc.gov/tm/letters/01letters/tm01-70.htm, viewed August 1, 2008.
[50] 15 U.S.C. § 6809(4)(A). 16 C.F.R. §313.3(n)(1)(i). Financial information is "personally identifiable" if the consumer provides it to the financial institution; if it is about a consumer resulting from any transaction between the consumer and the institution involving a financial product or service; or if the financial institution otherwise obtains the information about a consumer in connection with providing a financial product or service to that consumer. Personally identifiable financial information includes information provided by the consumer on an application to obtain a financial product or service; account balance information; payment history; overdraft history; credit or debit card purchase information; the fact that an individual is or has been the institution's customer or has obtained from it a financial product or service; information gathered in the process of servicing or collecting on a consumer's credit account; and information collected through an Internet cookie. 16 C.F.R. §313.3(o).

- Not publicly available[51]; and
- Is provided by a consumer to a financial institution[52]; or
- Results from any transaction with the consumer[53]; or
- Results from any service performed for the consumer[54]; or
- Is otherwise obtained by the financial institution[55].

Nonpublic personal information includes data obtained from a list, description or grouping of multiple consumers (as contrasted with data relating only to a specific individual), but *only* if it is derived from nonpublic personal information[56] regarding provision of a financial product or service[57]. A list of names and addresses derived from a computer search of a published telephone directory is *not* nonpublic personal information[58]

Examples of nonpublic information include an individual's:

- Name and address if it is *not* published in a publicly available record such as a phone book;
- Social security number;
- Account number;
- The fact that the individual is a customer of a particular financial institution;
- Any information a consumer provides on an application;
- Information contained in an electronic "cookie" obtained in using a website; and

[51] 15 U.S.C. § 6809 (4)(B). FTC Staff Outline, p. 5. "Publicly available" means any information a financial institution has a reasonable basis to believe is lawfully made available to the general public from federal, state or local government record, or is contained in widely distributed media, or disclosure of which is required to be made public by Federal, State or local law. 16 C.F.R. §313.3(p)(1). A "reasonable basis" means that the information is of the type that is generally available to the public, *if* the financial institution has taken steps to affirm that the information is available to the general public and, if the consumer can direct that the information not be made public, whether that consumer has done so. 16 C.F.R. §313.3(p)(2).
[52] 15 U.S.C. § 6809 (4)(A)(i).
[53] 15 U.S.C. § 6809 (4)(A)(ii).
[54] *Id.*
[55] 15 U.S.C. § 6809(4)(A)(iii).
[56] 15 U.S.C. § 6809(4)(C)(i) and (ii).
[57] 16 C.F.R. §313.3(n)(1)(ii). The FTC staff offers as an example of a list that does *not* constitute nonpublic information a list of persons who purchased washing machines from a retailer, if the list was not otherwise derived from information obtained in providing a financial service or product. FTC Staff Outline p. 7.
[58] 16 C.F.R. § 313.3(n)(2)(ii).

- Information on a consumer report obtained by a financial institution[59].

A list of names and street addresses (or any other list) is "nonpublic information," if it is derived from a list that contains nonpublic personal financial information. For example, a list of names and street addresses taken from a list that includes names, street addresses and financial institution account numbers is nonpublic personal information[60], even if the account numbers do not appear on the derived list, or if it identifies the listed individuals as the consumers of a financial institution, and *even if* the same list could be derived independently by searching the telephone directory. But, a list of names and street addresses derived *strictly* from public sources such as a telephone directory and *not containing* any financial information would not be nonpublic personal information[61].

There is, of course, *no* GLB restriction on a financial service provider's disclosure to other parties of *publicly available* information. This includes any information that the provider has a reasonable basis to believe[62] is lawfully made available to the general public from federal, state or local records, widely distributed media or disclosures to the general public required by Federal, State, or local law[63]. Public information that can be freely distributed includes such information as the fact that an individual is a mortgage customer of a particular financial institution, *if that fact is recorded in public real estate records*[64]; published telephone numbers; and information lawfully available to the general public on a website, including a website that requires a password or fee for access[65].

C. Who is a "consumer"? Who is a "customer"? What is the difference?

The Act and the agency rules draw a distinction between a "consumer" and a "customer." Different notice requirements sometimes apply to these two categories of individuals. Financial service providers owe greater disclosure requirements to customers than to consumers.

---

[59]FTC Staff Outline p. 6.
[60]16 C.F.R. § 313.3(n)(3)(i).
[61]16 C.F.R. § 313.3(n)(3)(ii)
[62]*Id.* The FTC staff states that a financial institution cannot assume particular information is publicly available. The institution must take steps to determine if the information is of the type generally made available to the public, whether an individual can opt to keep the information nonpublic and [if so] whether the particular consumer has directed that the information not be disclosed.
[63]FTC Staff Outline p. 6.
[64]*Id.* Similarly, public information would include liens recorded in a public record, bankruptcy notices naming an individual, and lawsuits filed by or against an individual and recorded by a clerk of court.
[65]*Id.* Some fee for access websites will search public records and provide requesting customers with a wide range of information, such as a history of a search subject's past home addresses, marriages and divorces, bankruptcies, civil judgments, liens against property and criminal records. Other websites such as facebook.com and myspace.com may contain personal information self-posted by an individual or posted by another person about that individual.

A "consumer" is "an individual who obtains, from a financial services provider, financial products or services which are to be used primarily for personal, family or household purposes." The term also includes such an individual's legal representative[66].

A "customer" of a financial institution is a consumer with whom the provider has a "continuing relationship" under which it provides "one or more financial products or services to the consumer that are customarily to be used primarily for personal, family or household purposes"[67]. For example, an individual who takes a payday loan from Lender A is Lender A's customer, because the relationship continues until the loan is fully repaid. But if the individual uses Check Casher B to cash a check, that consumer is B's consumer but not its customer, since there is no continuing relationship beyond the cashing of the check. And that remains true even if the consumer regularly cashes checks with B[68]. As indicated below in the discussion of what disclosures are required under the Act and Agency rules, Check Casher B can make a more simplified disclosure to this consumer than Lender A must make to an individual who is its customer.

D. What is a "nonaffiliated third party"?

A "nonaffiliated third party," with respect to a financial services provider, is *any* individual or entity[69] except:

- The provider's own affiliates; and
- A person employed jointly by the provider and any company that is not its affiliate.

A nonaffiliated third party includes an unaffiliated entity that jointly employs such a person[70].

IV. Which Federal Agencies Regulate which Financial Services Providers?

The establishment of rules to implement Gramm-Leach-Bliley, and the enforcement of these rules, is divided among various Federal agencies, according to what kinds of financial service providers each of these agencies primarily regulates. In addition, because most aspects of insurance are under the sole jurisdiction of the States, insurers

[66]15 U.S.C. § 6809(4)(9). 16 C.F.R. § 313.3(e)(1). From this definition, it follows that a cash purchase involving no credit (and no extended payments that would under law legally constitute credit), such as paying full cash price for a used car, is not a transaction involving a "consumer," for GLB purposes, because no financial products or services are obtained in the transaction. Similarly, an individual who purchases a car on credit primarily for business use is not a "consumer" for purposes of the Act, because the obtained product is not to be used primarily for personal, family or household purposes. And, in the same vein, the purchase of a car, whether or not on credit, from a generous relative who is not in the car business and does not usually engage in such transactions would not constitute purchase by a "consumer" for the Act's purposes, because there is no financial institution involved.
[67] 16 C.F.R. § 313.3(h).
[68]See 16 C.F.R. § 313.3(i)(2)(L)(ii).
[69]The FTC rule refers to "anyone." See *fn. 69*, below.
[70]16 C.F.R. § 313.3(m)(1).

are for the most part regulated with respect to the Act by the State insurance regulators[71]. The Federal agencies are:

- **The Federal Trade Commission**, with regard to all financial service providers governed by the Act that do not fall under the jurisdiction of another federal Agency or under State insurance authority[72];

- **The Federal Reserve Board** with respect to State Federal Reserve System member banks, bank holding companies and certain of their nonbank subsidiaries or affiliates, state uninsured banks, agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and "Edge" and "Agreement" corporations[73];

- **The Office of Thrift Supervision** (part of the Treasury Department), with respect to savings associations whose deposits are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations, but not subsidiaries that are brokers, dealers, persons providing insurance, investment companies or investment advisors[74];

- **The Office of the Comptroller of the Currency** (part of the Treasury Department), with respect to national banks, District of Columbia banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities, with certain exceptions[75];

- **The Federal Deposit Insurance Corporation**, with respect to banks insured by the FDIC (other than members of the Federal Reserve System), insured state branches of foreign banks, and certain subsidiaries of such entities[76];

---

[71] 15 U.S.C. § 6804(a)(1). See Section VI below and Appendix A.
[72] 16 C.F.R. § 313.1(b).
[73] 12 C.F.R. §216(1)(b). An "Edge" corporation is a US banking corporation organized under Section 25 (a) of the Federal Reserve Act (the popular name of Section 25 is the Edge Act) to carry out international banking activities. An Edge corporation is generally required to verify that every deposit taken or credit transaction conducted is related to an international transaction. http://www.anz.com/edna/dictionary.asp?action=content&content=edge_corporation, viewed October 10, 2008. An "Agreement" corporation is a state chartered bank, formed to carry out international transactions, that enters into an agreement with the Federal Reserve Board to limit its activities to those permitted under the Edge Act. http://financial-dictionary.thefreedictionary.com/Agreement+corporation, viewed October 10, 2008.
[74] 12 C.F.R. § 573.1(b).
[75] 12 C.F.R. § 40.1(b)(1). The exceptions are: a broker or dealer that is registered under the Securities Exchange Act of 1934; a registered investment adviser (with respect to the investment advisory activities of the adviser and activities incidental to those investment advisory activities); an investment company registered under the Investment Company Act of 1940; an insurance company that is subject to supervision by a State insurance regulator (with respect to insurance activities of the company and activities incidental to those insurance activities); and an entity that is subject to regulation by the Commodity Futures Trading Commission.
[76] 12 C.F.R. § 332(1)(b).

- **The National Credit Union Administration**, with respect to federally chartered credit unions[77];

- **The Securities and Exchange Commission**, with respect to broker-dealers, funds, investment companies and investment advisers, whether domestic or foreign, that are registered with the SEC, as well as unregistered broker-dealers operating within the U.S.[78];

- **The Commodity Futures Trading Commission**, with respect to futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers that are subject to the jurisdiction of the Commission, regardless whether they are required to register with the Commission[79].

The Federal Trade Commission is the primary enforcement agency with regard to the vast majority of financial service providers covered by Gramm-Leach-Bliley. And because, unlike most depository institutions, these providers are not subject to direct licensing, regulation and periodic examination requirements, the providers under the FTC's jurisdiction include the ones most likely to violate GLB and the other laws and regulations that protect consumers' financial information privacy and security.

V. How to Contact the Federal Agencies

Consumers can contact the Federal agencies with inquiries or complaints about Gramm-Leach-Bliley issues.

Federal Trade Commission.
Mailing address: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Toll free phone: 1-877-382-4357; TTY: 1-866-653-4261. Links to online complaint forms at the website. Website: http://ftc.gov/ftc/contact.shtm.

Federal Reserve System. Mailing address: Federal Reserve Consumer Help, PO Box 1200, Minneapolis, MN 55480. Phone: 888-851-1920; TTY: 877-766-8533; Fax: 877-888-2520. E-mail: ConsumerHelp@FederalReserve.gov. Website: http://www.federalreserveconsumerhelp.gov/?District=13.

Office of Thrift Supervision. Mailing address: 1700 G Street, NW, Washington, DC 20552. Phone: 1-800-842-6929; TTY: 1-800-877-8339; Fax: 202-906-7342. E-mail: consumer.complaint@ots.treas.gov. Website: http://www.ots.treas.gov/?p=ConsumerComplaintsInquiries.

Comptroller of the Currency. Mailing address: Office of the Comptroller of the Currency, Customer Assistance Group, 1301 McKinney Street, Suite 3450, Houston, TX

[77] 12 C.F.R. § 716(1)(b).
[78] 17 C.F.R. § 248(1)(b). The SEC rule is also known as Regulation S-P.
[79] 17 C.F.R. § 160.1(b).

77010. Toll free phone: 1-800-613-6743: Fax: 703-812-1020. E-mail: Customer.Assistance@occ.treas.gov. Website: http://www.occ.treas.gov/customer.htm.

Federal Deposit Insurance Corporation. Mailing address: Federal Deposit Insurance Corporation, Consumer Response Center, 2345 Grand Boulevard, Suite 100, Kansas City, MO 64108-2638. Phone: Toll free phone: 877-275-3342; TDD: 800-925-4618. E-mail: (customer assistance form): https://www2.fdic.gov/starsmail/index.asp. Website: http://www.fdic.gov/consumers/consumer/ccc/index.html.

National Credit Union Administration
Mailing address: National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314-3428. Phone: 703-518-6300; Toll free Consumer Assistance Hotline: 1-800-755-1030. Website: http://www.ncua.gov/consumerinformation/index.htm.

Securities and Exchange Commission
Mailing address: SEC Complaint Center, 100 F Street NE, Washington, D.C. 20549-0213. Fax: 202-772-9295. Link to online financial privacy complaint form: http://www.sec.gov/complaint/selectconduct.shtml (click on 5th button). Website: http://www.sec.gov/index.htm.

Commodity Futures Trading Commission
Mailing address: Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581. Phone: 202-418-5000; Toll free: 1-866-366-2382; TTY: 202-418-5514. E-mail: questions@cftc.gov (inquiries); enforcement@cftc.gov (complaints). Online electronic complaint form: http://www.cftc.gov/customerprotection/redressandreparations/howtoreportinformationtous/complaintform/index.htm. Website: http://www.cftc.gov/index.htm.

VI. State Regulators Enforce Insurance Companies' Gramm-Leach-Bliley Obligations

State insurance authorities are tasked by Gramm-Leach-Bliley with enforcing the Act's requirements regarding the state-regulated insurance industry. The state insurance commissioner's professional association, the National Association of Insurance Commissioners (NAIC), has issued two model regulations for adoption by state commissioners. One is the NAIC model regulation on Privacy of Consumer Financial and Health Information. The other is the NAIC's Standards for Safeguarding Customer Information Model Regulation. Some states still rely on an earlier NAIC model rule, the Insurance Information and Privacy Protection Model Act, issued by NAIC in 1982[80].

As of March 1, 2002, all fifty states and the District of Columbia had taken some action to ensure that insurance companies under their jurisdiction meet GLB's disclosure and notice requirements. In addition, some states have included or retained provisions in their regulations or laws that, in their respective views, provide greater protections or more restrictive requirements than those contained in GLB. All fifty-one jurisdictions have

[80]See http://www.wileyrein.com/publication.cfm?publication_id=12328.

regulations regarding privacy practices, notices, and consumer opt out procedures and/or standards for securing customer information, with respect to the insurance industry. [81]

A. State Insurance Authorities

The information in Appendix A identifies and provides contact information for the state regulators who administer Gramm-Leach-Bliley with respect to insurance companies. Where feasible, the relevant regulations are identified, as well. And, for those that are viewable online, a link is provided to a reproduction of the text of the statute or regulation(s) that were in effect as of October 2008. Consumer inquiries to these regulators about GLB should provide the relevant regulation or statute if it is cited in Appendix A[82].

VII. Consumers' Rights to Receive Disclosures and to Opt Out of Having Their Information Shared

The Act establishes legal requirements that a "financial institution" must meet *before* making any disclosure of "nonpublic personal information" about a "consumer" to a "nonaffiliated third party." The first requirement is to give initial notice of privacy policies and practices to the institution's consumers and customers. The second is to afford the consumer or customer the opportunity to opt out of having such information disclosed *before* the information is disclosed. It is important to understanding the initial notice requirements to remember the distinction between a "consumer" and a "customer," as described in Section "III C," above.

The Agency rules provide for four kinds of disclosure forms regarding a financial services provider's privacy policies and practices:

- The initial complete disclosure form to be provided to customers, in most cases at the time the customer relationship is established;
- A short form of disclosure to be provided to consumers who are not (or not yet) customers;
- The revised form, to update customers when provider's privacy policies or practices are changed; and

[81] "Financial Privacy: Status of State Actions on Gramm-Leach-Bliley Act's Privacy Functions," U.S. General Accounting Office, Report to the Ranking Minority Member, Committee on Energy and Commerce, U.S. House of Representatives, April 2002, p.3, http://www.gao.gov/new.items/d02361.pdf, viewed September 24, 2008.

[82] Where it is indicated that the text of a law or regulation is "reproduced at" an Internet address, the state agency posting the information --sometimes the insurance regulator, but sometimes the Secretary of State or the State Compiler of Statutes and Regulations -- may not vouch for the precise accuracy of the online text, as compared with the official copy of the text as officially filed with whichever Agency is the State repository of official documents, or as officially published in print. The use of scanners to copy printed text for web page use may introduce errors.

- The annual notice to customers.

A. Notice of privacy policies and practices

A provider generally may not, directly or through any affiliate, disclose to an unaffiliated third party any nonpublic personal information about a consumer unless the institution has first given that consumer a notice of its privacy policy that complies with the Act[83].

B. Initial, Annual and Revised Privacy Notices

A notice must be given to a provider's *consumer* before any nonpublic personal financial information is disclosed to a nonaffiliated third party. A notice is required to be given to a consumer who is the provider's *customer* no later than when the "customer relationship" with that consumer is established.

In the case of credit extended to purchase goods or services, a "customer relationship" comes into being at the time at which the credit relationship is established between a provider and a consumer[84]. Other examples of the establishment of a customer relationship are when the consumer:

- Opens a credit card account;
- Executes a contract of insurance;
- Agrees to obtain financial, economic or investment advisory services for a fee;
- Agrees to provide/receive credit counseling or tax preparation services;
- Provides any personally identifiable financial information to a provider in an effort to obtain a mortgage loan;
- Executes a lease for personal property; or
- Becomes the subject of an attempt to collect on an account acquired from another financial institution[85].

When an existing customer of a financial institution obtains a new financial product or service from the institution, that customer is entitled to a new notice *unless* the notice most recently provided by the institution to that customer (initial, revised or annual) was accurate with respect to the new financial product or service[86].

---

[83] 15 U.S.C. § 6802(a).
[84] 15 U.S.C. § 6809(11). The FTC rule describes this in terms of the time that a loan is "originated," 16 C.F.R. § 313.4(c)(2).
[85] 16 C.F.R. § 313.4(c)(3)(i)(c)
[86] 16 C.F.R. § 313.4(d).

When a financial institution purchases the servicing rights to a consumer's loan from another institution, the relationship with the new institution comes into being at the time of the purchase and a disclosure of the new owning institution's privacy policies and practices must be provided to the consumer[87].

The financial institution must give the customer clear and conspicuous notice[88] of its consumer privacy policies[89] in writing or in electronic form that can be retained or accessed later. (This retainability requirement does not apply to a consumer who is not a customer[90].) The initial disclosure must be updated at least annually[91]. Notices must describe the institution's policies and practices with respect to:

- The categories of nonpublic personal information that the institution collects[92];
- The categories of nonpublic personal information that will be disclosed[93];

[87]16 C.F.R. § 313.4(c)(3)(ii)(B).

[88]The FTC rule explains "clear and conspicuous" as reasonably understandable and designed to call attention to the nature and significance of the information in the notice. By "reasonably understandable," it means clear and concise language, concrete and plain language, and use of the active voice. A clear and conspicuous disclosure should use concise sentences, paragraphs, and sections; use short explanatory sentences or bullet lists whenever possible; avoid multiple negatives; avoid legal and highly technical business terminology whenever possible; and avoid explanations that are imprecise and readily subject to different interpretations. "Designed to call attention" means using plain language headings, easily read typeface and type size, wide margins and ample line spacing, and using boldface or italics for key words. On a website, the FTC suggests using text or visual cues to encourage scrolling down the page to view the entire notice, placement of the notice on a frequently accessed page or via a clearly labeled link and the absence of distracting graphics or sound. 16 C.F.R. § 313.3(b). FTC Staff Outline p. 7. These standards apply to the opt out notice as well as to the initial and annual notices. The FTC addresses three other kinds of notices, in addition to the three (initial, annual and opt out) specified in the Act: a "Short-Form" notice that can be provided to consumers, prior to sharing information about them, who are not the institution's customers; a "Simplified" notice to customers if the institution does not share nonpublic personal information about them during or after the customer relationship (other than sharing under the exceptions discussed above); and the "Revised" notice to consumers, customers, and former customers, whenever the institution needs to change the content of its notice.

[89]As defined by GLB.

[90]16 C.F.R. § 313.9(e).

[91] 15 U.S.C. 6803(a). 16 C.F.R. § 313.5(a). "Annually" means at least once in any period of 12 months during which the customer relationship exists. *Id.*

[92]15 U.S.C. § 6803(c)(2). 16 C.F.R. §313.6(a)(1). The FTC lists the following as disclosures that a financial institution can use (if appropriate) to describe categories of nonpublic personal information that the financial institution collects: (1) information obtained from the consumer, (2) information obtained from the consumer's transactions with a financial institution or its affiliate, (3) information obtained from affiliated third parties about the consumer's transactions with them, and (4) information obtained from a consumer reporting agency. Making this set of disclosures and including a few illustrative examples satisfies this disclosure requirement. 16 C.F.R. §313.6(c)91). FTC Staff Outline p. 8.

[93] 15 U.S.C. § 6803(c)(1)(A). 16 C.F.R. §313.6(a)(2). If the institution discloses nonpublic personal information to nonaffiliated third party service providers for purposes of marketing or servicing accounts, the disclosure in this respect only need state that nonpublic personal information is provided to other parties as permitted by law. Making these disclosures satisfies this disclosure requirement: 16 C.F.R. § 313.6(b). A financial institution may meet this disclosure requirement, if it reserves the right to disclose to nonaffiliated third parties all of the nonpublic financial information it may collect about a consumer, by simply stating that fact without providing any examples. *Id.*

- The categories of nonpublic personal information to affiliates and to nonaffiliated third parties to whom the information is disclosed[94];

- The categories of nonaffiliated third parties to whom such information is or may be disclosed[95];

- Disclosure policies and practices regarding nonpublic personal information of persons who have ceased to be customers of the financial institution and the categories of nonpublic personal information disclosed under these policies and practices[96];

- An explanation of the consumer's opt out right, including the methods by which that right may be exercised at the time of the notice[97];

- Protection of the confidentiality and security of nonpublic information[98];

- Disclosures required under the Fair Credit Reporting Act regarding the consumer's right to opt out of sharing among the financial institution's affiliates[99];

- Policies and practices of the financial institution with respect to protecting the confidentiality and security of nonpublic personal information[100].

If a financial institution changes its policies or practices regarding disclosure of nonpublic personal information to nonaffiliated third parties, it must provide a new notice that accurately reflects its revised policies and practices, and provide a consumer with a

[94]15 § U.S.C. 6803(a)(1). 16 C.F.R. § 313.6(a)(3). The FTC Rule provides the following as examples that a financial institution can use (if appropriate) to describe categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information: (1) financial service providers, such as mortgage brokers and insurance companies, (2) non-financial companies, such as magazine publishers, retailers, and direct marketers. The disclosure should include a few illustrative examples. *Id.*

[95]15 U.S.C. § 6803(c)(1)(A). 16 C.F.R. §313.6(a)(3). Under this provision, the financial institution does not have to give notice to the consumer regarding disclosure of the information to parties included in the exceptions of 15 U.S.C. § 6802(e), which are discussed below. See fn 63, *supra*, regarding suggested disclosures to nonaffiliated third parties.

[96]15 U.S.C. § 6803(a)(2). 16 C.F.R. § 313.6(a)(4) The FTC staff suggests the following as disclosures that a financial institution can use (if appropriate) to describe disclosures of nonpublic personal information it makes about former customers: (1) categories of nonpublic personal information disclosed and (2) categories of affiliates and nonaffiliated third persons to which such information is disclosed. FTC Staff Outline at p. 8.

[97]16 C.F.R. § 313.6(a)(6).

[98]15 U.S.C. § 6803(c)(3).

[99]15 U.S.C. § 6803(c)(4). 16 C.F.R. §313.6(a)(7). The Fair Credit Reporting Act requirements referred to are at 15 U.S.C. § 1681a (d)(2)(A)(iii).

[100]The disclosure need not include technical information regarding these measures. 16 C.F.R. § 313.6(a)(8).

new opt out notice and a new opportunity to opt out, including reasonable means to exercise the opt out right[101].

The simplified notice that the financial institution must provide if it does not share nonpublic personal information with nonaffiliated third parties during or after the customer relationship[102] should contain a list of the categories of nonpublic personal information collected, a statement that the financial institution does not share the information with affiliates and nonaffiliated parties and a statement of the institution's policies and practices with respect to safeguarding nonpublic personal information[103].

The Federal Trade Commission also requires that a provider that discloses nonpublic personal information to a nonaffiliated third person service provider or joint marketing partner must make a separate statement of the categories of nonpublic personal information disclosed (including illustrative examples). It also states that this separate notice must disclose whether the third party is a service provider that performs services on behalf of the financial institution itself, on behalf of products or services jointly marketed between two financial institutions or is another financial institution with whom the financial institution has entered into a joint marketing agreement[104].

C. Short Form Initial Disclosure and Opt Out Notice to Consumers Who Are Not Customers

The short form disclosure notice that can be provided to a service provider's consumers who are not its customers prior to sharing information about them must state that the provider's full privacy policy and practices disclosure is available on request. And it must identify a reasonable means by which the consumer may obtain the full notice, for example, a toll-free number or that one may be obtained on-site during in-person transactions[105].

Delivery of short form notices is subject to the same requirements as delivery of other notices, as discussed below.

D. Opt Out Notices and the Right to Opt Out

A consumer is entitled to a notice of his or her right to direct the financial services provider not to disclose nonpublic personal information to nonaffiliated third parties, as well as an explanation of how the consumer can exercise the option not to have the information disclosed[106].

---

[101]16 C.F.R. § 313.8.(a). FTC Staff Outline p. 10. Exceptions to the obligation to provide notice and opt out that apply to the original consumer rights also apply to these revised circumstances. See fn 71-73, below.
[102]See fn 59, *supra.* FTC Staff Outline p. 10.
[103]FTC Staff Outline p. 10.
[104]FTC Staff Outline pp. 8-9.
[105]FTC Staff Outline pp. 9-10.
[106]15 U.S.C. § 6802(b)(1). There is an exception to this non-sharing rule. A financial institution may share the nonpublic personal information with a nonaffiliated third party in order to have that party perform services for or functions on behalf of the financial institution, if the institution discloses to the consumer the

The opt out notice must include:

- A statement of the fact that the provider discloses or reserves the right to disclose nonpublic personal information about a consumer to nonaffiliated third parties, including a statement of the categories of such information that may be disclosed and a description of all the categories of nonaffiliated third parties to which disclosure may be made;

- A statement of the right of the consumer to opt out of these disclosures and a description of all the financial products or services the consumer obtains from the institution regarding which the opt out right applies; and

- A description of a reasonable means by which the consumer can opt out.

The reasonable means could be a toll-free phone number; a detachable mail-in form; check-off boxes on the opt out right disclosure form, if on a reply form that includes a return address; or, if the consumer has agreed to receive notices electronically, an electronic means such as a form to be returned by e-mail or via the provider's website[107].

A consumer may exercise the opt out right at any time[108]. The opt out decision remains effective unless and until the consumer revokes it in writing, or until the consumer agrees otherwise electronically[109]. The provider must comply with the consumer's opt out direction as soon as reasonably practical after it is received[110]. When a customer relationship is terminated, the opt out decision continues in effect with regard to nonpublic personal information the provider has collected during or related to that relationship. But it does not apply to any new relationship the customer may establish with the provider[111]. The customer who does enter into a new "covered" relationship with the institution must be given a new opt out notice and the right and means to exercise it. Information obtained in connection with that new relationship is protected from unauthorized sharing unless and until the customer exercises the new opt out right by electing not to opt out.

---

sharing of the information *and* requires the third party by contract to maintain the confidentiality of the information. The services, in such circumstances, may include marketing of the financial institution's products or services or of products or services jointly offered by the institution and one or more other financial institutions. 15 U.S.C. § 6802(b)(2)

[107]16 C.F.R. § 313.7(a)-(b). The FTC advises that it is *not* reasonable to require the consumer to write a letter to the financial institution as the only option for opting out.16 C.F.R. §313.7(a)(2)(ii)(D)(iii). FTC Staff Outline p. 9.

[108]16 C.F.R. § 313.7(f).

[109]16 C.F.R. § 313.7(g).

[110]16 C.F.R. § 313.7(e)

[111]16 C.F.R. § 313.7(g)(2).

A customer is entitled to a new privacy notice and a new opt out notice and right to opt out each time the provider changes its privacy policy or practices[112].

If the provider has permissibly delayed providing the opt out form under any of the exceptions, discussed above, then when providing the opt out form it must also provide a copy of the initial privacy notice in a form permissible under the Agency rules[113].

There are specific rules governing consumer opt out notice rights when there are two or more consumers who jointly obtain a financial product or service from a financial services provider. Disclosure to either (or any one) of the joint consumers meets the provider's opt out disclosure obligations, unless one or more of the others has requested a separate disclosure. Any one of the joint consumers may request an opt out. The institution has options when one of them does so. The institution may either treat an opt out direction by one as applying to both (or all) or it may permit each individual to opt out separately. The opt out notice must include a statement of how the institution will treat an opt out direction by one. If the provider's policy is to permit each joint consumer to opt out separately, it has a further policy option. It may treat an opt out by one as an opt out by all. Or, it may permit each individual to opt out separate (requiring exercise of the opt out right to be taken by each in order for the opt out to cover more than the original requester). If it permits each joint consumer to opt out separately, it is required to permit any one of the joint consumers to opt out on behalf of all. But nothing in this rule *requires* the institution to treat an opt out by one as an opt out by all, unless an opt out on behalf of all is requested. The institution *may not* require that all opt out separately before it implements any one opt out direction[114].

E. Delivery of Required Consumer Notices

A provider may deliver the notice to the customer within a reasonable time *after* the establishment of the customer relationship *if* establishing the customer relationship is not at the customer's election (such as when the servicing rights to the loan is sold by the provider that holds it to another financial institution) or when the customer requests delay in delivery of the notice in order to avoid substantial delay of the transaction[115]. Delivery may not be delayed if the loan transaction takes place in person at the provider's office or on its website[116].

The delivery of the required notices must be such that the consumer or customer is reasonably expected to receive actual notice in writing or, if the customer agrees, electronically[117]. Examples that the FTC considers to meet this requirement include:

- Hand delivery;

[112]16 C.F.R. § 313.8.
[113]16 C.F.R. § 313.7(c). See fn. 88, *supra.*
[114]16 C.F.R. § 313.7(d).
[115]16 C.F.R. § 313.4(e).
[116]16 C.F.R. § 313.4(e)(iii).
[117]16 C.F.R. § 313.9(a).

- Mail delivery to last known address;

- For a consumer who uses an ATM, posting of the notice on the screen and requiring acknowledgement of receipt of the notice as a necessary part of the transaction;

- For a consumer who conducts transactions electronically, posting the notice on the website and requiring acknowledgement of notice as a necessary part of the transaction;

- For a consumer who uses a website for electronic financial transactions and agrees to receive an annual notice at that website, post the current privacy notice in a clear and conspicuous manner on that website[118].

The notice cannot be posted only in a branch office or only on a website[119]. And customers must be provided notice in a form that can be retained or accessed at a later time[120].

The annual notice (only) may be reasonably be assumed to be delivered on the provider's website to a customer who uses that website to access financial products and services electronically and agrees to receive notices posted at the website by that provider, in a clear and conspicuous manner[121]. The provider may elect not to provide the annual notice if the customer has requested not to receive any information regarding the customer relationship, so long as the notice remains available at the customer's request[122]. Certified Public Accountants are exempt from the requirement to provide customers with an annual notice[123].

F. Exceptions

There are several exceptions to the consumer right to receive initial notices and to opt out. (However, to take advantage of these opt out exceptions, the financial services provider must deliver the initial privacy policy and practices notice to a customer and enter into a contract with the third party or parties to prohibit disclosure or use of the information other than for the purpose for which it was disclosed[124].) A provider must give notice but not the right to opt out with regard to its sharing of nonpublic personal information with a third party service provider that provides services on the consumer's account on behalf of the provider . The same exception applies when a provider gives

[118]16 C.F.R. § 313.9(b).
[119]Website only posting will not provide notices to consumers who do not obtain financial products or services electronically. 16 C.F.R. §313.9(b)(2)(ii).
[120]16 C.F.R. §313.9(b)(2). FTC Staff Outline pp. 10-11.
[121]16 C.F.R. § 313.9(c)(1).
[122]16 C.F.R. § 313.9(c)(2).
[123]15 U.S.C. § 6803(d).
[124]See FTC Staff Outline at pp. 11-12.

nonpublic personal information to one or more other financial institutions with which the provider has entered into a joint marketing agreement[125].

There are also situations that are exceptions from both the right to notice and the right to opt out. The consumer can direct the institution to disclose the information without the provision of notice and the right to opt out and can consent to do so at the institution's request as well as on his or her own accord[126]. And the provider may disclose such nonpublic personal information as is necessary to perform a transaction requested by the consumer[127], or in connection with servicing or processing a financial product or service requested or authorized by the consumer, in connection with maintaining or servicing the consumer's account, or in connection with a proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction with the consumer[128].

A provider may also disclose nonpublic personal information pertaining to a customer without regard to the notice and opt out requirements for any of these purposes:

- In order to protect the confidentiality or security of the institution's records pertaining to the consumer, the service or product provided to the consumer, or the underlying transaction, when disclosing the customer's account number [129];

- To protect the confidentiality or security of the institution's records pertaining to the consumer service, products or transaction[130];

- To protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability[131];

- If required to control the institution's risk or to resolve customer disputes or inquiries[132].

- To persons holding a legal or beneficial interest relating to the consumer[133] or who are acting on behalf of the consumer in a fiduciary or representative capacity[134].

There are exceptions, as well, for provision of nonpublic personal information to insurance rate advisory organizations; to guaranty funds or agencies; to agencies that

[125]16 C.F.R. § 313.14(a)(1).
[126]15 U.S.C. § 6802(e)(2). 16 C.F.R. § 313.15(a)(1).
[127]15 U.S.C. § 6802(e)(1); 16 C.F.R. § 313.13(a)(3).
[128]15 U.S.C. § 6802(e)(1)(A)-(C).
[129]15 U.S.C. § 6802(3)(A). 16 C.F.R. § 313.15(a)(2)(i).
[130]16 C.F.R. § 313.13(a)(2)(i).
[131]15 U.S.C. § 6802(3)(B). 16 C.F.R. § 313.13(a)(2)(ii).
[132]15 U.S.C. § 6802(3)(C).16 C.F.R. § 313.13(a)(2)(iii).
[133]15 U.S.C. § 6802(3)(D). 16 C.F.R. § 313.13(a)(2)(iv).
[134]15 U.S.C. § 6802(3)(E). 16 C.F.R. § 313.13(a)(2)(v).

rate the financial institution; to persons assessing that institution's compliance with industry standards; and to the institution's attorneys, accountants, and auditors[135].

And, finally, there is an exemption for disclosure of nonpublic personal information, to the extent specifically permitted or required under other laws, to law enforcement agencies (including a federal functional regulator, appropriate officials of the Treasury Department, a state insurance authority or the Federal Trade Commission)[136]; to self-regulatory organizations (for an investigation of a matter related to public safety); to a consumer credit reporting agency (in accordance with the Fair Credit Reporting Act)[137]; and to comply with laws, properly authorized investigations, subpoenas or summonses by legal authorities having jurisdiction over the financial service provider for examination, compliance or other purposes[138].

G. Restrictions on Reuse and Redisclosure of Information

Unaffiliated third parties receiving nonpublic personal information about a consumer in accordance with these sharing provisions may not reuse or redisclose the information by disclosing it to a another third party unless that party is affiliated with either itself or the original financial services provider[139].

VIII. Nondisclosure of a Consumer's Account Number and Use of Financial Information for Marketing Purposes

There are two consumer protections regarding the sharing of nonpublic personal financial information for marketing purposes. One applies to financial institution's sharing information with *nonaffiliated* third parties. The other applies to sharing it with *affiliates*.

A. Sharing Account Numbers With Nonaffiliated Third Parties

As previously stated, Gramm-Leach-Bliley generally forbids a financial institution to disclose a consumer's account number to a nonaffiliated third party for marketing purposes, whether for telemarketing, direct mail marketing or other marketing through electronic mail[140]. This prohibition applies to the numbers of credit card accounts, bank accounts and transaction accounts. A "transaction account" is an account to which a third party can initiate charges[141], such as a Visa, Mastercard or American Express card account. There are four exceptions to this prohibition:

---

[135]15 § U.S.C. 6802(4).
[136]16 C.F.R. § 313.13(a)(4).
[137]15 U.S.C. § 1681 *et seq.* § 313.13(a)(5).
[138]15 U.S.C. 6802(4)-(8).16 C.F.R. § 313.13(a)(7). See also, FTC Staff Outline at pp. 11-12.
[139]15 U.S.C. § 6802(c). 16 C.F.R. § 313.11. This prohibition includes direct disclose and disclosure through an affiliate of the "receiving" third party. The receiving party may share the information with another third party, however, if the financial institution could have done so lawfully. FTC Staff Guideline pp. 12-13.
[140]15 U.S.C. § 6802(d). This marketing restriction seems to apply regardless of whether the nonaffiliated third party may disclose the account number or access code for purposes that require it, such as billing, account servicing or account collection. 16 C.F.R. §313.12. FTC Staff Outline pp. 13-14.
[141]16 C.F.R. § 313.12(c)(2). FTC Staff Outline p. 13.

- Disclosure to a consumer reporting agency[142];

- Disclosure to an agent or service provider to perform marketing of the financial institution's own products or services, provided that the agent or service provider is not authorized to directly initiate charges to the account;

- Disclosure to a participant in a private label credit card program or an affinity program where the participants are identified to the consumer at the time the customer enters into the program; and

- Disclosure of an encrypted account number to a nonaffiliated third party, provided that the financial institution does not give the third party the means to decode the number or code[143].

B. Consumer Information Sharing with Affiliates for Marketing Solicitation Purposes

In addition to the GLB restrictions on the sharing of account numbers with *nonaffiliated* third parties for marketing purposes, there are also restrictions on the use of a much broader range of information contained in a consumer credit report[144], if shared by a financial services provider with an *affiliate* for marketing purposes, unless the consumer receives, as a part of the marketing solicitation, the opportunity to opt out of having the shared information used this way. This restriction is contained not in Gramm-Leach-Bliley, but in Section 624 of the Fair Credit Reporting Act[145]. The FTC implementing Rule[146] became enforceable October 1, 2008[147].

---

[142]16 C.F.R. § 313.12(a).
[143]15 U.S.C. § 6802((d). 16 C.F.R. §313(b). FTC Staff Outline pp. 13-14.
[144]According to the National Consumer Law Center, the information shared in the absence of a consumer opt out could include much information "bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living… . This could include your name, address, Social Security number, employer, date of birth, credit score, what types of credit accounts you have, your payment record on this accounts (such as your history of making late payments), your credit limits and amount of credit you have used. Even information not typically found on your credit report could be shared, such as where you have used your credit card, your income, your assets or the value of your home or car." See "4 Ways to Opt Out of Credit Card Affiliate Marketing," Mueller, article at CreditCards.com, http://www.creditcards.com/credit-card-news/4-tips-opt-out-affiliate-marketing-1282.php, viewed December 1, 2008.
[145]The "sharing with affiliates" opt out requirement was added through a provision of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. 108-159, 117 Stat. 1952, 15 U.S.C. § 1681s-3, which became law on December 4, 2003.
[146]16 C.F.R. § 624.1 - 624.4, reproduced at http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr;sid=b7b8994e702c077c148934f5b4545be0;rgn=div5;view=text;node=16%3A1.0.1.6.69;idno=16;cc=ecfr, viewed December 1, 2008. The Federal Reserve System has a parallel Rule for federally regulated financial institutions that are subject to the Fair Credit Reporting Act.
[147]16 C.F.R. § 680.28.

The Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Comptroller of the Currency, the Office of Thrift Supervision, and the Federal Deposit Insurance Corporation adopted this rule jointly with the FTC with respect to the financial institutions that each of them regulate[148].

The FTC Rule provides the following example, which best illustrates how the Rule's restrictions on affiliate sharing work:

> *A consumer has a homeowner's insurance policy with an insurance company. The insurance company furnishes eligibility information about the consumer to its affiliated creditor. Based on that eligibility information, the creditor wants to make a solicitation to the consumer about its home equity loan products. The creditor does not have a pre-existing business relationship with the consumer and none of the other exceptions apply. The creditor is prohibited from using eligibility information received from its insurance affiliate to make solicitations to the consumer about its home equity loan products unless the consumer is given a notice and opportunity to opt out and the consumer does not opt out.*[149]

In these and similar circumstances, the consumer is entitled to a statement consisting of a short notice and a long notice. The statement is *not* a prerequisite to the solicitation. Instead, unlike the GLB opt out notice (regarding sharing with nonaffiliated parties), it must accompany and be a part of each written solicitation[150].

The *short notice* must state that the consumer has the right to opt out of receiving "prescreened" solicitations. It must also describe a "reasonable and simple method for the consumer to opt out." It must provide a toll-free number the consumer can call to exercise that right. The short notice must be in the same language as the services offered (for example, if the offer is in Spanish, the short notice must be in Spanish). It also must direct the consumer to the existence and location of the long notice, and must state the heading for the long notice. The short notice must not contain any other information than that required by the Rule. And, the Rule has print size and format requirements intended to make the short notice "clear and conspicuous, and simple and easy to understand."

The long notice must provide the information required by the Fair Credit Reporting Act about the consumer's marketing solicitation opt out rights under that Act[151] and it *must* begin with the heading "PRESCREEN&OPT-OUT NOTICE"[152]. The required disclosures are:

---

[148] 12 C.F.R. Parts 41, 222, 334, 571 and 717). See also for a concise summary of the Rule, "Affiliate Marketing Rule Alert: Compliance Deadline Is October 1, 2008," Privacy Law Blog, Proskauer Rose LLP, http://privacylaw.proskauer.com/2008/09/articles/direct-marketing/affiliate-marketing-rule-alert-compliance-deadline-is-october-1-2008/, viewed December 2, 2008.
[149] 16 C.F.R. § 680.21(a)(2).
[150] 16 C.F.R. § 642.3.
[151] 15 U.S.C. § 1681m(d) . See 16 C.F.R. § 643.2(b)(1).
[152] 16 C.F.R. § 642.3(b)(2)(iii).

- That information contained in the consumer's consumer credit report (that is, the information used to pre-screen the solicitation to the consumer) was used in connection with the transaction;

- That the consumer received the offer of credit or insurance because the consumer satisfied the criteria for credit worthiness or insurability under which the consumer was selected for the offer;

- If applicable, that the credit or insurance may not be extended if, after the consumer responds to the offer, the consumer does not meet the criteria used to select the consumer for the offer or any applicable criteria bearing on credit worthiness or insurability or does not furnish any required collateral;

- That the consumer has a right to prohibit information contained in the consumer's file with any consumer reporting agency from being used in connection with any credit or insurance transaction that is not initiated by the consumer; and

- That the consumer may exercise this right of prohibition by notifying a notification system established under the FCRA to opt out of having his or her credit reports used for prescreening purposes.

There are also requirements regarding the format of the long notice that are intended to make it easily readable and easily distinguished from the written solicitation itself. The long and short notices must be appear in the solicitation. (This avoids the situation where the consumer disposes of the notices before reading the solicitation.)

There are requirements for the delivery of the required opt out notice similar to the requirements in the GLB Rule. These include provisions for hand delivery, mail delivery, e-mail delivery (where the consumer uses electronic means to access the written offer), and Internet website posting (on a Website where the consumer accesses the solicitation)[153].

There are certain exceptions to this notice and opt out requirement, the most important of which is that a financial services provider may send solicitations to a consumer without the notice and right to opt out *if* that provider has a pre-existing business relationship with that consumer[154].

Generally, if the consumer exercises to opt out, that decision is effective for at least five years (but the provider may offer a longer opt out effective period, or even allow an opt out without a termination date). The consumer may revoke the opt out at any point after exercising it. In addition, the consumer is entitled to renew the opt out at the end of any opt out period[155].

---

[153] 16 C.F.R. § 680.26.
[154] 16 C.F.R. § 680.21(c).
[155] 15 U.S.C. §1681 *et seq*. 16 C.F.R. § 680.22(b) ; 16 C.F.R. § 680.22(b), 680.27.

The Marketing Solicitation Rule's requirements are stated in terms of a business affiliate that uses the consumer information, not in terms of a business affiliate that provides the information to another. Therefore, liability for any violations would usually lie with the affiliate making the marketing solicitation if the Rule's requirements are not met.

IX. Nondisclosure by Tax Preparers of a Consumer's Tax-Related Information

Tax returns often contain data that are among a taxpayer's most private financial information. The Internal Revenue Code (IRC) contains a requirement governing the unauthorized use of a taxpayer's tax-related information. It prescribes a criminal penalty for any tax return preparer[156] who knowingly or recklessly makes unauthorized disclosure or use of tax return information for any purpose other than preparing or helping to prepare a tax return[157]. It also establishes civil penalties for violation of this prohibition[158]. However, the IRS continues to take its long-held view that taxpayer information can be shared with a third party by a tax preparer if the taxpayer consents to the sharing.

The plain language of the Internal Revenue Code seems to prohibit sharing. This interpretation would make information in tax returns a matter solely between the taxpayer and the IRS (with the preparer serving only as an intermediary). However, the IRS does not view the law in the same light as do consumer advocates. The IRS Rule to implement a recent change in the law, contrary to arguments advanced by consumer groups during the rulemaking process, continues the pre-amendment IRS sharing policy based on taxpayer consent[159]. The Rule merely tightens the requirements of the consent forms. There are no rules either prohibiting or governing the further use of the information by anyone once it has been transferred to a third party in accordance with the Rule.

---

[156] 26 U.S.C. § 7216(a) "Tax return preparers" include not only those who are regularly engaged in the business of preparing tax returns for others and those who are compensated for helping professional tax return preparers, but also any who is *compensated*, even on a casual basis, for helping a relative, friend or acquaintance to prepare a tax return. 26 C.F.R. § 301(b)(2). This definition of who is a tax preparer is so strict that if a taxpayer purchases tax preparation software and is prompted by the software to register the software with the software provider, the registration information is taxpayer information and the software provider is a tax preparer for purposes of the IRS Rule. 26 C.F.R. § 301.7216-1(b)(3)(D)(ii) Example 1.

[157] 26. U.S.C. § 7216(a). A violation of section 7216 is a misdemeanor, with a maximum penalty of up to one year imprisonment or a fine of not more than $1,000, or both, together with the costs of prosecution.

[158] 26 U.S.C. § 6713. 26 C.F.R. §301. 6713. The civil penalty for violating section 6713 is $250 for each prohibited disclosure or use, not to exceed a total of $10,000 for a calendar year. As a practical matter, the government may choose to seek civil penalties under this provision, rather than criminal penalties, when the evidence that the unlawful use or disclosure was "knowing" or "reckless" (in other words, criminal) is weak.

[159] An IRS tax guidance document implicitly admits the difference between the more absolute language of the statute and the policy of the IRS Rule promulgated by the Secretary of the Treasury. Part III Administrative, Procedural, and Miscellaneous 26 CFR 301.7216-3: "Disclosure or use permitted only with the taxpayer's consent," reproduced at http://www.irs.gov/pub/irs-drop/rp-08-35.pdf, viewed December 14, 2008.

The new IRS Rule[160], as did the old Rule[161], covers tax preparer marketing uses (by the preparer receiving the information from the taxpayer) and disclosure (preparer transfer of information to another party) for marketing purposes of a consumer's tax-related information[162].

The taxpayer information that is protected by the new Rule includes *any* information furnished *in any way* to the tax preparer by the taxpayer or by another person in connection with the preparation of a tax return. It includes even the taxpayer's name and address, as well as the tax identification number[163]. It includes information derived from or generated in the preparation of a tax return. For example, the net income, the total deductions taken by the taxpayer, or the total of taxes owed or paid, which are exactly the kinds of calculations the taxpayer may not know or provide to the preparer but pays the preparer to calculate. It also includes information generated by the Internal Revenue Service (IRS), such as acknowledgement of receipt or notice of rejection of a return filed electronically[164].

The restrictions on disclosure do not apply, of course, to the tax preparer's provision of the information to the IRS[165]. And, there is a significant exception that allows a tax preparer to compile and maintain a separate list containing solely the names, addresses, e-mail addresses, and phone numbers of taxpayers whose tax returns the tax return preparer has prepared or processed. This list may be used by the compiler *solely* to contact the taxpayers on the list for the purpose of offering tax information or additional tax return preparation services to the listed taxpayers. The compiler of the list may not transfer the taxpayer list, or any part thereof, to any other person unless the transfer takes place in conjunction with the sale or other disposition of the compiler's tax return preparation business. A person who acquires a taxpayer list, or a part thereof, in conjunction with a sale or other disposition of a tax return preparation business is subject to the provisions of this paragraph with respect to the list[166]. In short, a taxpayer who uses the services of a tax preparer should not be surprised to receive a solicitation of further business from that preparer. Solicitations from other preparers may come from a list otherwise derived, but may not come from the taxpayer's tax preparer's list.

---

[160]26 C.F.R. § 301.7216-3, reproduced at http://edocket.access.gpo.gov/cfr_2008/aprqtr/26cfr301.7216-3.htm, viewed December 14, 2008. The new Rule is effective January 1, 2009.

[161]The statutory restrictions and IRS rules are much older than the new implementation Rule. The criminal penalties go back to the Revenue Act of 1971, P.L. 92-178 (65 Stat. 529). Previous IRS regulations date back to 1974 (29 Federal Register 11537, March 29, 1974). Both statute and regulations have been amended from time to time.

[162]The Rule goes beyond marketing issues, however. While the Rule discusses marketing use and disclosure of information for marketing purposes in some detail, it applies to *any* use or disclosure, marketing or otherwise, that is not in accordance with the Rule's restrictions.

[163] 26 C.F.R. § 301(b)(3). An identification number typically is the taxpayer's Social Security number, but in the event of a return other than a personal income tax return or quarterly estimated tax filing, for instance a household employer return, could be another number issued by the Internal Revenue Service to a taxpayer.

[164] 26 C.F.R. § 301.7216(b)(3)(A).

[165] 26 C.F.R. § 301.7216-2(b).

[166] 26 C.F.R. §301.7216-2(n).

And, there are other narrow but necessary exceptions[167]. However, unless a disclosure is authorized by one of the exceptions in the Rule, the taxpayer's knowing and voluntary written consent is required for other disclosures or uses of the information. And, with one important exception, the tax preparer may not condition the provision of any services on the taxpayer's furnishing consent for other disclosures or uses. Such a condition would render the consent involuntary, and the consent would not satisfy the requirements of this section of the Rule[168]. The exception is that the preparer *may* condition services upon the taxpayer's consent to disclosure of the tax return information to another tax return preparer for the purpose of performing services that assist in the preparation of, or provide auxiliary services in connection with, the preparation of the tax return[169].

The IRS Rule prescribes the information that must be included in a taxpayer written consent:

- The name of the tax return preparer;
- The name of the taxpayer;
- The intended purpose of disclosure and the particular use authorized;
- The specific recipient or recipients of the information;
- If the tax return preparer intends to use tax return information to generate solicitations for products or services other than tax return preparation, identification of each specific type of product or service for which the tax return preparer may solicit use of the tax return information;
- The information to be disclosed or used;
- If another tax return preparer to whom the tax return information is to be

[167] A tax preparer can furnish the information to another tax preparer who is a officer, employee or member of the same tax preparation firm within the U.S. (If the employee, officer or firm member receiving the information is outside the U.S., knowing written consent is required); to employees, officers or members of another U.S. tax preparation firm that is assisting in preparation of the return, *but only* if the services provided by the second firm are not substantive determinations or advice affecting the tax liability reported by taxpayers; to an attorney for the purposes of obtaining a legal opinion in the process of preparing the return; to the preparer's contractors in connection with the programming, maintenance, repair, testing, or procurement of equipment or software used for purposes of tax return preparation, but only to the extent necessary for the person to provide the contracted services, and only if the tax return preparer ensures that all individuals who are to receive disclosures of tax return information do in fact receive certain required notices (such a contractor becomes a tax preparer for purposes of the Rule and also is subject to the Rule's information disclosure restrictions). A tax preparer who is a practicing attorney may use the tax information to provide the taxpayer with other services such as estate planning, accounting or other legal services. § 301.7216-2(h)(1)(i). And, of course, there are exceptions for disclosure under legal processes in the Courts and Federal agencies. 26 C.F.R. § 301.7216-2.

[168] 26 C.F.R. § 301.7216-3(a)(1).

[169] 26 C.F.R. § 301.7216-3(a)(2). As a tax preparer, the second preparer would be subject to the same disclosure restrictions and notice requirements as the taxpayer's original tax preparation service provider.

disclosed is located outside of the United States, a special IRS consent form must be completed;

- If the information is from or related to a tax return in the Form 1040 series (1040, 1040NR, 1040A, 1040EZ), the IRS may require the consent to be on an IRS-provided form[170].

The form must be signed and dated by the taxpayer[171].

There can be *no* retroactive consent. A taxpayer must provide written consent *before* a tax return preparer discloses or uses the taxpayer's tax return information for purposes other than tax preparation[172]. A tax return preparer may not request a taxpayer's consent to disclose or use tax return information for purposes of solicitation of business unrelated to tax return preparation *after* the tax return preparer provides a completed tax return to the taxpayer for signature[173]. And, with regard to tax return information for each tax return that a tax return preparer prepares, if the taxpayer declines a request for consent to the disclosure or use of tax return information for purposes of solicitation of business unrelated to tax return preparation, the tax return preparer may not repeat the solicitation for consent for a purpose substantially similar to that of the rejected request[174].

If the taxpayer *does* give consent to a preparer's request, the consent document may or may not specify the duration of the taxpayer's consent to the disclosure or use of tax return information. But if it does not, the consent to the disclosure or use of tax return information expires one year from the date the taxpayer signed the consent[175]. The taxpayer must be given a copy of the executed consent form at the time of execution. The preparer may choose to meet this requirement by allowing the taxpayer at the time of executing the form to print the executed consent form or to save it electronically[176].

If the tax preparer requests to disclose the taxpayer's entire tax return, the consent form *must* disclose that the taxpayer has the right to direct a more limited disclosure of the information in the return[177].

Finally, the IRS requires businesses that are authorized to electronically file a taxpayer's tax return to establish and maintain security systems to assure the privacy of taxpayer information[178].

---

[170] 26 C.F.R. § 301.7216-3(a)(3)(E)(ii).
[171] 26 C.F.R. § 301.7216-3(a).
[172] 26 C.F.R. § 301.7216-3(b)(1).
[173] 26 C.F.R. § 301.7216-3(b)(2).
[174] 26 C.F.R. § 301.7216-3(b)(3).
[175] 26 C.F.R. § 301.7216-3(b)(5).
[176] 26 C.F.R. § 301.7216-3(c)(3).
[177] 26 C.F.R. § 301.7216-3(c)(2).
[178] See Internal Revenue Bulletin 2005-35, August 29, 2005, containing Revenue Procedure 2005-60, reproduced at http://www.irs.gov/irb/2005-60_IRB/ar20.html, viewed December 4, 2008.

Because this paper was published less than a year after the effective date of the new IRS Rule, there is no enforcement history at this time under the new Rule. There appears to have been limited enforcement under the old Rule.

X. Standards for Safeguarding Customer Information

A. The Gramm-Leach-Bliley Safeguards Program

The federal agency and state standards under GLB for safeguarding customer information are non-technical. (As indicated below, the application of technology by the institution, however, is a necessity to compliance with these requirements.) Rather than specifying what technologies are to be used and how to use them, the Agency rules establish the required elements for a program that each financial services provider must develop, implement and maintain in order to assure information security.

The program must be in writing and must describe the administrative, technical, and physical safeguards established and maintained by the provider. The program must be appropriate to the size and complexity of the institution, the nature and scope of its activities and the sensitivity of the customer information protected by the program[179]. The program must be reasonably designed to achieve the objectives of the Act and the implementing Agency rule[180], which are to:

- Insure the security and confidentiality of customer information[181];
- Protect against any anticipated threats or hazards to the security or integrity of such information[182]; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the customer[183].

The required six elements of the information security program are:

- Designation of one or more employees to coordinate the program[184];
- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information[185];

[179]The FTC expressed concern that its rules be sensitive to the abilities of smaller and less sophisticated financial institutions. 67 Fed. Register 36484, at col. 3, Thursday, May 23, 2002.
[180]16 C.F.R. § 314.3(a).
[181]16 C.F.R. § 314.3(b)(1).
[182]16 C.F.R. § 314.3(b)(2).
[183]16 C.F.R. § 314.3(b)(3).
[184]16 C.F.R. § 314.4(a).
[185]16 C.F.R. § 314.4(b).

- At a minimum, assessment of the sufficiency of any safeguards in place to control these risks, including the following:
    1. Employee training and management[186];
    2. Information systems including network and software design, information processing, storage, transmission, and disposal[187];
    3. Detecting, preventing and responding to attacks, intrusions or other systems failures[188];

- Designing and implementing information safeguards to control the risks the institution identifies through risk assessment and regularly testing or otherwise monitoring the effectiveness of the safeguard' key controls, systems and procedures[189];

- Overseeing the institution's service providers by:
    1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information protected by the program[190]; and
    2. Requiring service providers, by contractual obligation, to implement and maintain such safeguards[191].

- Evaluating and adjusting the program in light of the results of the required testing and monitoring, any changes in the institution's operations or business arrangements and any other circumstances the institution knows or has reason to know that may have a material impact on its security program[192].

B. The Disposal Rule

There is an additional protection for information pertaining to a consumer contained in or derived from consumer credit reports. Credit reports rank high among the records of nonpublic personal information a financial institution is likely to possess regarding many of its customers. The Federal Trade Commission, Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission require the proper disposal of such information. An institution that is subject to both the FTC Disposal Rule and the Gramm-Leach-Bliley Act should include the measures it takes to meet the Disposal Rule's requirements into its Safeguards program.

---

[186] 16 C.F.R. § 314.4(b)(1).
[187] 16 C.F.R. § 314.4(b)(2).
[188] 16 C.F.R. § 314.4(b)(3).
[189] 16 C.F.R. § 314.4(c).
[190] 16 C.F.R. § 314.4(d)(1).
[191] 16 C.F.R. § 314.4(d)(2).
[192] 16 C.F.R. § 314.4(e).

The Disposal Rule, like the Safeguards Rule, is flexible and allows the provider leeway to adopt appropriate technology to assure proper disposal of information covered by the Rule[193]. Appropriate means for complying with the Disposal Rule include the following actions:

- Burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;

- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;

- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include:

    - reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule;
    - obtaining information about the disposal company from several references;
    - requiring that the disposal company be certified by a recognized trade association;
    - reviewing and evaluating the disposal company's information security policies or procedures[194].

C. The Red Flag Rule

Additional protection of nonpublic personal information was recently established. The federal GLB enforcement agencies (except for the CFTC) require financial institutions to have a "Red Flag" program that identifies and responds to signals that a consumer may have been the victim of identity theft[195]. The rules are required under the Fair and Accurate Credit Transactions Act (FACTA), which made several improvements to the Fair Credit Reporting Act. The rules also require credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances[196].

---

[193] 16 C.F.R. Part 682. The Disposal Rule is based on requirements of the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act. See "FACTA Disposal Rule Goes Into Effect June 1," FTC press release, June 1, 2005, reproduced at http://www.ftc.gov/opa/2005/06/disposal.shtm, viewed November 15, 2008. The Rule is broader than GLB, however. It even applies, for example, to individuals who acquire a consumer report in the process of hiring a nanny or a home improvement contractor. The Rule is reproduced online at www.ftc.gov/os/2004/11/041118disposalfrn.pdf, viewed November 25, 2008.

[194] *Id.*

[195] 16 C.F.R. Part 681 (Federal Trade Commission); 12 C.F.R. part 41, (Office of the Comptroller of the Currency); 12 C.F.R. Part 222 (Federal Reserve System); 12 C.F.R. parts 334 and 364 (Federal Deposit Insurance Corporation); 12 C.F.R. Part 571 (Office of Thrift Supervision); 12 C.F.R. Part 717 (National Credit Union Administration). The Red Flag Rule has been adopted pursuant to Section 114 of the Fair and Accurate Transactions Act of 2003 (FACT).

[196] *Ibid*, p. 63718.

These rules went into effect November 1, 2008, with respect to the federal enforcement Agencies, except for the Commodity Futures Trading Commission (which has no Red Flag Rule) and the Federal Trade Commission. Enforcement of the FTC Rule is scheduled to go into effect November 1, 2009 with respect to financial services providers under the Federal Trade Commission's enforcement jurisdiction[197]. The FTC's delay in the effective date of its Rule gives financial services providers under its jurisdiction more time to comply, but also extends the period of consumer risk the Rule is meant to reduce with respect to those providers most likely to expose consumers to risk.

Only certain customer accounts, however, are covered by the Red Flag Rule. A "covered account" is:

- One that is primarily for personal, family, or household purposes and that involves or is designed to permit multiple payments or transactions; or

- Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft[198].

Any account that does not meet this definition is not covered by the Red Flag Rule, even if it is otherwise subject to the requirements of Gramm-Leach-Bliley.

The Rule provides that the financial services provider's Red Flag Program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. There are four basic elements that a Red Flag Program must meet; it must have reasonable procedures to:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;

- Detect Red Flags that have been incorporated into the Program;

- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and

- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft[199].

As is the case with the GLB Safeguards Program requirements, the Rule is flexible and permits each provider to design a Red Flag Program appropriate to its size and complexity.

---

[197]See "FTC Announced Expanded Business Education Campaign on "Red Flag' Rules," FTC press release July 29, 2009, reproduced at http://www.ftc.gov/opa/2009/07/redflag.shtm, viewed September 1, 2009.
[198] 72 Federal Register No. 217, November 9, 2007, p. 63719.
[199]*Ibid*, p. 63720.

D. State Security Breach Notification Requirements

Some state laws address customer notification requirements that go into effect when safeguard systems fail. Forty-six states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have laws requiring a financial institution to notify customers under certain circumstances when their data has been breached[200]. These laws are discussed in Section XIV below.

XI. Pretexting

Gramm-Leach-Bliley prohibits "pretexting," which is the practice of obtaining customer information possessed by a financial services provider relating to a person (other than the requesting party) by:

- Making a false, fictitious or fraudulent statement or representation to an officer, employee or agent of a provider;
- Making such a statement to a customer of a provider;
- Submitting to a provider a document, knowing that the document is forged, counterfeit, lost, stolen, was fraudulently obtained or contains a false, fictitious or fraudulent statement or representation[201].

There is an important exception to the pretexting rule that applies when a state-licensed private investigator, acting under a valid court order, seeks information necessary to collect child support from the subject of the inquiry[202].

Gramm-Leach-Bliley includes criminal penalties for knowing and intentional pretexting violations[203], so the U.S. Department of Justice may also enforce these provisions, and the FTC refers appropriate cases to the Department[204]. Violations of the pretexting

---

[200]See http://www.crowell.com/PDF/SecurityBreachTable.pdf, viewed November 15, 2008. See also, "Safeguard Your Company Against a Data Breach," Dovell Bennett, e-published at http://www.articlesbase.com/technology-articles/safeguard-your-company-against-a-data-breach-516720.html, viewed November 15, 2008.

[201]15 U.S.C. § 6821(a). This rule does not apply under certain circumstances, such as when the financial institution is testing its customer information security system, or when it is investigating misconduct or negligence on the part of its own employees, 15 U.S.C. § 6821(d), or when an insurance financial institution is investigating criminal activity, insurance fraud or insurance misrepresentation 15 U.S.C. § 6821 (e).

[202]15 U.S.C. § 6821(g).

[203]Criminal pretexting violations bear heavy penalties. A prison sentence of up to five years and fines under the criminal code can be imposed for knowing and intentional violations. Up to 10 years and a double fine can be imposed for violations committed while violating another federal law or as part of a pattern of illegal activity involving more than petty gains. 15 U.S.C. § 6823.

[204]See U.S. v. Peter Easton, No. 05 CR 0797 (S.D.N.Y), final judgment entered November 17, 2005, cited in Prepared Statement of the Federal Trade Commission before the Committee on Energy and Commerce, U.S. House of Representatives, "Why Aren't Phone Records Safe From Pretexting?," February 1, 2006, reproduced at http://www.ftc.gov/os/2006/02/commissiontestimonypretexting.pdf.

provisions also constitute violations of the Federal Trade Commission Act's ban on unfair and deceptive practices[205].

XII. Private Institutional Rules

Gramm-Leach-Bliley recognizes private institutional rules as a means of achieving and demonstrating compliance with the Act's requirements. A number of financial services providers that cumulatively engage in a very large number of consumer transactions utilize the rules, guidelines, and network facilities of the National Automated Clearinghouse[206] to manage their transactions. These include online payday lenders, whose payments and collections occur online by EFT into and out of borrowers' bank accounts. Some stores also extend credit using debit authorization to borrowers' bank accounts. These rules include the following measures related to safeguards for consumer transactions:

- Transmission of ACH Information Via Unsecured Electronic Networks: Any banking information, including, but not limited to, an Entry, Entry Data, a routing number, an account number, and a PIN or other identification symbol, that is transmitted or exchanged between [commercial parties subject to network rules] via an Unsecured Electronic Network, must prior to the key-entry and through transmission of any banking information, (1) be encrypted using a commercially reasonable security technology that, at a minimum, is equivalent to 128-bit RC4 encryption technology, or (2) be transmitted via a secure session utilizing a commercially reasonable security technology that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology. (There is an exception for non-Internet telephone transmittals of data[207].)

- Origination of Entries: For each entry for which any banking information, including, but not limited to, an Entry, Entry Data, a routing number, an account number, and a PIN or other identification symbol is transmitted or exchanged between [commercial parties subject to network rules] via an Unsecured Electronic Network, the Originator has, prior to the key entry and through transmission of any banking information, (1) encrypted the banking information using a commercially reasonable security technology that, at a minimum, is equivalent to 128-bit RC4 encryption, or (2) transmitted or received the banking information via a secure session using a commercially reasonable security technology that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology[208].

---

[205]15 U.S.C. § 45(a) by reference to an identical provision in the Fair Credit Reporting Act, 15 U.S.C. § 1692 *et. seq*.

[206]2007 ACH Rules: A Complete Guide to Rules & Regulations Governing the ACH Network, National Automated Clearing House Association, Herndon, VA 2007

[207]Ibid, ARTICLE ONE, Section 1.6.

[208]Ibid, ARTICLE TWO, Section 2.2.1.6.

- Obligations of Originators: For each entry for which any banking information, including, but not limited to, an Entry, Entry Data, a routing number, an account number, and a PIN or other identification symbol is transmitted or exchanged between [commercial parties subject to network rules] via an Unsecured Electronic Network, the Originator has, prior to the key entry and through transmission of any banking information, (1) encrypted the banking information using a commercially reasonable security technology that, at a minimum, is equivalent to 128-bit RC4 encryption, or (2) transmitted or received the banking information via a secure session using a commercially reasonable security technology that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology. (There is an exception for non-Internet telephone transmittals of data[209].)

XIII. Enforcement Actions under Gramm-Leach-Bliley

Laws and regulations are only as good as their enforcement. Here is a look at representative major enforcement work by the federal Agencies charged with implementing the Gramm-Leach-Bliley Act. Most of the enforcement actions have been taken by the Federal Trade Commission. This is as expected, since the FTC has jurisdiction over the least regulated sector of financial services providers, the one most likely to include "bad actors."

A. Federal Trade Commission.

The Federal Trade Commission enforces GLB with regard to the broadest spectrum of financial services providers, including those likely to have the most contact with low-income consumers. It is not surprising, therefore, that the FTC has taken more enforcement actions under GLB than the other GLB enforcement agencies.

1. Failure to Provide Notice, Inaccurate Description of Privacy Policy and Practices, Unauthorized Disclosure and Unauthorized Use of Nonpublic Personal Information.

It should be noted that the FTC's power to ban the practice of *undisclosed* sharing of consumer information did not originate with the GLB Act. In 1972, long before GLB was enacted, the FTC issued a consent order against H&R Block, the well-known tax preparer, for utilizing information given to it by customers for the purpose of preparing their tax returns, for other, undisclosed purposes as well. The FTC alleged this practice to be deceptive in violation of Section 5 of the Federal Trade Commission Act[210]. However, the GLB sharing restrictions are broader and more specific than those imposed by the FTC; under GLB, financial services providers are under greater restrictions on sharing than they are under the FTC Act.

In January 2003, the FTC filed a complaint in U.S. District court charging that 30 Minute Mortgage, Inc., sent spam e-mails and maintained web sites where it advertised "3.95%

[209]Ibid, ARTICLE THREE, Section 3.3.
[210]*H&R Block, Inc.*, 80 F.T.C. 304 (1972) (consent), *modified,* 100 F.T.C. 523 (1982)

30 Year Mortgages" and described itself as a "national mortgage lender." The FTC charged that in the e-mails and on the website the company urged potential customers to complete detailed online loan applications that included such information as Social Security numbers, income, and assets. The company assured consumers that their sensitive information would be protected because it would be transmitted using Secure Sockets Layer (SSL) technology. The FTC alleged that 30 Minute Mortgage was not a "national mortgage lender" and did not offer 3.95% 30 year loans. Instead, the company allegedly sold or offered to sell thousands of completed applications to nonaffiliated third parties without consumers' consent. The FTC also alleged that consumers' sensitive personal and financial information was not protected in transmission because the web sites at times did not use SSL or other encryption technology[211].

In 2004, the Federal Trade Commission obtained an order from the U.S. District Court for the District of Colorado, enjoining Sainz Enterprises, LLC, a Colorado telemarketer of bank credit cards, from further failure to meet the GLB notice requirements, providing nonpublic personal information obtained from telemarketing targets to unauthorized nonaffiliated third parties and reusing or redisclosing such information in a manner that violates the Act[212].

In 2004, the FTC in Federal District Court charged a California business, that claimed to provide consumers with debt relief services, with Gramm-Leach-Bliley violations, as well as with violating the FTC's Do Not Call Rule and making numerous unlawful misrepresentations. The GLB violations involved a failure to inform consumers how their personal financial information would be used. The company misrepresented itself as a nonprofit organization, when in fact it simply generated leads for the other participants in the scheme, who then charged consumers thousands of dollars in fees to enroll in their debt negotiation programs. The defendants deceptively claimed these programs were an effective way to stop creditors' collection efforts and eliminate consumers' debts. The FTC alleged that the defendants failed to disclose important information to consumers before they enrolled, including the fact that very few people were able to reduce their debts through the debt negotiation programs; that consumers would suffer late fees, penalties, and other charges; and that participation in the program might actually hurt their credit rating. The Agency's actions not only closed down the businesses involved in the scheme, but resulted in more than $24 million in restitution to consumers who were harmed by the scheme[213].

---

[211]The case was filed in the U.S. District Court for the Southern District of Florida. The court entered stipulated final judgments. The court entered the default judgment against 30 Minute Mortgage on December 2, 2003. Final default judgment and order for permanent judgment reproduced at http://www.ftc.gov/os/2003/12/031126finalstolz.pdf, viewed October 15, 2008. See "Internet Mortgage Scam Halted," Federal Trade Commission press release, reproduced at http://www.ftc.gov/opa/2003/12/30mm2.shtm, viewed October 14, 2008.

[212]Court order reproduced at http://www.ftc.gov/os/caselist/0323180/041015stip0323180.pdf, viewed October 13, 2008.

[213]Federal Trade Commission v. National Consumer Council, *et al.*, U.S. District Court for the Central Division of California, Southern Division, Case No. SA CV-040474 CJC (JWJx), settlement agreement and proposed final order for injunction reproduced at

In 2005, the FTC obtained a final order in Federal District Court enjoining Debt Management Foundation Services and other defendants from failing to provide each future customer with a clear, conspicuous, and accurate notice of its privacy practices[214].

In 2008, the FTC obtained a consent order from Premier Capital Lending, Inc., a Texas lender, in which the company agreed to cease and desist from failing to accurately represent to consumers its privacy policy and practices[215]; it also agreed to comply with the Safeguards Rule (see below).

2. Safeguarding the Security of Customer Information.

In all, as of 2007 the FTC had brought fourteen compliance actions against financial services providers that failed to meet the Gramm-Leach-Bliley Act, Fair Credit Reporting Act and Federal Trade Commission Act requirements for securing consumer information. The Commission also declined to bring actions against companies that experienced security breaches despite having reasonable safeguards programs in place[216].

In 2004, Nationwide Mortgage Group, Inc. and Sunbelt Lending Services, Inc. were the first companies charged by the FTC with violating the Safeguards Rule's requirements. The agency charged that both companies "failed to comply with the Rule's basic requirements, including that they assess the risks to sensitive customer information and implement safeguards to control these risks." "In addition, Nationwide failed to train its employees on information security issues; oversee its loan officers' handling of customer information; and monitor its computer network for vulnerabilities," the FTC stated. The FTC said, "Sunbelt also failed to oversee the security practices of its service providers and of its loan officers working from remote locations throughout the state of Florida." The FTC did note in its announcement of the charges that many other mortgage and auto financing companies included in its compliance survey were in compliance with the safeguard rules[217].

---

http://www.ftc.gov/os/caselist/0323185/050330receivership0323185.pdf, viewed October 14, 2008. See also, "Debt Services Operations Settle FTC Charges," FTC press release, March 30, 2005, reproduced at http://www.ftc.gov/opa/2005/03/creditcouncel.shtm, viewed October 14, 2008.

[214]Federal Trade Commission v. Debt Management Foundation services *et al.,* (Middle District of Florida, Tampa Division), Civ. No. 8:04-cv-01674-EAK-MSS, stipulated final judgment and order reproduced at http://www.ftc.gov/os/caselist/0423029/050330sstip0423029.pdf, viewed October 14, 2005.

[215]Federal Trade Commission Docket C-4216. Decision and Order reproduced at http://www.ftc.gov/os/caselist/0723013/080415decision.pdf, viewed October 13, 2008. See also, "Debt Services Operations Settle FTC Charges," FTC press release dated March 30, 2005, reproduced at http://www.ftc.gov/opa/2005/03/creditcouncel.shtm, viewed October 14, 2008.

[216]Remarks of Lydia B. Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission, before the National Association of Mortgage Brokers 2007 Legislative and Regulatory Conference, reproduced at http://www.ftc.gov/speeches/parnes/0703NAMB.pdf, viewed October 14, 2008.

[217]"FTC Enforces Gramm-Leach-Bliley's Safeguards Rule Against Mortgage Companies," FTC press release dated November 16, 2004, reproduced at http://www.ftc.gov/opa/2004/11/ns.shtm, viewed October 13, 2008. Sunbelt consent order agreement reproduced at http://www.ftc.gov/os/2002/05/sec526annrpt.htm, viewed October 13, 2004.

The FTC took action in 2005 against the Superior Mortgage Company, a New Jersey mortgage lender which the Agency alleged had failed to (1) assess risks to its customer information until more than a year after the Safeguard Rule's effective date; (2) institute appropriate password policies to control access to company systems and documents containing sensitive customer information; (3) encrypt or otherwise protect sensitive customer information before sending it by e-mail; and (4) take reasonable steps to ensure that its service providers were providing appropriate security for customer information and addressing known security risks in a timely fashion. Each of these acts constitutes a failure to comply with the GLB Safeguard Rule. As is usual in such actions, the Commission also alleged that the company deceived its customers by misrepresenting the security of their data[218].

In March of 2008, Goal Financial, LLC, a marketer and originator of student loans, settled an FTC allegation of safeguards rule violations. The FTC alleged that Goal failed: (1) to adequately assess risks to the information it collected and stored in its paper files and on its computer network; (2) to adequately restrict access to personal information stored in its paper files and on its computer network to authorized employees; (3) to implement a comprehensive information security program, including reasonable policies and procedures in key areas such as the collection, handling, and disposal of personal information; (4) to provide adequate training to employees about handling and protecting personal information and responding to security incidents; and (5) in a number of instances to require third-party service providers by contract to protect the security and confidentiality of personal information. Taken together, the Agency alleged, these practices by Goal put its customers' nonpublic personal information at risk by failing to implement the required GLB-required safeguards adequately[219].

In November 2008, the FTC obtained a consent order under which Premier Capital Lending, Inc., a Texas lender, settled charges that it violated the GLB requirement to secure customer information. Premier allowed a third-party home seller to access the data without taking reasonable steps to protect it. A hacker then compromised the data by breaking into the home seller's computer, obtaining the lender's credentials, and using them to access hundreds of consumer credit reports. The FTC also charged Premier with violating its own representations to consumers that it secured the information as required under GLB. Such misrepresentations violate the ban in section 5 of the Federal Trade Commission Act against deceptive practices[220].

3. The Disposal Rule

In December 2007, the FTC charged American United Mortgage Company, an Illinois mortgage company, with leaving loan documents containing consumers' sensitive

[218]FTC Docket No. C-4153 (December 14, 2005). See Federal Register, volume 70, No. 193, October 6, 2005, pp. 58414-415 regarding the settlement by consent order.
[219]Federal Register , Vol. 73, No. 51, Friday, March 14, 2008, p. 13898.
[220]Federal Trade Commission Docket C-4216. The Decision and Order is reproduced at http://www.ftc.gov/os/caselist/0723013/080415decision.pdf, viewed October 13, 2008.

personal and financial information in and around an unsecured dumpster, in violation of the Disposal Rule. The data involved Social Security numbers, bank and credit card account numbers, income and credit histories, and consumer reports. The company agreed to pay a $50,000 fine[221]. As noted above, a provider's methods for compliance with the Rule are required by the FTC to be made a part of a financial institution's safeguard program.

4. Pretexting

Pretexting was considered a violation of the Federal Trade Commission Act prior to the Gramm-Leach-Bliley Act. GLB added to the Agency's arsenal of legal authorities against this practice and in some respects increased the penalties.

After GLB's passage in 1999, the FTC brought over a dozen cases alleging violations of the pretexting provisions, involving various business practices. The Agency launched "Operation Detect Pretext" in 2001. This program combined a broad monitoring program, the widespread dissemination of industry warning notices, consumer education, and aggressive law enforcement. In the initial monitoring phase of "Operation Detect Pretext," FTC staff "surfed" more than 1,000 websites and reviewed more than 500 advertisements in print media, seeking to identify firms that were offering to conduct searches of consumers' financial data. The FTC staff found approximately 200 firms that offered to obtain and sell consumers' asset or bank account information to third parties.

The FTC initially filed lawsuits in three Federal District Courts to halt these pretexting practices.[222] In one particularly egregious case, the defendants targeted consumers who had no credit or bad credit with offers of pre-approved, low-interest rate Visa or MasterCard credit cards, providing they would let the defendants access their bank accounts to debit an advance fee for the cards. Defendants represented to their targets that they were eligible for these cards based on a prior credit application, though these representations were a ruse and the defendants had no prior contact with their targets[223].

The anti-pretexting provisions of the Act can also be used by the government to stop Internet spam "phishing" practices. In 2003, the FTC and the Justice Department filed charges in Federal District Court against an alleged spammer named Zachary Keith Hill, alleging that Hill sent spam e-mail messages representing himself to be from Internet

---

[221]See "Company Will Pay $50,000 Penalty For Tossing Consumers' Credit Report Information in Unsecured Dumpster," FTC press release, December 18, 2007, reproduced at http://www.ftc.gov/opa/2007/12/aumort.shtm, viewed November 15, 2008.

[222]*FTC v. Victor L. Guzzetta, d/b/a Smart Data Systems*, No. CV-01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. AMD-01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L.Garrett, d/b/a Discreet Data Systems*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002). FTC press release "As Part of "Operation Detect Pretext" FTC Sues to Halt "Pretexting," April 18, 2001, http://www.ftc.gov/opa/2001/04/pretext.shtm, viewed October 13, 2008.

[223]Federal Trade Commission v. Sun Spectrum Communications Organization *et al.* (U.S.D.C. Southern District of Florida), Civil Case 03-8110, filed December 2, 2003, complaint reproduced at http://www.ftc.gov/os/caselist/0323032/031202cmp0323032.pdf, viewed October 13, 2008.

service provider AOL or, in some cases, from the online payment mechanism PayPal. Through various misrepresentations contained in these messages, Hill obtained personal and financial information, including credit card and bank account information. Hill and others with whom he shared the information thus gleaned, then used the information that consumers had submitted to purchase goods or services on those consumers' credit cards, debit cards, and/or bank account information without the consumers' knowledge or authorization[224].

In 2003, the FTC obtained another injunction in Federal District Court. A defendant known as CJ allegedly used hijacked corporate logos and deceptive spam e-mails to fraudulently obtain consumers' credit card numbers and other financial data via the Internet[225].

In another 2003 action, the FTC obtained a Federal District Court injunction halting the scamming practices of seven corporations and nine individuals operating as "The Assail Telemarketing Network." Part of the scheme involved obtaining bank account numbers from consumers by false pretenses, a violation of the pretexting prohibition[226].

In the same year, the FTC obtained yet another consent judgment in a Federal District Court against a company and its principal operator who used "spoof" e-mails to obtain nonpublic personal information from recipients. This operator misrepresented the e-mails as coming from Prudential (implying a well-known insurer) and Fannie Mae (the Federal National Mortgage Corporation). The defendant agreed, as a part of the consent order, to stop spoofing and engaging in pretexting or any other GLB violations[227].

---

[224]U.S.D.C. Southern District of Texas, complaint dated December 3, 2003, reproduced at http://www.ftc.gov/os/caselist/0323102/040322cmp0323102.pdf, viewed October 14, 2008. A plea agreement was entered by the defendant on February 9, 2004. See Federal Trade Commission, Fourth Annual Report To Congress Under Section 526(B) Of The Gramm-Leach-Bliley Act ("Fraudulent Access to Financial Information"), reproduced at http://www.ftc.gov/os/2004/07/fourthannualglbrpt.pdf, p. 1, viewed November 4, 2008. The FTC and the Justice Department filed a separate complaint against Hill in the U.S. District Court for the Eastern District of Virginia, Alexandria Division, see "FTC, Justice Department Halt Identity Theft Scam," FTC press release dated March 22, 2004, viewed at http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm, October 13, 2008.

[225]*FTC v. C.J.*, Civ. No. 03-5275 (Central District of California, stipulated permanent injunction entered July 25, 2003) order prohibits defendant from future violations of the FTC Act and the Gramm-Leach Bliley Act. See "FTC, Justice Department Halt Identity Theft Scam," FTC press release dated March 22, 2004, viewed at http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm, October 13, 2008.

[226]Federal Trade Commission v. Assail, Inc., *et al.*, U.S. District Court for the Western District of Texas, Waco Division, stipulated order and permanent injunction dated September 22, 2003, reproduced at http://www.ftc.gov/os/caselist/assail/050124stipordspecialtyoutsourcing.pdf, viewed October 15, 2008. See also, "FTC Charges Telemarketing Network with Selling Bogus Advance-Fee Credit Card Packages," FTC press release dated January 17, 2003, reproduced at http://www.ftc.gov/opa/2003/01/assailnetwork.shtm, viewed October 14, 2008.

[227]Federal Trade Commission v. Universal IT Solutions and Anthony Tamraz, U.S. District Court, Central District of California, Southern Division, SAVC 02-1026 Doc (MLGx), order entered into April 28, 2003, Stipulated Judgment and Order reproduced at http://www.ftc.gov/os/caselist/dojsweep/030505universalstip.pdf, viewed October 13, 2008.

In 2004, the FTC in Federal District Court obtained an injunction against a minor (unnamed in the publicly released documents) who obtained nonpublic personal information from consumers in a scam that involved obtaining and making unauthorized use of other individuals' credit card numbers[228].

Pretexting is the most abusive of the practices that constitute violations of Gramm-Leach-Bliley. It involves fraudulent schemes and fraudulent intent. While pretexting was considered fraudulent conduct under other laws well before GLB was enacted, the Act gave the Commission additional tools to deal with it[229].

B. Federal Reserve System

The small number of formal actions taken by the Federal Reserve System (FRS) and the other depository institution regulatory Agencies listed below, as contrasted with the number of FTC actions described above, should not be surprising. Depository financial institutions such as banks, thrift institutions, and credit unions undergo periodic examinations for the "safety and soundness" of their business practices and their financial positions. The certainty of periodic examination is a powerful incentive to be in timely compliance with regulatory requirements. Minor irregularities under such statutes as Gramm-Leach-Bliley may be noted in, and voluntarily corrected as a result of, a bank examination report without the need for the enforcement agency to resort to a formal procedure.

1. Privacy of Customer Information

In 2008, the FRS entered into a consent order prohibiting a former bank official from further violations of the Gramm-Leach-Bliley data privacy provisions. The official, while employed at an Illinois state-chartered FRS member bank, allegedly removed a computer from the bank and used the nonpublic personal customer information in the computer for the purposes of his own start-up trust company[230].

2. Failure to Establish and Maintain an Adequate Safeguards Program

In 2008, the FRS entered into a written agreement with Newnan Coweta Bancshares, Inc., and Neighborhood Community Bank, of Newnan, Georgia, in which the banks agreed to implement the use of appropriate technology to assure the adequacy of their customer information safeguards system[231].

---

[228]Federal Trade Commission v. [name redacted], a Minor, By His Parents, U.S. Federal District Court for the Eastern District of New York, Brooklyn Office, Civil Case No. 04 2086, stipulated judgment and final order for injunction reproduced at http://www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf, viewed October 15, 2008.

[229]A list of FTC pretexting enforcement actions can be viewed at http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.html, viewed October 13, 2008.

[230]In the Matter of John H. Lohmeier, Docket No. 08-029-E-1, Order of Prohibition dated October 1, 2008, reproduced at http://www.federalreserve.gov/newsevents/press/enforcement/enf20081002a1.pdf, viewed November 11, 2008.

[231]Docket Nos. 08-018-WA/RB-HC and 08-018-WA/RB-SM, signed September 2, 2008, reproduced at http://www.federalreserve.gov/newsevents/press/enforcement/enf20080910a1.pdf , viewed November 11,

C. Office of the Comptroller of the Currency

1. Privacy Violations and Failure to Establish and Maintain an Adequate Safeguards Program

In October 2002, ACE Cash Express, Inc., and Goleta National Bank, Goleta, California, signed cease and desist orders with the Office of the Comptroller of the Currency regarding unlawful practices that included violations of the rules for establishing and maintaining safeguards for the privacy of customers' information and violations of the privacy provisions of GLB, as well[232].

D. Federal Deposit Insurance Corporation (FDIC)

1. Failure to Establish and Maintain an Adequate Safeguards Program

Eight banks under the FDIC's GLB enforcement jurisdiction have been charged with failure to establish and maintain an adequate safeguards program. These include: Elderton State Bank of Elderton, Pennsylvania[233]; American State Bank, Tulsa, Oklahoma[234]; Centennial Bank, Ogden, Utah[235]; First American Bank, Jackson, Mississippi[236]; SouthwestUSABank, Las Vegas, Nevada[237]; Columbia Savings Bank, Cincinnati, Ohio[238]; Family Bank and Trust Company, Palos Hills, Illinois[239]; Cleveland Community Bank, Cleveland, Mississippi[240].

2008. The Banking Commissioner of Georgia also joined the agreement and, therefore, would have the power to prosecute future violations of the agreement.

[232]Consent Order EA #2002-93, reproduced at http://www.occ.treas.gov/ftp/eas/Goleta%20Consent.pdf , viewed October 18, 2008. See also, OCC Administrator of National Banks News Release NR 2002- 85, October 29, 2002, reproduced at www.occ.treas.gov/ftp/release/2002-85.doc, viewed October 18, 2008. The details of the violations are not spelled out in these consent orders at the level of detail provided by those of some other agencies.

[233]In the Matter of Elderton State Bank, Elderton, Pennsylvania, Docket No. 03-131b (10-7-03). Decision and Order reproduced at http://www.fdic.gov/bank/individual/enforcement/12108.html#HN7, viewed October 17, 2008.

[234]Docket No. 04-245b (3-23-05), Decision and Order reproduced at http://www.fdic.gov/bank/individual/enforcement/12381.html#HN19, viewed October 17, 2008.

[235]Docket No. 03-163b (8-27-03), Decision and Order reproduced at http://www.fdic.gov/bank/individual/enforcement/12082.html, viewed October 17, 2008.

[236] Docket No. 02-032b (5-15-02), Decision and Order reproduced at http://www.fdic.gov/bank/individual/enforcement/11931.html, viewed October 17, 2008.

[237] Docket FDIC-06-216(b), November 9, 2006, Order to Cease and Desist reproduced at http://www.fdic.gov/bank/individual/enforcement/2006-11-04.pdf, viewed October 17, 2008.

[238]Docket FDIC-07-183b, November 13, 2007, Order to Cease and Desist reproduced at http://www.fdic.gov/bank/individual/enforcement/2007-11-02.pdf, viewed October 17, 2008.

[239]Docket No. 02-092b, Cease and Desist Order reproduced at http://www.fdic.gov/bank/individual/enforcement/11980.html, viewed October 17, 2008.

[240]Docket No. 04-260b (12-15-04), Cease and Desist Order reproduced at http://www.fdic.gov/bank/individual/enforcement/12335.html, viewed October 17, 2008.

Two things are notable about these banks' GLB violations. One is that they were all charged with a wide variety of other serious violations of good banking practices, the GLB violations being only one class of violation. The other is that some of the violations were enjoined *years* after the banks were first obligated to comply with the Act's safeguards program requirements. This may suggest that the FDIC is not as effective as it should be in detecting GLB violations among financial institutions that are not otherwise engaged in widespread violation of FDIC rules.

E. Securities and Exchange Commission

1. Privacy Violations

In August 2007, the SEC charged NEXT Financial Group, a Houston-based securities broker/dealer and one of the nation's fastest-growing broker/dealers with very serious and systematic violations of Gramm-Leach-Bliley. The SEC alleged that NEXT allowed those of its registered representatives ("reps") who were leaving the firm's employment to take customers' nonpublic personal customer information with them, without disclosing this to the customers involved and without providing a reasonable opportunity for the customer to opt out of such sharing of the information. The departed "reps" and their new employers were nonaffiliated third parties. The SEC also charged that NEXT failed to safeguard this customer information. The SEC alleged, additionally, that NEXT willfully aided and abetted and caused violations of the regulations by reversing the process, encouraging and systematically helping, registered "reps" who were joining NEXT from other brokerage firms (that is, new NEXT "rep" recruits) to disclose their customers' nonpublic personal information to NEXT without proper notice to the customers and without affording the customers a reasonable opportunity to opt out of such sharing of their information. In the case of information coming to NEXT through its new reps[241], NEXT was a nonaffiliated third party. As relief for the alleged violations, the SEC's Division of Enforcement sought a cease-and-desist order and a civil monetary penalty. With certain narrow exceptions, an SEC Administrative Law Judge in June, 2008, found that NEXT had violated the law as charged by the SEC enforcement staff, enjoined NEXT from future Gramm-Leach-Bliley violations and imposed a fine of $125,000, in light of the large volume of information that had been unlawfully shared[242].

---

[241]This information included (1) name of the primary account owner, trustee, or custodian and the secondary account owner; (2) brokerage account numbers; (3) direct account numbers (*i.e.*, mutual fund account numbers and variable annuity account numbers); (4) whether or not each brokerage account is "managed"; (5) Social Security numbers or tax identification numbers of the primary and secondary account owners; (6) account types (*i.e.*, individual retirement account (IRA), Roth IRA, joint, trust, Uniform Gift to Minors Act or Uniform Transfers to Minors Act); (7) net worth; (8) annual income; (9) years of investment experience; (10) mailing address and, if that is a post office box, the actual residential address, with suite or apartment numbers, if applicable; (11) home telephone number; (12) date of birth of the primary account owner; (13) bank name, city, state, and zip code; (14) passport number; (15) driver's license number; (16) occupations of the primary and secondary account owners; and (17) the primary and secondary account owners' employers, with their cities, states, zip codes, work telephones, and facsimile numbers. SEC Administrative Proceeding File No. 3-12738, Initial Decision, June 18, 2008, reproduced at http://www.sec.gov/litigation/aljdec/2008/id349jtk.pdf, viewed October 18, 2008.

[242]Ibid., p. 54.

F. Commodity Futures Trading Commission

Not unexpectedly, we found no cases enforcing the Gramm-Leach-Bliley Act. The CFTC's GLB Rule applies only in the seemingly very limited number of situations (if indeed there are any) in which an individual is engaged in commodity futures trading for personal, family or household purposes.

XIV. State Financial Privacy Statutes

A. General State Privacy Laws

Most states have laws addressing at least some aspects of financial information privacy. Some of the broader state laws are equivalent to the Gramm-Leach-Bliley Act. A few state laws exceed the GLB requirements, which GLB allows to the extent they are not inconsistent with GLB.

A few states have broad financial information privacy protection laws. Some of these laws, by prohibiting virtually all disclosures for commercial purposes without the consumer's authorization, establish an opt in requirement for disclosure that is, by definition, more protective than Gramm-Leach-Bliley's opt out provision[243].

Illinois, for example, has a general prohibition on unauthorized disclosure of customers' financial records by banks, savings and loans, credit unions, regulated consumer installment lenders, lenders regulated under the Consumer Sales Finance Agency Act, and other financial services providers under the jurisdiction of any state financial institution regulatory authority[244]. Because each disclosure of protected information made for commercial purposes would require the consumer's authorization, these provisions are, in effect, opt in requirements, rather than GLB-style opt out requirements.

Even these laws, however, may have weaknesses. The tough Illinois requirements, for example, are not found in Illinois' Payday Loan Reform Act that governs payday lenders or the Community Currency Exchange Act that regulates check cashing and money wiring services[245].

---

[243]This information does not address state insurance laws and regulations, which are summarized in Appendix A.

[244]With various exceptions related to law enforcement and other legal process, institutional regulatory examination and other necessary disclosures. 205 ILCS 5/48.1(c), reproduced at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1178&ChapAct=205%26nbsp%3BILCS%26nbsp%3B5%2F&ChapterID=20&ChapterName=FINANCIAL+REGULATION&ActName=Illinois+Banking+Act, viewed December 12, 2008. ILCS 305/10 Sec. 10(c), reproduced at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1185&ChapAct=205%26nbsp%3BILCS%26nbsp%3B305%2F&ChapterID=20&ChapterName=FINANCIAL+REGULATION&ActName=Illinois+Credit+Union+Act, viewed December 12, 2008.

[245]815 ILCS 122/1-1 and Public Act 094-0538, respectively.

Alaska has an opt in requirement[246] that applies to commercial banks, savings banks, credit unions, premium finance companies, small loan companies, bank holding companies, financial holding companies, trust companies, savings and loan associations, and deferred deposit advance licensees[247]. Connecticut has such an opt in provision regarding the customer records of all banks and credit unions and in connection with any mortgage loan[248]. Neither Alaska nor Connecticut restricts these protections to state residents, as do numerous of the state laws discussed below.

North Dakota also has an opt in provision, prohibiting any unauthorized disclosure of customer information except to comply with legal processes and other very limited procedures to fulfill legal or regulatory purposes. The law applies to any financial institution authorized to do business in the state, but it only protects residents and others domiciled in the state.

Vermont law strictly prohibits unauthorized disclosure by a broad range of financial service providers of a customer's personal financial information, with the usual, necessary exceptions enabling law enforcement and investigation and the necessities of service providers in managing a customer's account. This restriction also amounts to an opt in requirement. Unlike numerous other state financial privacy laws, it protects all customers, not just state residents[249].

B. State "Shredding" and Safeguards Laws

A substantial number of states have so-called "shredding" or "document disposal" laws that govern financial services providers' safe disposal of consumers' financial records. And at least ten states have a safeguards requirement that applies to the personal financial information of state residents. Some of these laws apply to both computer and paper records while others apply only to computer data bases.

C. State Breach of Data Notification Laws

As of November 4, 2008, forty-four states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have laws that require notification of consumers whose personal identification data has been breached. Under some laws, a breach automatically triggers the notice requirement. Under others, notice is only required if the breach is deemed possible or likely to result in harm to the consumer, and is excused if such risk is not

---

[246]Alaska Stat. 06.01.028, reproduced at http://touchngo.com/lglcntr/akstats/Statutes/Title06/Chapter01/Section028.htm, viewed December 12, 2008.

[247] Alaska Stat. 06.01.050(3), reproduced at http://touchngo.com/lglcntr/akstats/Statutes/Title06/Chapter01/Section050.htm, viewed December 12, 2008.

[248]Conn. Gen. Stat. Ann. Chapter 664 §§ 36a-41 - 45, accessible via the search function at http://search.cga.state.ct.us/dtsearch_pub_statutes.html, viewed December 12, 2008.

[249] Vermont Statutes Title 8, Chapter 200, §§ 10101 -10205, reproduced and available through the index at http://www.leg.state.vt.us/statutes/sections.cfm?Title=08&Chapter=200, viewed December 8, 2008.

present. Only Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota have no breach notification law[250].

Data breach notification laws are to some degree a state equivalent of the previously-discussed federal Red Flag rules that require a financial services provider to notify consumers of a breach of their financial data in some circumstances. Some of these state laws require notification only under certain circumstances, such as if the data is not encrypted[251] or not redacted[252]. A few state laws apply the requirements to encrypted data, as well, if there is reason to believe that the encryption formula has also been accessed without authorization.

Some states have an exception if the breach has been evaluated and determined not possible or likely to result in harm to the consumer. Others require notification of breach without an assessment of potential harm. Some require, in the event of a large breach, that the party responsible for breach notifications also notify all nationwide consumer credit reporting agencies regarding the breach[253]. And a majority apply only to computerized information, but not to paper records[254].

The state notification laws usually place the legal burden of notifying a consumer about a data security breach on the owner or licensee of the data base. Presumably, a financial services provider either owns or licenses the data it uses that may be subject to a breach. If not, it may not be responsible for the actual notification to the consumer. However, these laws also typically require *any user* of the data to notify the owner or licensor of any breach of which the user becomes aware. That notification triggers the notification responsibility of the owner or licensor. Therefore, a financial institution that uses a personal information data base -- whether it is the owner, a licensor or merely a user -- whenever it becomes aware of a breach must take some action, whether direct or indirect, to trigger the notice requirements.

---

[250]"State Security Breach Notification Laws," National Conference of State Legislators, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm, viewed December 10, 2009.

[251]Encrypted means coded by use of an algorithm. An algorithm is a mathematical formula that converts data so as to be essentially meaningless without the conversion formula and, practically speaking with regard to large amounts of data, without a computer or other device that can use the algorithm to convert the encrypted data back into original form. Some state definitions treat numbers as redacted if only the last few in the series of numbers are accessible, such as the last five digits of a social security number or the last four digits of a drivers license number. See Code of Virginia 18.2-186.6A.

[252]Redaction means physically altered so as to obliterate protected information or otherwise render the protected information unreadable. Redaction is a term that applies to paper records, as redaction of an electronic record would render the information useless to the legitimate database user. As paper databases give way to electronic records, redaction becomes an outdated mode of data protection and the statutory term "redacted" becomes meaningless.

[253] See, e.g., § 28-3852 of the D.C. law, referenced below. The typical state law trigger point for notifying national consumer credit reporting agencies is 1,000 notices relating to an incident of breach, but New York's trigger point is 5,000 notices related to a breach, while Minnesota's trigger point is only 500 notices. Some state laws' requirements to notify credit reporting agencies only apply if the party is not already obligated to do this by the federal Fair Credit Reporting Act.

[254]See, for instance, the Washington law, discussed below.

Typical of what triggers a notice requirement under these laws is unauthorized acquisition from a data base of "a resident's first name and last name or first initial and last name in combination with *any one or more* of the following data elements that relate to such resident":

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a customer's financial account;

provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public[255]. Some states, like Oregon, include passport information in the list of "trigger" data. Many state laws protect account numbers, credit card and debit card numbers only if the access code as well as the identification number has been breached or when the identification number can be used without the code. A very few states include biometric identifiers such as fingerprints, iris or retina prints or even RNA profiles as triggering information. Some financial services providers have begun to use these markers to verify the identity of consumers and customers for such purposes as ATM access and check cashing. Again, notification still may not be required by some state laws if it is determined that the breach is not likely to result in harm to the consumer.

Breach notification laws protect specific types of information that would facilitate identity theft and fraudulent use of the consumer's account by unauthorized users, rather than protecting all consumer financial information (for example, account balances or patterns of purchases) for privacy purposes.

Some state notification laws expressly do not apply to parties that are subject to the Gramm-Leach-Bliley Act. They deal only with businesses other than GLB-covered financial services providers and leave it entirely up to the Federal agencies that enforce GLB to deal with breach notice requirements. Others treat compliance with the GLB-required Safeguards rules as compliance with the state law, but reserve the right of state enforcement in the event of a required breach notification failure. Or, they may condition acceptance of compliance with GLB (or even with the service provider's own internal guidelines) as compliance with the state law only if the provider meets state law requirements for timely delivery of the notice of breach.

Typically, the state laws only require notification of breach to state residents. They leave protection of nonresidents to federal requirements and/or other states' applicable laws. But, some states protect all customers regardless of residence or domicile. Some state

[255]See Massachusetts General Laws, Title 15, Chapter 93H, Section 1(a), definition of "personal information," reproduced at http://www.mass.gov/legis/laws/mgl/93h-1.htm.

laws allow consumers to file civil suits to recover damages resulting from violations of data breach notification requirements.

Below are highlights of consumer financial information privacy protection laws in the various states and some territories of the U.S..

Alabama
Alabama law has been characterized as requiring banks to disclose customer records only in response to lawful demands by a court or governmental agency[256]. However, the plain language of the statute seems only to command banks to produce customer records pursuant to legal process and to render bank officials harmless for complying with such processes[257].

Alaska
Alaska law generally requires a customer's opt in consent for a financial institution to disclose customer information, rather than providing the consumer a right to opt out. It provides no blanket exception or authorization for sharing information among affiliated companies, although there is permission for sharing with marketing partners[258]. Alaska's new data breach notification law will take effect July 1, 2009. It protects unencrypted and unredacted personal information, as well as encrypted data if the key to encryption may have been compromised[259].

Arizona
Arizona has a data security breach notification law that protects unencrypted, unredacted personal information. Compliance with Gramm-Leach-Bliley constitutes compliance with the Arizona statute[260]. Arizona also has a personal information Safeguards requirement that applies to a resident's personal information[261].

Arkansas
Arkansas has a law that requires data security breach notification in the event unencrypted personal information is breached. The same law also contains a shredding requirement[262].

---

[256]E.g.g, Compilation of State and Federal Privacy Laws, Smith, (Privacy Journal) (1992), p. 6 and myfaircredit.com, http://www.myfaircredit.com/forum/viewtopic.php?t=139, viewed December 8, 2008, at item (g).
[257]Alabama Code, Section 5-5A-43.
[258]Alaska Stat. § 6.01.028. See also, "Financial Privacy Laws Affecting Sharing Customer Information Among Affiliated Institutions," Congressional Research Service, updated February 27, 2003, reproduced at http://epic.org/privacy/fcra/RS21427.pdf, viewed November 25, 2008.
[259]Alaska Statutes 45.48.010, accessible at 2008 H.B. 65.
[260](Ariz. Rev. Stat. Ann. § 44-7501(H)).
[261] "Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt.
[262](Ark. Code Ann. § 4-110-101 Et Seq.).

California
The California Financial Information Privacy Act, Cal. Fin. Code §§ 4050-60, which is commonly referred to as S.B. 1, was enacted in 2003. Parts of this law that exceeded the GLB Act by providing an opt-out on sharing information with affiliates were ruled invalid by the U.S. Ninth Circuit Court of Appeals, based on a finding that they were inconsistent with the Fair Credit Reporting Act. The state had argued that the provision was an extension of the state's right to exceed the requirements of the GLB Act. But parts of it, including a ban on sharing non-financial information such as a consumer's purchasing patterns, were upheld on appeal[263]. (A lower Federal court had ruled California's extra requirements to be legal[264].) California also has a data security breach notification law that applies to unencrypted personal information; it protects residents' information held by a private party or the state government[265]. And, it has a safeguards requirement that applies to the personal information of state residents[266].

Colorado
Colorado has a shredding law with a fairly rare provision (see Texas notice of security breach law, discussed below) that includes biometric data among the records that must be properly destroyed or disposed of[267]. Colorado's data security breach notification law protects residents' unencrypted, unredacted personal information. It applies only to parties not subject to GLB[268].

Connecticut
Connecticut law requires consumer opt in consent for disclosure by banks and credit unions, rather than a consumer opt out right. Connecticut law also prohibits financial institutions from unauthorized sharing with third parties of any information from consumers' records obtained in connection with mortgage applications[269]. It also requires all financial institutions in the state to comply with Gramm-Leach-Bliley. Connecticut has a shredding and a data security breach notification law that applies to unencrypted information relating to residents of the state[270]. It has a safeguards requirement for the personal information of residents[271]. And it makes it a state misdemeanor to knowingly

---

[263]"Part of State's Financial Privacy Law Upheld", San Francisco Chronicle online, September 5, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/09/05/BUVJ12OCR8.DTL, viewed December 5, 2008.
[264] "Judge upholds State's Financial Privacy Law," July 1, 2004, *Los Angeles Times* online, http://articles.latimes.com/2004/jul/01/business/fi-privacy1, viewed December 5, 2008.
[265](Cal. Civ. Code § 1798.82). See summary at http://www.ncsl.org/programs/lis/privacy/02enact-finpriv.htm, viewed December 5, 2008.
[266]"Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt.
[267]Colo. Rev. Stat. § 6-1-713, reproduced at http://www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=, viewed December 14, 2008.
[268](Colo. Rev. Stat. § 6-1-716).
[269]Raised Bill No. 7073, reproduced at http://www.cga.ct.gov/2007/TOB/H/2007HB-07073-R00-HB.htm, viewed December 10, 2008.
[270](Conn. Gen. Stat. § 36a-701b).
[271] "Developments in Security and Privacy Law," Computer Security Institute, Fall 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt.

and willingly violate either the Connecticut or the GLB restrictions on unauthorized disclosure *or* to even knowingly and willingly induce or attempt to induce such a violation[272].

Delaware
Delaware has a data security breach notification law that protects residents' unencrypted personal information[273].

District of Columbia
D.C. has a data breach notification law that protects residents' unencrypted personal information. The law applies only to providers that are not in compliance with Gramm-Leach-Bliley's Safeguards requirements. The D.C. law allows District residents who have suffered injury from the data breach to file civil suits to recover damages[274].

Florida
Florida law requires that official court and other state records redact (remove or make illegible) each Social Security number, and any complete bank account, debit, charge, or credit card number[275]. Florida has a data security breach notification law that protects residents' unencrypted personal information[276].

Georgia
Georgia has a data security breach notification law that applies to "information brokers" and "data collectors." It covers any business that "engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties"[277].

Hawaii
Hawaii's consumer financial information privacy law conforms to the Gramm-Leach-Bliley Act[278]. Hawaii has a data security breach notification law that protects unencrypted and unredacted personal information. It is one of the few state laws that extend its protections equally to state residents and non-residents alike. And, like the D.C. law, it provides for civil suits to recover damages for injury attributable to a violation of the law's requirements. Furthermore, the Hawaii statute provides consumers with protection

---

[272] Conn. Gen. Stat. Chapter 664, §36a-57.
[273](Del. Code Ann. Tit. 6, § 12b-101).
[274] D.C. Code, Title 28, Chapter II, http://www.dccouncil.washington.dc.us/images/00001/20061218135855.pdf, viewed December 8, 2008.
[275] Chapter 2002-391. See summary at http://www.ncsl.org/programs/lis/privacy/02enact-finpriv.htm, viewed December 5, 2008.
[276](Fla. Stat. § 817.5681).
[277] (Ga. Code Ann. § 10-1-911).
[278]Hawaii Rev. Stat. §§ 431: 3A-101 *et seq*., reproduced at http://www.capitol.hawaii.gov/hrscurrent/Vol09_Ch0431-0435E/HRS0431/HRS_0431-0003A-0101.htm and following pages, viewed December 14, 2008.

against breach of security of information possessed by the state government[279]. Hawaii also has a shredding law[280].

Idaho
Idaho has a data security breach notification law that protects residents' unencrypted personal information[281].

Illinois
Illinois has a financial information privacy law with an opt in, rather than an opt out, requirement regarding sharing of nonpublic personal financial information[282]. Illinois has a data security breach notification law that applies to private businesses and units of the state government. It protects unencrypted and unredacted personal information pertaining to residents of the state. The Illinois statute also requires safe disposal of personal data or written material pertaining to a consumer that has been collected by a state agency[283].

Indiana
Indiana has a data security breach notification law covering unencrypted information relating to state residents[284]. Personal information held by the state government is also subject to a breach notification requirement[285].

Iowa
Iowa has a breach of data base notification requirement that protects unencrypted, unredacted personal information[286].

Kansas
Kansas financial information privacy law conforms to Gramm-Leach-Bliley and combines financial privacy rights with health privacy rights. Its data security breach notification law protects unencrypted, unredacted personal information[287].

Louisiana
Louisiana law prohibits banks and bank affiliates from disclosing any customer information, except among affiliates, with the usual exceptions for complying with legal process and business needs contemplated by the federal Fair Credit Reporting Act[288].

---

[279](Hawaii Revised Stat. §§ 487N-1 et seq.).
[280]Act 136. See summary at http://www.ncsl.org/programs/lis/CIP/priv/breach06.htm, viewed December 10, 2008.
[281](Idaho Code Ann. § 28-51-104 Et Seq.).
[282] Testimony of Edmund Mierzwinski, "Oversight hearing on Financial Privacy and the Gramm-Leach-Bliley Financial Services Modernization Act," Committee on Banking, Housing and Urban Affairs, September 9, 2002, reproduced at http://www.privacyrights.org/ar/USPirg-GLB0902.htm, viewed December 8, 2008.
[283] (815 Ill. Comp. Stat. Ann. 530/5, /10). See, "Illinois Passes Privacy Act," consumeraffairs.com, May 18, 2005, http://www.consumeraffairs.com/news04/2005/il_privacy.html, viewed December 8, 2008.
[284] (Ind. Code § 24-4.9) *et seq*.
[285]Ind. Code Sec. 4-1-11 *et seq*.
[286]Iowa Code Chapter 2007-1154.
[287]Kansas Stat. 50-7a01, 50-7a02.
[288]Louisiana Rev. Stat. 6:333, reproduced at http://www.legis.state.la.us/lss/lss.asp?doc=105934.

This law pertains to records without regard to their encryption or redaction and protects all customers, not only residents of the state. Louisiana law also prohibits disclosure by any financial institution of nonpublic customer information to a third party for the purpose of soliciting the sale of insurance and the financial institution itself cannot use the data for that purpose[289]. Louisiana has a data security breach notification law that applies to unencrypted and unredacted information pertaining to state residents. Louisiana law allows civil suits for damages resulting from failure to notify in accordance with the notification law. Compliance with the federal requirements is treated as compliance with the state law, but companies subject to the federal requirements remain subject to Louisiana law[290].

Maine

Maine has a statute that conforms various state privacy laws to Gramm-Leach-Bliley[291]. The Maine Notice of Risk to Personal Data Act requires notification of data breach to any state resident whose unencrypted, unredacted personal information has been breached. The Maine law applies to units of state government as well as to businesses[292].

Maryland

Maryland law prohibits unauthorized disclosure of financial records pertaining to a customer. The consumer's authorization must specify the recipient in order for the information to be shared. This amounts to an opt in provision. This law applies to customers without regard to their residence in the state. It contains the usual exceptions pertaining to law enforcement and investigations, probate and guardianship matters[293]. Maryland has a data security breach notification law that applies to information that is unencrypted and unredacted. It requires security measures to be taken commensurate with the nature of the information and with the size and nature of the business. It contains a requirement for destruction of records. The law protects residents of Maryland. The law is effective January 1, 2009[294]. Maryland also has a safeguards requirement that applies to personal information pertaining to residents[295].

Massachusetts

Massachusetts has a personal information safeguards law that includes a data security breach notification requirement. State agencies are also required to safeguard consumers' personal data. The requirements protect residents of the state. Compliance with federal law is deemed to be compliance with Massachusetts law only insofar as the business

---

[289]Louisiana Rev. Stat. 22:1604, reproduced at http://www.legis.state.la.us/lss/lss.asp?doc=508597.
[290](La. Rev. Stat. Ann. § 51:3071 Et Seq.)
[291] P.L. 2001, c. 262. See summary at http://www.ncsl.org/programs/lis/privacy/01enact-finpriv.htm, viewed November 25, 2008.
[292]Me. Rev. Stat. tit. 10 §§ 1347 et seq.
[293]Maryland Code, Financial Institutions, Title 1 §1-302, reproduced at http://www.michie.com/maryland/lpext.dll?f=templates&fn=main-h.htm&cp=mdcode.
[294]Chapter 531, Subtitle 35 §14-3502, text reproduced at http://michie.lexisnexis.com/maryland/lpext.dll?f=templates&fn=main-h.htm&cp, viewed December 8, 2008.
[295]Maryland Code, Title 14 §14-3503, reproduced at http://michie.lexisnexis.com/maryland/lpext.dll?f=templates&fn=main-h.htm&cp, viewed December 8, 2008.

responsible for security of the data meets the state timelines for notification[296]. Massachusetts also has a shredding requirement[297]. Massachusetts has a safeguards requirement that applies to the personal information of residents and requires the encryption of a consumer's personal data contained on a service provider's laptop computers. These provisions are scheduled to become effective May 1, 2009[298]. In 2010, the encryption requirement will extend to other portable devices as well[299].

Michigan
Michigan has a data security breach notification law that protects a resident's unencrypted and unredacted personal information[300].

Minnesota
Minnesota has a data security breach notification law that protects a resident's unencrypted personal information[301].

Missouri
Missouri has a consumer financial information privacy statute requiring compliance with Gramm-Leach-Bliley[302]. Missouri law conforms to Gramm-Leach-Bliley with regard to unauthorized disclosure of customer information to third parties[303]. In July, 2009, Missouri enacted a law protecting Missouri residents from security breaches by notifying affected consumers in writing or electronically expeditiously and without unreasonable delay. The Attorney General enforces this law[304].

Montana
Montana law conforms to Gramm-Leach-Bliley. It includes a data security breach notification law that protects resident's unencrypted information. Among the information included in the list of "triggering" data is the number of an identity card issued by a Native American tribe. It includes a shredding requirement regarding disposal of records containing personal information[305].

---

[296](Massachusetts General Laws Ann. 93H §§ 1 et seq.).
[297]Massachusetts General Law 931.
[298]201 CMR 17.00.
[299]"Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt.
[300](Michigan Compiled Laws Ann. 445.72).
[301](Minn. Stat. § 325e.61). While the caption of the relevant section suggests that the law applies only to "data warehouses," the language is typical of state notification laws, in that the responsibility for compliance lies with the party that "owns" or "licenses" the data base, but any user is held legally responsible for notifying the owner or licensor of any breach of which it becomes aware.
[302]See http://www.ncsl.org/programs/lis/privacy/01enact-finpriv.htm, viewed November 25, 2006.
[303]Mo. Rev. Stat. Chapter 362, § 362.422 reproduced at http://www.moga.mo.gov/statutes/c300-399/3620000422.htm.
[304] Missouri HB 770, reproduced at http://house.mo.gov/content.aspx?info=/bills091/bilsum/intro/sHB770I.htm, viewed August 25, 2009.
[305](Mont. Code Ann. § 30-14-1704).

Nebraska
Nebraska has a data security breach notification law that protects unencrypted personal information[306].

Nevada
Nevada has a data security breach law that includes a safeguards requirement, a shredding requirement and notification requirements in the event of a breach of personal information pertaining to residents[307].

New Hampshire
New Hampshire has a data security breach notification law. The New Hampshire disclosure requirements protect all consumers whose data has been breached, not only state residents. The New Hampshire law allows consumers injured by any violation of this law to file a civil lawsuit to recover damages, which may be double or treble damages if the violation is intentional[308].

New Jersey
New Jersey has a data security breach notification law that protects New Jersey residents. It applies to state-held records as well as business records. The law also has a shredding requirement[309].

New York
New York has a data security breach notification law that protects the private personal information of state residents[310]. New York recently amended its law governing disposal of records containing personal information[311].

North Carolina
North Carolina has a consumer financial privacy statute that restricts the state's right to access a consumer's financial information, except as specifically otherwise authorized by law or legal order. It also has a state financial information privacy protection act that conforms to the Gramm-Leach-Bliley Act[312]. North Carolina has a data security breach notification law. This statute also includes a shredding requirement[313]. The language of the North Carolina statute appears to limit the right of notification to state residents. Starting October 1, 2009, North Carolina consumers can, without paying a fee, place a security freeze on their credit reports. This new law also makes North Carolina the first

---

[306]Neb. Rev. Stat. § 87-801 *et seq*.
[307](Nev. Rev. Stat. 603a.010 Et Seq.).
[308](N.H. Rev. Stat. Ann. § 359-C:19 Et Seq.).
[309] http://lis.njleg.state.nj.us/cgi-bin/om_isapi.dll?clientID=211680932&Depth=4&TD=WRAP&advquery=%2256%3a8-163%22&headingswithhits=on&infobase=statutes.nfo&rank=&record={17AFD}&softpage=Doc_Frame_Pg42&wordsaroundhits=2&x=33&y=17&zz=.
[310](N.Y. Gen. Bus. Law § 899-Aa).
[311]See http://www.ebglaw.com/showclientalert.aspx?Show=9027, viewed December 10, 2008.
[312]North Carolina Financial Privacy Act (1985 (Reg. Sess., 1986), c. 1002, S. 1.), N.C. General Statutes, chapter 53B, accessible at http://law.onecle.com/north-carolina/53b-financial-privacy-act/index.html, viewed December 5, 2008.
[313](N.C. Gen. Stat.§ 75-60 Et Seq.).

state in the nation to require credit monitoring services to tell consumers how they can get credit reports for free. In addition, the new law allows Registers of Deeds and Clerks of Court to remove consumers' Social Security numbers from their websites, prevents creditors from reporting victims' debts caused by criminals to national credit bureaus, and requires businesses and state and local government agencies to report all security breaches to Cooper's office, not just those that impact 1,000 people or more."[314]

North Dakota
North Dakota has a consumer financial privacy law that requires a customer's written consent. This is an opt in consent requirement, rather than an opt out. The law only protects persons resident or domiciled in the state. Consent must specify the recipient of the information and the duration of the consent. Doing business with the customer may not be based on the grant of a waiver of consent and any waiver obtained despite this restriction is deemed legally invalid. The customer has a right to file a civil suit for damages plus a $1000 penalty if injured by an unlawful disclosure. The law contains the usual exceptions for obtaining the information through legal process[315]. North Dakota has a data security breach notification law that applies to the unencrypted, personal information of state residents[316].

Ohio
Ohio has a data security breach notification law that protects the personal information of state residents[317].

Oklahoma
Oklahoma law prohibits any bank, savings bank, savings association, building and loan association, savings and loan association or credit union from disclosing customer information to any unit of state government except in accordance with legal process. However, this law authorizes exchange of information among these institutions for normal business purposes[318]. Oklahoma has a security breach notification law that protects the unencrypted, unredacted personal information pertaining to a state resident[319]. Oklahoma also has a data security breach notification law that applies to the unencrypted information held by state agencies that pertains to state residents[320].

Oregon
Oregon has a data security breach notification law that protects the unencrypted and unredacted personal information of residents. The Oregon law protects passport

---

[314] Press Release, "Cooper Praises New Laws to Protect Consumers from Foreclosure, ID Theft," North Carolina Department of Justice, August 7, 2009.
[315] N.D. Cent. Code, Chapter 6-08.1, reproduced at http://www.legis.nd.gov/cencode/t06c081.pdf, viewed December 8, 2008.
[316] (N.D. Cent. Code § 51-30-01 Et Seq.).
[317] (Ohio Rev. Code Ann. § 1349.19).
[318] Okla. Stat. Title 6, Ch. 6, §§ 2201 -2206, accessible at http://www.oscn.net/applications/oscn/deliverdocument.asp?lookup=Previous&listorder=36100&dbCode=STOKST06&year= *et seq*.
[319] 2008 H.B. 2245.
[320] Okla. Stat. 74-3113.1

information as well as the more usual financial information[321]. Oregon has a safeguards requirement that applies to the personal information of residents[322].

Pennsylvania
Pennsylvania has a data security breach notification law that protects the unencrypted personal information of its residents[323].

Puerto Rico
Puerto Rico has a data security breach notification law that protects the unencrypted personal information of Puerto Rican citizens. This law allows affected consumers to file civil suits for damages caused by violations of the notification requirements[324].

Rhode Island
Rhode Island has a data security breach notification law that protects the unencrypted personal information of state residents[325]. Rhode Island has a safeguards requirement that applies to the personal information of residents[326].

South Carolina
South Carolina has a data security breach notification law that protects the unencrypted, unredacted personal information of state residents[327].

Tennessee
Tennessee law allows financial institutions to furnish information or records to the same extent provided under federal law, so long as consumer disclosure requirements and opt-out provisions are fulfilled[328]. Tennessee has a data security breach notification law that protects the unencrypted personal information of any state resident. An injured customer is authorized to file a civil suit to recover damages resulting from a violation of the disclosure requirements. However, the law only applies to financial service providers that are not subject to Gramm-Leach-Bliley[329]. Customers of service providers subject to GLB must rely on the federal law for protection of their rights. Tennessee law also has a data protection safeguards law that applies to laptop computers owned by units of state or local government. It protects only state citizens. Citizens can file a civil suit for damages

---

[321](S.B. 583).
[322]"Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt
[323]73 Pa. Cons. Stat. Ann. § 2303.
[324]Title 10, Chapter 310 §§ 4051-4055, accessible through the index at http://www.michie.com/puertorico/lpext.dll?f=templates&fn=main-h.htm&cp=prcode.
[325](R.I. Gen. Laws § 11-49.2-3)).
[326]"Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt.
[327]Title 37 S.C. Code 1976, Chapter 20, accessible at Act 190.
[328]See summary at http://www.ncsl.org/programs/lis/privacy/01enact-finpriv.htm.
[329]Tennessee Code, Title 47, Chapter 18, Section 47-18-2107, reproduced at http://www.michie.com/tennessee/lpext.dll?f=templates&fn=main-h.htm&cp=tncode, viewed December 15, 2008.

due to noncompliance with this law[330]. Since these computers can contain consumer financial information (for example, in the case of a court-owned computer containing data about alimony or child support orders), this law affords a degree of consumer financial privacy protection.

Texas

Texas has a data security breach notification law protecting state residents, but this law does not apply to service providers that are subject to Gramm-Leach-Bliley. The Texas law goes beyond most other state laws by including among the triggering data any unique biometric data such as fingerprints, voice prints, retina or iris images[331]. Texas has a safeguards requirement that applies to the personal information of residents and it has a shredding requirement. These provisions also apply only to service providers that are not subject to federal requirements[332].

Utah

Utah has a data security breach notification law[333]. Utah has a safeguards requirement and a security breach notification requirement that applies to the unencrypted personal information of residents. The Utah law also has a shredding provision[334].

Vermont

Vermont has an "opt in," rather than an "opt out," right for consumers regarding the sharing of their nonpublic personal information, with certain exceptions. This rule applies to all service providers regulated by the Vermont Department of Banking, Insurance, Securities & Health Care Administration or Banking Division[335]. The law prohibits disclosure of private personal financial information by financial institutions except as provided in a list of exceptions, none of which appear to permit inter-affiliate sharing of customer information[336]. Vermont has a data security breach notification law that protects

---

[330]Tennessee Code, Title 47, Chapter 29, Section 47-18-2901, reproduced at http://www.michie.com/tennessee/lpext.dll?f=templates&fn=main-h.htm&cp=tncode, viewed December 15, 2008.

[331](Tex. Bus. & Comm. Code Ann. § 48.001 Et Seq.).

[332]Texas Business and Commerce Code, § 48.102, reproduced at http://www.statutes.legis.state.tx.us/SOTWDocs/BC/pdf/BC.48.95170.83211.pdf, viewed December 15,2008 . See also, "Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt, viewed December 8, 2008.

[333](Utah Code Ann. § 13-44-101 Et Seq.), viewed December 8, 2008.

[334]"Developments in Security and Privacy Law," Computer Security Institute, Fall, 2008, PowerPoint presentation accessible at www.pepperlaw.com/pepper/pdfs/Adlerp_CSIFallLegalDevSecPrivLaw2008rec(2)lFinal.ppt, viewed December 8, 2008.

[335]Regulation B-2001-1, reproduced at http://www.bishca.state.vt.us/BankingDiv/regsbulletins/bnkregs/REG_B2001_01.pdf, viewed December 8, 2008.

[336]Vermont Stat. Anno. §§ 10201 - 10205.

personal information pertaining to residents and nonresidents alike[337] and it has a shredding requirement[338].

Virginia
Virginia has a data security breach notification law that protects unencrypted and unredacted personal information pertaining to Virginia residents[339].

Virgin Islands
The U.S. Virgin Islands has a data security breach notification law that protects the personal information of its residents. A consumer injured by a violation of the requirements may file a civil suit for damages[340].

Washington
Washington has a shredding requirement[341]. It also has a data security breach notification law that protects unencrypted data pertaining to state residents. Any customer injured by a failure to comply with the breach notification requirements can file a civil suit to recover damages[342].

West Virginia
West Virginia has a data security breach notification law that protects unencrypted and unredacted personal information pertaining to residents of the state[343].

Wisconsin
Wisconsin has a data security breach notification law that protects unredacted personal identifying information pertaining to residents of the state. The law applies to units of state and local government as well as to lenders and other businesses. It protects unencrypted, unredacted information and applies to out of state service providers providing services to state residences, as well as to service providers doing business in Wisconsin. Protection is not limited to state residents. The notice law includes biometric data and an individual's DNA profile in the definition of personal information[344]. Wisconsin has a shredding law. A consumer injured by violation of the shredding requirements may file a civil suit for resulting damages[345].

---

[337](Vt. Stat. Ann. Tit. 9, § 2430 Et Seq.).
[338]Vt. Statutes, Title 9, Chapter 62, § 2445, reproduced text accessible through index at http://www.leg.state.vt.us/statutes/sections.cfm?Title=09&Chapter=062, viewed December 10, 2008.
[339]Code of Virginia 18.2-186.6.
[340]Virgin Islands Code Title 14, Chapter 110, Subchapter 1, sections accessible through the index at http://www.michie.com/virginislands/lpext.dll?f=templates&fn=main-h.htm&cp=vicode.
[341]Title 19 RCW, sections 19.215.005 to 19.215.030. See summary at http://www.ncsl.org/programs/lis/privacy/02enact-finpriv.htm, viewed December 5, 2008.
[342](Wash. Rev. Code § 19.255.010).
[343] W.V. Code §§ 46A-2A-101 et seq.
[344]Wisc. Stat. 134.98, reproduced at http://www.legis.state.wi.us/statutes/Stat0134.pdf, viewed December 15, 2008.
[345]Wisc. Stat. 134.97, reproduced at http://www.legis.state.wi.us/statutes/Stat0134.pdf, viewed December 15, 2008.

Wyoming

Wyoming has a data security breach notification law that protects personal identifying information pertaining to state residents if either the consumer's name or the identifying information is unredacted. The requirements apply to any bank holding company, bank, savings and loan association, credit union or trust company doing business in the state. The Wyoming law protects the number of identity cards issued by Native American tribes[346].

[346]Wyo. Code Title 40, Article 5, §§ 40-12-501 and 502, accessible via index at http://michie.lexisnexis.com/wyoming/lpext.dll?f=templates&fn=main-h.htm, viewed December 15, 2008.