

**PRIVACY NOTICES**  
**GRAMM\_LEACH\_BLILEY ACT**  
**WHO, WHAT, WHERE, WHEN, WHY & HOW**  
**(AN INTERIM REVIEW)**

Nicholas M. Monaco, Esq.  
(573) 634-2522

The Gramm\_Leach-Bliley Act (GLB) requires that every financial institution inform its customers about the institution's information practices with respect to the gathering, use and disclosure of the customer's nonpublic personal financial information. Financial institutions covered include banks, brokerage houses, insurance companies, insurance agents and brokers and third party administrators.

There are several important questions that an insurer must answer at the start of its compliance efforts. First, what products does the insurer sell that are purchased primarily for personal, family or household purposes? GLB does not apply to insurance primarily purchased for other purposes. Second, are products really considered to be insurance under state law? Some states, for example, do not consider certain warranties to be insurance, while other states do. If the product is not deemed to be insurance in a given state, the insurer should refer to the GLB regulation adopted by the Federal Trade Commission. In case of variable products, the SEC's GLB regulation will have to be considered. Third, what, in fact, are the companies' practices regarding the use and disclosure of information? What persons and companies are allowed access to the information and for what purpose? What plans are there to share information with non-affiliated third parties to market products, any products? Are there written agreements with third parties to protect the information and use it only for the purpose they are given the information?

Complicating matters in the long run is the fact that GLB allows each state to add requirements as long as they do not contravene a GLB requirement. Fortunately the NAIC has adopted the NAIC Model Regulation and it appears most states will follow its requirements. GLB's notice requirement is like the hub of a wheel. Everything flows to and from the hub. The notice is the repository of the company's record information practices. And it had better be accurate. If it is not, the company faces the prospect of state officials, including state attorneys general alleging violations of trade practice restrictions and common law fraud, with attendant penalties and negative press.

A privacy notice as contemplated by GLB and addressed in NAIC Model Regulations is the means whereby a financial institution shall disclose its standards for the treatment of information and its practices either to permit or prevent disclosure of information. This requirement has been the subject of discourse both at the federal and state level. The genesis of the requirement is the recognition that multi-financial institutions deal with information required to conduct business for individuals and entities. The purpose of the notice appears to rest upon the protection of personal or otherwise confidential or restricted information which is needed to create the financial services required by the individual or entity. The intended result is to protect the information and authorize its use as and when required to deliver the service or product of the multi-financial service institutions. These objectives give rise to the need to know: Who? What? When? Why? How?

**Who?** The customer. Who is a Customer? It may be a consumer who has a relationship with the financial institution which provides financial products or services. The definition of a consumer is very broad and includes an individual or legal representative who seeks, obtains or has obtained an insurance product or service from a financial institution which is used primarily for personal, family or household purposes and about whom *nonpublic personal information* is obtained. The rights of the customer are well protected and disclosure of nonpublic financial information to an unaffiliated third party other than as authorized by the customer is actionable.

**What?** Information concerning the financial status and health of the customer seeking to obtain an insurance product or service from the financial institution or information that the financial institution *otherwise obtains* about a customer in connection with providing a financial product or service to that customer.

1. **Financial Information.** This information must be personally identifiable to obtain an insurance product or service. It may also include information about any transaction between the customer and the financial institution. This may include multiple transactions and not be limited to a particular or instant transaction. Included would be account balances and payment history as well as any information obtained either

directly or otherwise by the financial institution relating to the customer's financial dealings with the financial institution, as well as information on the Internet and consumer reports.

2. **Health Information.** Generally, nonpublic health information is that which identifies an individual who is the subject of the information and there is a reasonable basis to believe that the information could be used to identify the individual. The NAIC Health Information Privacy Model Act and the health privacy regulations proposed by the Department of Health and Human Services (HHS) define health information as any information or data that relates to the past, present or future mental or behavioral health or condition of an individual, the provision of health care to an individual or payment for provision of health care to an individual. The financial institution may not disclose nonpublic information about a customer unless the customer authorizes the disclosure. Such authority may be revoked at any time and may not remain valid longer than 24 months. This generally requires either a written or electronic authorization by the customer. There are, however, certain circumstances when a specific authorization is not required. These include claims administration, underwriting, loss control, risk management, sale, merger or transfer of all or part of the business of the financial institution or one of its operating units. Excluded is information concerning the list of names and addresses of customers of any entity which is not a financial institution. Also should the information not identify the customer, it is not included.

**When?** There are various times when privacy notices are required to be issued by a financial institution, as follows:

1. **Initial Privacy Notice.** Generally, a notice of the financial institution's Initial Privacy Notice practices must be no later than when the customer relationship is established. A customer relationship means a continuing relationship under which the financial institution offers one or more financial products to a customer used primarily for personal, family or household purposes.
2. **Annual Privacy Notice.** Notice of a financial institution's privacy practices must be issued not less than annually during the continuation of the customer relationship, generally referred to as the Annual Privacy Notice. Annually is defined as at least once in any consecutive twelve (12) month period. The twelve-month period must be applied consistently as to each customer. This notice is to be delivered to existing customers and must contain any changes or any additional information relative to any practice relating to new products purchased by the customer.
3. **Revised Privacy Notice.** At any time a new insurance product or service is purchased by an existing customer, a Revised Privacy Notice containing any additional information obtained is required to be delivered to the customer. This precludes the financial institution from waiting to apprise the customer until the Annual Notice is delivered. However, should the most recently delivered notice contain the information which would have to be added, no Revised Privacy Notice is required.

The financial institution must anticipate the disclosure of a *new category* of nonpublic personal financial information to any nonaffiliated third party. Likewise, a Revised Notice is required to be delivered before nonpublic personal financial information is disclosed to a new category of nonaffiliated third party. Also, a Revised Notice must be delivered before disclosure is made to a nonaffiliated third party of such information as to a former customer unless the former customer has exercised the opportunity to opt out regarding that disclosure.

4. **Opt Out Notices.** The Opt Out Notice must include the provision that the financial institution reserves the right to disclose nonpublic personal financial information about its customers to nonaffiliated third parties and that the customer has the right to opt out of that disclosure in accordance with a specified reasonable means to exercise the right to opt out.

The financial institution may provide the right to opt out of the financial institution's privacy practices at the time of the Initial Notice of privacy policy. If the right to opt out is not provided at the time of the Initial Notice but at some time thereafter, a copy of the Initial Notice must be delivered with the Opt Out Notice. When there exists a joint relationship between customers, Opt Out Notices must be delivered as the joint relationship may require.

A customer may exercise the right to opt out at any time; however if not exercised, the right to opt out shall extend until it is invoked by the customer.

Should the relationship between the customer and the financial institution be terminated for any reason, the opt out direction will continue to apply to information that was obtained during the course of the customer relationship. The Opt Out Notice also may allow the customer flexibility so that a customer may select certain personal financial information or certain nonaffiliated third parties to whom such information may not be disclosed. Only the information which the customer elects will be affected by the exercise of this right given to the customers by law or regulation.

Generally, in the absence of the delivery of the Initial Notice, the financial institution may not disclose nonpublic information about a customer to a nonaffiliated third party. Also, the financial institution must provide to the customer an Opt Out Notice so that the customer will have a reasonable opportunity to Opt Out. If the customer has not exercised the right to Opt Out, the customer's personal financial information may not be disclosed to a nonaffiliated third party.

In order to protect the customer, the financial institution must not either directly or through an affiliate disclose other than to a consumer reporting agency the policy number or access code for a customer's transaction for use in telemarketing, direct mail or electronic mail to the customer. The exception to this prohibition permits the disclosure to the financial institution's agent or service provider so long as there are reasonable restrictions.

**Why?** Security from misuse of private personal information. The customer's personal information might be used by unauthorized persons to the customer's detriment. Misuse of such information may create liability, embarrassment and loss of credit, as well as emotional and physical harm to the customer. There is also the frustration that results from annoying telemarketing and other electronic or personal tactics to gain access to the customer or the customer's property.

**How?** By Delivery. The financial institution which is required to deliver the various notices discharges its responsibility by distributing the required notices as specified by the customer. The delivery may be effected by mail at the last known address given by the customer or by the customer's designated electronic transmission system.

When there are joint or multiple product customers, care must be taken to be assured that the financial institution has discharged its responsibility. Likewise, should an issue be raised by the customer as to whether notices have been received, the financial institution is well advised to establish proof and a tracking system to assure itself that proper delivery has been made. This becomes significant also when there are several affiliated financial institutions.

### *General*

The Privacy Notice Requirements are required by both the new Federal and State Laws or Regulations. The NAIC is now adopting a Model Interim Regulation. The Executive and Plenary Committees of the NAIC did so on September 27, 2000. The Federal government regulations were adopted by the OCC, FDIC and OTS on February 2, 2000 to clarify Title V of the Gramm\_Leach\_Bliley Act. These regulations should be read with the understanding that these regulations interpret the legal obligations that GLB imposed by statute. On the other hand, the Federal Department of Health and Human Services (HHS) issued regulations on November 3, 1999 which are intended to establish legal obligations and their implementation.

In order to complete the regulatory oversight of privacy notices and other financial regulation by the various states, the process of adopting laws or regulations is under way. As of February 2001, thirty\_one (31) states have taken no action. A few states\_\_Arizona, Hawaii, Kansas, Missouri, and Nebraska\_\_have legislation pending. The states of Alabama, Colorado, Connecticut, District of Columbia, Illinois, Indiana, Iowa, Louisiana, New Hampshire, New York, Washington and Wisconsin have adopted Administrative Regulations.

Since both financial and health information are separately treated both on the Federal and State level, the laws and regulations relate to either or both. The states of Hawaii, Iowa and Louisiana cover *personal information generally*. The other states which have begun the process of adopting statutes or regulations through February 2001 cover financial and health information. It is anticipated that the states in which no action has been taken through February

2001 will begin the process of considering the regulation of privacy information. This is an evolving regulatory matter. The NAIC provides an update periodically to assist in compliance.

Final regulations were issued under Section 504(a) of GLB by the Federal Trade Commission on May 24, 2000 and the OCC on June 1, 2000. By this, the Federal government has taken the early initiative and these requirements exist. On the state level, the process is ongoing and the language of the statute or regulation adopted by the states should be carefully reviewed and compared with the Federal laws and regulations. Where there is an inconsistency, conflict of laws questions arise as well as the issue of Federal Preemption.

GLB, with one exception, does not impede the free flow of information. The exception is the sharing of information with a nonaffiliated company for a purpose that is not permitted in the extensive list of permissible sharing listed in the NAIC model. Under GLB a company may not share data with a nonaffiliated third to market that party's products unless there is a written joint marketing agreement in place, or the customer has had a reasonable opportunity and amount of time to prevent the disclosure, i.e., the opportunity to opt out. If a company determines it must or otherwise wants to grant its customers the right to opt out, it must have the programs in place to keep track of the customer's election for years to come.