

Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)¹

Introduction

On November 12, 1999, President Clinton signed into law the Gramm-Leach-Bliley Act (the Act or GLBA). Title V, Subtitle A of the Act governs the treatment of nonpublic personal information about consumers by financial institutions. Section 502 of the Subtitle, subject to certain exceptions, prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties, unless the institution satisfies various notice and opt-out requirements, and provided that the consumer has not elected to opt out of the disclosure. Section 503 requires the institution to provide notice of its privacy policies and practices to its customers. Section 504 authorizes the issuance of regulations to implement these provisions.

Accordingly, on June 1, 2000, the four federal bank and thrift regulators published substantively identical regulations implementing provisions of the Act governing the privacy of consumer financial information. The regulations establish rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information, as summarized below. A more complete discussion appears later in this chapter.

- A financial institution must provide a notice of its privacy policies, and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information, to a nonaffiliated third party if the disclosure is outside of the exceptions in sections 13, 14 or 15 of the regulations.
- Regardless of whether a financial institution shares nonpublic personal information, the institution must provide notices of its privacy policies to its customers.
- A financial institution generally may not disclose customer account numbers to any nonaffiliated third party for marketing purposes.
- A financial institution must follow reuse and redisclosure limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

The privacy regulations became effective on November 13, 2000. Compliance was required as of July 1, 2001.

Definitions and Key Concepts

In discussing the duties and limitations imposed by the regulations, a number of key concepts are used. These concepts include “financial institution”; “nonpublic personal

information”; “nonaffiliated third party”; the “opt out” right and the exceptions to that right; and “consumer” and “customer.” Each concept is briefly discussed below. A more complete explanation of each appears in the regulations.

“**Financial institution**” is any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities, as determined by section 4(k) of the Bank Holding Company Act of 1956. Financial institutions can include banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents².

“**Nonpublic personal information**” generally is any information that is not publicly available and that:

- a consumer provides to a financial institution to obtain a financial product or service from the institution;
- results from a transaction between the consumer and the institution involving a financial product or service; or
- a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

Information is publicly available if an institution has a reasonable basis to believe that the information is lawfully made available to the general public from government records, widely distributed media, or legally required disclosures to the general public. Examples include information in a telephone book or a publicly recorded document, such as a mortgage or securities filing.

Nonpublic personal information may include individual items of information as well as lists of information. For example, nonpublic personal information may include names, addresses, phone numbers, social security numbers, income, credit score, and information obtained through Internet collection devices (i.e., cookies).

There are special rules regarding lists. Publicly available information would be treated as nonpublic if it were included on a list of consumers derived from nonpublic personal information. For example, a list of the names and addresses of a financial institution's depositors would be nonpublic personal information even though the names and addresses might be published in local telephone directories because the list is derived from the fact that a person has a deposit account with an institution, which is not publicly available information.

However, if the financial institution has a reasonable basis to believe that certain customer relationships are a matter of public record, then any list of these relationships would be considered publicly available information. For instance, a list

¹ This section fully incorporates the examination procedures issued under DCA RD Memo 01-002: Interagency Examination Procedures for Reviewing Compliance with Part 332-Privacy of Consumer Financial Information.

² These regulators are the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.