Privacy Under the Gramm-Leach-Bliley Act

Apr 01 2000

Posted By: William E. Taibl

Practice Area: Banking and Commercial Finance

EXECUTIVE SUMMARY

This article discusses and addresses a number of issues related to the key definitions under the Gramm-Leach-Bliley Act and related proposed regulations. An understanding of these definitions is essential if a financial institution is to draft an effective and compliant privacy policy.

This article also provides helpful commentary on the implementation of the "opt out" concepts under the Act and proposed regulations applicable to consumers and customers in relationship to a financial institution's ability to disclose non-public personal information to non-affiliated third parties.

In very general terms and subject to various exceptions, a financial institution may not disclose nonpublic personal information to nonaffiliated third parties unless the following three requirements are satisfied: (i) an opt out notice satisfying the regulatory requirements is given to the consumer; (ii) the financial institution has given the consumer a reasonable opportunity to opt out of the disclosure before the time the financial institution discloses the information; and (iii) the consumer does not opt out.

A bank's privacy policies, including the implementation procedures, must be carefully crafted to ensure that they are consistent with the key definitions and appropriately implement the "opt out" rights of the financial institution's consumers and customers.

BACKGROUND

Privacy of consumer financial information has drawn a great deal of attention since the issue surfaced as one of the final controversial items to be resolved in the development of the financial services reform legislation, which resulted in the Gramm-Leach-Bliley Act of 1999 (the "Act"). The Act directed the primary financial institution regulatory agencies within the federal government to issue regulations to implement the privacy provisions of the Act.

In February, pursuant to this legislative mandate, the federal agencies published in the *Federal Register* proposed implementing regulations. The comment period on the proposed regulations expired on March 31, 2000.

On the surface, the concept of privacy of consumer financial information seems well intentioned and perhaps reasonably manageable. However, like so many legislative and regulatory initiatives and directives, the realization of the intended benefits becomes mired in the details of implementation. This Act and the proposed regulations are no exception to this unfortunate scenario.

Within the short life of the Act and even shorter life of the proposed regulations, much has been written about the intention of Congress as expressed in the privacy provisions of the Act. Citations to Congressional floor debate are already surfacing in efforts to add clarification to Congress' intent, and as part of the publication of the proposed regulations, the federal agencies are requesting comments on a significant number of issues which require clarification.

With this kind of backdrop, the Act and the proposed regulations provide fertile ground for commentary on almost every aspect of their implementation. A comprehensive analysis of the Act and proposed regulations would result in a book rather than an article. We have, therefore, for the purposes of this article elected to focus on a narrow, but very important aspect of the Act. In this article we will discuss key definitions and the planning and implementation issues related to the "opt out" rights of consumers and customers as they relate to the sharing of Nonpublic Personal Information ("NPPI") with Nonaffiliated Third Parties ("NATP").

DEFINITIONS

The key to understanding the "opt out" rights and to establishing a privacy policy and compliance program, which satisfies the requirements of the Act and the proposed regulations, is to have a thorough understanding of a handful of definitions. While all of the definitions must be carefully considered when developing a privacy policy and related compliance programs, the following terms require special attention:

Affiliate. This definition has significance since neither a consumer nor a customer has a right to opt out of information sharing with an affiliate. An affiliate means any company that controls, is controlled by, or is under common control with another company. The definition includes both financial institutions and entities that are not financial institutions.

Control. There are three concepts included within the definition of control, which are relevant to the understanding of the definition of "affiliate." Control of a company means: (i) ownership, control or a power to vote 25% or more of the outstanding shares of any class of voting securities of the company; or (ii) control in any manner over the election of a majority of directors, trustees or general partners (or individuals exercising similar functions of the company); or (iii) the power to exercise, directly or indirectly, the controlling influence over the management or policies of the company. The third concept is subject to further oversight by the federal agency having regulatory authority over the financial institution to determine what constitutes "controlling influence."

Nonaffiliated Third Party ("NATP"). This term means any person (which includes natural persons as well as corporate business entities) except (i) any affiliate of the financial institution, and (ii) a person employed jointly by a financial institution and any company that is not the financial institution's affiliate; however, the definition does include the other company that jointly employees the individual. Also, the definition includes any company that is an affiliate as a result of conducting merchant banking or investment banking activities or insurance company investment activities of the types described in specified provisions of the Bank Holding Company Act. The definition of NATP is critical in determining whether a financial institution has an obligation to provide notices of its privacy policy or to provide customers or consumers with an "opt out" right.

Consumer. This term means an individual who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family or household purposes, and that individual's legal representative. The definition includes six examples, which further attempt to clarify the breath of this definition. The Act and proposed regulations distinguish consumers from customers for the purposes of notice requirements. Not all consumers are customers. The financial institution is required to give a consumer specified notices only if the institution intends to disclose NPPI about the consumer to a NATP for a purpose that is not authorized by one of the various exceptions to the notice requirement. However, a financial institution must give customers notice of the institutions privacy policy at the time of establishing a customer relationship and annually thereafter during the continuation of that relationship. If a consumer never becomes a customer, the financial institution is not required to provide any notices to the consumer unless the institution intends to disclose NPPI about that consumer to a NATP outside of the specified exceptions to the notice requirements.

Customer. A customer is any consumer who has established a "customer relationship." "Customer relationship" is also a defined term. A consumer becomes a customer of the financial institution at the time of entering into a continuing relationship with the institution.

Customer Relationship. This definition is key in understanding the definition of customer. Customer relationship means a continuing relationship between a consumer and the financial institution in which the financial institution provides one or more financial products or services to the consumer. The definition attempts to clarify that it does not cause a consumer to become a customer based upon isolated transactions. The expectation is that there would be a relationship of a continuing nature. Through examples within this definition, the proposed regulations identify a number of common relationships, which would be deemed to be customer relationships and a number of transactions, which would not be considered as establishing a continuing relationship. One of the examples confirms that a consumer withdrawing cash from a financial institution's ATM or purchasing a cashier's check or money order would not become a customer by reason of such transactions. The proposed regulations also make it clear that if the financial institution completely severs its relationship with the customer, the consumer will cease to be a customer. However, there are a number of unresolved issues concerning what constitutes the severance of a continuing relationship which would cause the consumer to cease to be a customer.

Nonpublic Personal Information ("NPPI"). This is an extremely important definition which has generated a great deal of discussion and debate. The regulatory agencies, because of the importance of this definition and the various ways that it may be interpreted, not only have requested comments concerning the appropriate scope of the definition, but have also proposed two alternative definition concepts referred to in the proposed regulations as Alternative A and Alternative B. Both alternative definitions rely upon the additional defined terms of "Personally Identifiable Financial Information" and "Publicly Available Information." In general, NPPI means Personally Identifiable Financial Information that (i) is provided by a consumer to a financial institution, (ii) results from any transaction between the financial institution and the consumer involving a financial product or service or (iii) is otherwise obtained by the financial institution in connection with providing a financial service or product to the consumer. Alternative A provides a much broader definition of NPPI and more information will be treated as NPPI under this alternative than would be the case under Alternative B. In order for information to be considered publicly available under Alternative A, the information must, in fact, be obtained by the financial institution from government records, widely distributed media or government mandated disclosures. The fact that the information is available from those sources is immaterial if the financial institution does not actually obtain the information from one of those sources. Under Alternative B, the definition of NPPI will be narrower. If the information is lawfully available to the general public, then it will be publicly available and excluded from the scope of NPPI, regardless of whether the institution obtained it from a publicly available source, unless it is part of a list of consumers that is derived using personally identifiable financial information.

Personally Identifiable Financial Information. The proposed regulations define Personally Identifiable Financial Information, although there is no definition provided in the Act. This definition is extremely broad and treats any personally identifiable information as financial if it is obtained by a financial institution in connection with providing a financial product or service to a consumer. With this definition, information obtained in connection with providing a financial product or service may be deemed to be "Personally Identifiable Financial Information," even though the information would not traditionally be considered financial. The proposed regulations do provide a series of examples in an effort to further clarify the scope of this definition. There are differences between this definition under Alternative A and Alternative B, which support the differences in the definition of "NPPI" under those two alternatives as noted above in the comments to the definition of "NPPI."

Publicly Available Information. The definitions of this term under Alternative A and Alternative B are very similar with only one major exception. Alternative A does not treat information as publicly available unless it is obtained from one of the public sources listed in the proposed regulations. Alternative B treats information as publicly available if it could be obtained from one of the public sources listed in the regulations, even if it was obtained from a source not listed in the definition. The public sources that are identified within the definition consist of the following: (i) federal, state or local government records; (ii) widely distributed media; or (iii) disclosures to the general public that are required to be made by federal, state or local law. To simplify compliance and record keeping requirements and to reduce the scope of information, which is considered to be NPPI, Alternative B would be a better option from the perspective of most financial institutions.

TRIGGERING THE RIGHT TO OPT OUT

The initial and annual notices that a financial institution is required to provide about its privacy policies must include an explanation of the right of the consumer to opt out of the disclosure of NPPI to NATP's. The notice must also include a description of the methods by which the consumer may exercise that right.

Subject to specified exceptions, a financial institution may not, directly or through any affiliate, disclose any NPPI about the consumer to a NATP unless the following requirements are satisfied: (i) an opt out notice satisfying the regulatory requirements is given to the consumer; (ii) the financial institution has given the consumer a reasonable opportunity to opt out of the disclosure before the time (the proposed regulations suggest 30 days) the financial institution discloses the information to the NATP; and (iii) the consumer does not opt out.

Opt out means a direction by the consumer that the financial institution not disclose NPPI about the consumer to a NATP, other than as permitted by specific exceptions as set forth in the Act and proposed regulations. It is permissible for a financial institution to establish a policy which would permit the consumer to select certain NPPI or certain NATP's with respect to which a consumer wishes to opt out rather than requiring the consumer to opt out under all circumstances.

Since the focus of the privacy provisions of the Act is to generally prohibit a financial institution from sharing NPPI about a consumer with a NATP unless the institution provides the consumer with the required notice of the opt out right, any time the institution intends to provide NPPI to a NATP, the opt out right is triggered subject to a series of exceptions noted in both the Act and the proposed regulations. Without the exceptions, the general rule against disclosure coupled with the opt out right would make the conduct of financial transactions nearly impossible.

OPT OUT EXCEPTIONS

Three separate sections of the proposed regulations address exceptions to the opt out requirements. Under the first set of exceptions, a consumer does not have the right to opt out from the disclosure of NPPI to a NATP for use by the third party to perform services for, or functions on behalf of, the financial institution, including the marketing of the financial institution's own products and services. Also excluded from the opt out right would be the sharing of such information with NATP's for the purposes of marketing financial products and services offered pursuant to a joint agreement between two or more financial institutions. Both of these exceptions are subject to specific additional conditions.

First, the financial institution must fully disclose to the consumer that it may provide this information to the NATP before the information is shared.

Second, the financial institution must enter into a contract with the third party that requires the third party to maintain the confidentiality of the shared information. The agreement with the third party must also limit the third party's use of the information solely for the purposes for which the information was disclosed or for such other purposes as may be permitted by other exceptions set forth in the regulations.

If the joint agreement concept is being relied upon, the joint agreement must be related to joint marketing activities and must be between or among only financial institutions. The joint marketing agreement concept must be documented in writing and the participating financial institutions must jointly offer, endorse or sponsor a financial product or service.

The opt out rights also do not apply if the financial institution discloses NPPI under other specified circumstances. These situations are described, with some detail, in the proposed regulations under Sections ____.10 and ____.11. We have attached copies of those two proposed sections for your convenient reference.

PLANNING AND IMPLEMENTATION ISSUES

Prior to drafting a privacy policy or establishing compliance standards and procedures related to the opt out right, it is essential for the financial institution to determine what information, if any, it collects that would be subject to the opt out right and the extent to which any of the exceptions to the opt out right may be applicable. In doing this analysis and when considering the disclosures that will be made in the financial institutions privacy policy, it should be noted that the Act does not require the financial institution to list the categories of persons to whom information may be disclosed pursuant to the exceptions set out in the proposed regulations at Sections ___.10 and ___.11. The proposed regulations provide that a financial institution is required only to inform consumers that the financial institution makes disclosures as permitted by law to NATP's in addition to the NATP's described in the notice. The "permitted by law" reference is intended to cover the exceptions in Sections ___.10 and ___.11. Notwithstanding this permitted generic reference to the exceptions, the financial institution may wish to consider including a statement in its notice that nonexclusively identifies some of the more basic exceptions to minimize the risk that the consumer may have expectations of greater confidentiality than what is feasible to effectively conduct the consumers transactions with the financial institution.

It is also essential for the financial institution to clearly establish methods by which the consumer may opt out and the financial institution's procedures for tracking and segregating the Non-Personal Financial Information that is not subject to disclosure by reason of the consumers exercise by his or her right to opt out. The institution's data processing capabilities must be carefully considered when establishing these methods and procedures.

Examples within the proposed regulations identifying methods by which a consumer may opt out include providing check off boxes in prominent locations on the notices, including a reply form together with the opt out notice or, in the event of electronic transactions, using electronic mail or a process at the financial institutions website if the consumer agrees to the electronic delivery of information. The proposed regulations indicate that a financial institution does not provide a reasonable means of opting out if the only means of opting out is for the consumer to write his or her own letter to the financial institution to exercise the opt our right.

A consumer may exercise the right to opt out at any time. The financial institution receiving the opt out direction from the consumer must comply with the direction as soon as reasonably practicable. The financial institution will need to determine the amount of time it would take to process the opt out notifications which it receives to ensure that there are no improper disclosures of NPPI. At the present time the proposed regulations do not establish a specific response time for the financial institutions to implement a customers election to opt out.

In the event the financial institution elects to provide a partial opt out alternative for its consumers, the financial institution will need to ensure that its data processing systems can segregate the information accordingly.

In the event a financial institution changes its disclosure policies, the financial institution will be required to provide a revised notice and a new opportunity to opt out before disclosing NPPI to a NATP. The institution will need to wait a reasonable period of time subsequent to the issuance of the revised notice before releasing the information. The information may only be released if the consumer does not opt out of the disclosure. Again, the institution will need to have a means to track the receipt of any opt out elections made by its consumers.

The proposed regulations do provide several examples of circumstances, which would require a change in terms notice.

A consumer's direction to opt out is effective until revoked by the consumer in writing, or if the consumer agrees, in electronic form.

At the present time, there is no clear direction in the proposed regulations on how financial institutions are to handle joint accounts. The primary issue is whether all parties to an account must opt out before the opt out becomes effective. If all the parties do not opt out, what information can be shared concerning the account? These issues remain open for review and comment. Administratively, the best solution to this problem would be to permit the financial institutions to require all parties on joint accounts to opt out to make the opt out effective. Most other solutions to this problem would result in significant problems for the financial institutions in identifying which information could be shared and which information would need to remain confidential to avoid the risk of improper disclosure. Absent the ability to require all parties to opt out to make the opt out effective, the likely safe harbor for the financial institutions would be to treat the entire account relationship as confidential in the same manner as if all parties had opted out.

CONCLUSION

This article has only scratched the surface of the full spectrum of issues related to the implementation of the privacy provisions under the Act and the proposed regulations. As financial institutions begin to work with the privacy concepts as well as with the specific language of the Act and proposed regulations, numerous issues of interpretation and implementation will continue to arise. This article is based upon the language of the Act, portions of the reported legislative history for the Act, the proposed regulations as issued by the agencies in February and other collateral sources which have been published providing commentary on these privacy issues. As noted in this article, the agencies have asked for comment concerning the proposed regulations. In many cases, it is anticipated that the final regulations will be substantially similar to the proposed regulations; however, it is also expected that there will be revisions including the ultimate decision on the part of the regulators concerning which alternative to implement in relationship to the definition of NPPI.

Financial institutions should now be working on their internal due diligence to determine the sources of NPPI which they collect and use, as well as to determine the NATP's with whom they share this information. This examination must also take into consideration the applicable exceptions to the notice and opt out rights.

Systems will need to be reviewed to determine the ability of the financial institution to segregate the information that it will not be permitted to share and to maintain the confidentiality of such information.

Only after these matters have been considered and there is a thorough understanding of the Act and regulations, can the financial institutions safely finalize their privacy policy and compliance procedures.

We fully expect this whole process to be a dynamic one which will be constantly changing as new information becomes available concerning the interpretation of the Act and the proposed regulations and the relationship of this new law to the functional capabilities of the financial institutions.
