RESCINDED

This document and any attachments are superseded by Comptroller's Handbook - Consumer Compliance Examination - Privacy of Consumer Financial Information.

Privacy of Consumer Financial Information

Background and Overview

On November 12, 1999, President Clinton signed into law the Gramm-Leach-Bliley Act (the Act). 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.

LINKS
Program
Questionnaire
Appendix A

Accordingly, on June 1, 2000, the four federal bank and thrift regulators[1] 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 document.

- 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.

[1] 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.

The privacy regulations became effective on November 13, 2000. Compliance is 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:

A "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 agents.[2]

Nonpublic Personal Information:

"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).

[2] Certain functionally-regulated subsidiaries, such as brokers, dealers, and investment advisers will be subject to privacy regulations issued by the Securities and Exchange Commission. Insurance entities may be subject to privacy regulations issued by their respective state insurance authorities.

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 of mortgage customers where the mortgages are recorded in public records would be considered publicly available information. The institution could provide a list of such customers, and include on that list any other publicly available information it has about the customers on that list without having to provide notice or opt out.

Nonaffiliated Third Party:

A "nonaffiliated third party" is any person except a financial institution's affiliate or a person employed jointly by a financial institution and a company that is not the institution's affiliate. An "affiliate" of a financial institution is any company that controls, is controlled by, or is under common control with the financial institution.

Opt Out Right and Exceptions:

The Right

Consumers must be given the right to "opt out" of, or prevent, a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party, unless an exception to that right applies. The exceptions are detailed in sections 13, 14, and 15 of the regulations and described below.

As part of the opt out right, consumers must be given a reasonable opportunity and a reasonable means to opt out. What constitutes a *reasonable opportunity to opt out* depends on the circumstances surrounding the consumer's transaction, but a consumer must be provided a reasonable amount of time to exercise the opt out right. For example, it would be reasonable if the financial institution allows 30 days from the date of mailing a notice or 30 days after customer acknowledgement of an electronic notice for an opt out direction to be returned. What constitutes a *reasonable means to opt out* may include check-off boxes, a reply form, or a toll-free telephone number, again depending on the circumstances surrounding the consumer's transaction. It is not reasonable to require a consumer to write his or her own letter as the only means to opt out.

The Exceptions

Exceptions to the opt out right are detailed in sections 13, 14, and 15 of the regulations. Financial institutions need not comply with opt-out requirements if they limit disclosure of nonpublic personal information:

- To a nonaffiliated third party to perform services for the financial institution or to function on its behalf, including marketing the institution's own products or services or those offered jointly by the institution and another financial institution. The exception is permitted only if the financial institution provides notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. The contract must provide that the parties to the agreement are jointly offering, sponsoring, or endorsing a financial product or service. However, if the service or function is covered by the exceptions in section 14 or 15 (discussed below), the financial institution does not have to comply with the additional disclosure and confidentiality requirements of section 13. Disclosure under this exception could include the outsourcing of marketing to an advertising company. (Section 13)

- As necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or under certain other circumstances relating to existing relationships with customers. Disclosures under this exception could be in connection with the audit of credit information, administration of a rewards program, or to provide an account statement. (Section 14)

- For specified other disclosures that a financial institution normally makes, such as to protect against or prevent actual or potential fraud; to the financial institution's attorneys, accountants, and auditors; or to comply with applicable legal requirements, such as the disclosure of information to regulators. (Section 15)

Consumer and Customer:

The distinction between consumers and customers is significant because financial institutions have additional disclosure duties with respect to customers. All customers covered under the regulation are consumers, but not all consumers are customers.

A "consumer" is an individual, or that individual's legal representative, who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes.

A "financial service" includes, among other things, a financial institution's evaluation or brokerage of information that the institution collects in connection with a request or an application from a consumer for a financial product or service. For example, a financial service includes a lender's evaluation of an application for a consumer loan or for opening a deposit account even if the application is ultimately rejected or withdrawn.

Consumers who are not customers are entitled to an initial privacy and opt out notice only if their financial institution wants to share their nonpublic personal information with nonaffiliated third parties outside of the exceptions.

A "customer" is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship between a consumer and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

- For example, a customer relationship may be established when a consumer engages in one of the following activities with a financial institution:

  — maintains a deposit or investment account;

  — obtains a loan;

  — enters into a lease of personal property; or

  — obtains financial, investment, or economic advisory services for a fee.

Customers are entitled to initial and annual privacy notices regardless of the information disclosure practices of their financial institution.

There is a special rule for loans. When a financial institution sells the servicing rights to a loan to another financial institution, the customer relationship transfers with the servicing rights. However, any information on the borrower retained by the institution that sells the servicing rights must be accorded the protections due any consumer.

- Note that isolated transactions alone will not cause a consumer to be treated as a customer. For example, if an individual purchases a bank check from a financial institution where the person has no account, the individual will be a consumer but not a customer of that institution because he or she has not established a customer relationship. Likewise, if an individual uses the ATM of a financial institution where the individual has no account, even repeatedly, the individual will be a consumer, but not a customer of that institution.

Financial Institution Duties

The regulations establish specific duties and limitations for a financial institution based on its activities. Financial institutions that intend to disclose nonpublic personal information outside the exceptions will have to provide opt out rights to their customers and to consumers who are not customers. All financial institutions have an obligation to provide an initial and annual notice of their privacy policies to their customers. All financial institutions must abide by the regulatory limits on the disclosure of

account numbers to nonaffiliated third parties and on the redisclosure and reuse of nonpublic personal information received from nonaffiliated financial institutions.

A brief summary of financial institution duties and limitations appears below. A more complete explanation of each appears in the regulations.

Notice and Opt Out Duties to Consumers:

If a financial institution intends to disclose nonpublic personal information about any of its consumers (whether or not they are customers) to a nonaffiliated third party, and an exception does not apply, then the financial institution must provide to the consumer:

- an initial notice of its privacy policies;
- an opt out notice (including, among other things, a reasonable means to opt out); and
- a reasonable opportunity, before the financial institution discloses the information to the nonaffiliated third party, to opt out.

The financial institution may not disclose any nonpublic personal information to nonaffiliated third parties except under the enumerated exceptions unless these notices have been provided and the consumer has not opted out. Additionally, the institution must provide a *revised notice* before the financial institution begins to share a new category of nonpublic personal information or shares information with a new category of nonaffiliated third party in a manner that was not described in the previous notice.

Note that a financial institution need not comply with the initial and opt-out notice requirements for consumers who are not customers if the institution limits disclosure of nonpublic personal information to the exceptions.

Notice Duties to Customers:

In addition to the duties described above, there are several duties unique to customers. In particular, regardless of whether the institution discloses or intends to disclose nonpublic personal information, a financial institution must provide notice to its customers of its privacy policies and practices at various times.

- A financial institution must provide an initial notice of its privacy policies and practices to each customer, not later than the time a customer relationship is established. Section 4(e) of the regulations describes the exceptional cases in which delivery of the notice is allowed subsequent to the establishment of the customer relationship.
- A financial institution must provide an *annual notice* at least once in any period of 12 consecutive months during the continuation of the customer relationship.

- Generally, new privacy notices are not required for each new product or service. However, a financial institution must provide a *new notice* to an existing customer when the customer obtains a new financial product or service from the institution, if the initial or annual notice most recently provided to the customer was not accurate with respect to the new financial product or service.

- When a financial institution does not disclose nonpublic personal information (other than as permitted under section 14 and section 15 exceptions) and does not reserve the right to do so, the institution has the option of providing a simplified notice.

Requirements for Notices

Clear and Conspicuous. Privacy notices must be clear and conspicuous, meaning they must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. The regulations do not prescribe specific methods for making a notice clear and conspicuous, but do provide examples of ways in which to achieve the standard, such as the use of short explanatory sentences or bullet lists, and the use of plain-language headings and easily readable typeface and type size. Privacy notices also must accurately reflect the institution's privacy practices.

Delivery Rules. Privacy notices must be provided so that each recipient can reasonably be expected to receive actual notice in writing, or if the consumer agrees, electronically. To meet this standard, a financial institution could, for example, (1) hand-deliver a printed copy of the notice to its consumers, (2) mail a printed copy of the notice to a consumer's last known address, or (3) for the consumer who conducts transactions electronically, post the notice on the institution's web site and require the consumer to acknowledge receipt of the notice as a necessary step to completing the transaction.

For customers only, a financial institution must provide the initial notice (as well as the annual notice and any revised notice) so that a customer may be able to retain or subsequently access the notice. A written notice satisfies this requirement. For customers who obtain financial products or services electronically, and agree to receive their notices on the institution's web site, the institution may provide the current version of its privacy notice on its web site.

Notice Content. A privacy notice must contain specific disclosures. However, a financial institution may provide to consumers who are not customers a "short form" initial notice together with an opt out notice stating that the institution's privacy notice is available upon request and explaining a reasonable means for the consumer to obtain it. The following is a list of disclosures regarding nonpublic personal information that institutions must provide in their privacy notices, as applicable:

1. categories of information collected;

2. categories of information disclosed;

3. categories of affiliates and nonaffiliated third parties to whom the institution may disclose information;

4. policies with respect to the treatment of former customers' information;

5. information disclosed to service providers and joint marketers (Section 13);

6. an explanation of the opt out right and methods for opting out;

7. any opt out notices the institution must provide under the Fair Credit Reporting Act with respect to affiliate information sharing;

8. policies for protecting the security and confidentiality of information; and

9. a statement that the institution makes disclosures to other nonaffiliated third parties as permitted by law (Sections 14 and 15).

Limitations on Disclosure of Account Numbers:

A financial institution must not disclose an account number or similar form of access number or access code for a credit card, deposit, or transaction account to any nonaffiliated third party (other than a consumer reporting agency) for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

The disclosure of encrypted account numbers without an accompanying means of decryption, however, is not subject to this prohibition. The regulation also expressly allows disclosures by a financial institution to its agent to market the institution's own products or services (although the financial institution must not authorize the agent to directly initiate charges to the customer's account). Also not barred are disclosures to participants in private-label or affinity card programs, where the participants are identified to the customer when the customer enters the program.

Redisclosure and Reuse Limitations on Nonpublic Personal Information Received:

If a financial institution receives nonpublic personal information from a nonaffiliated financial institution, its disclosure and use of the information is limited.

- For nonpublic personal information received under a section 14 or 15 exception, the financial institution is limited to:

  — Disclosing the information to the affiliates of the financial institution from which it received the information;

— Disclosing the information to its own affiliates, who may, in turn, disclose and use the information only to the extent that the financial institution can do so; and

— Disclosing and using the information pursuant to a section 14 or 15 exception (for example, an institution receiving information for account processing could disclose the information to its auditors).

- For nonpublic personal information received other than under a section 14 or 15 exception, the recipient's use of the information is unlimited, but its disclosure of the information is limited to:

  — Disclosing the information to the affiliates of the financial institution from which it received the information;

  — Disclosing the information to its own affiliates, who may, in turn disclose the information only to the extent that the financial institution can do so; and

  — Disclosing the information to any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which it received the information. For example, an institution that received a customer list from another financial institution could disclose the list (1) in accordance with the privacy policy of the financial institution that provided the list, (2) subject to any opt out election or revocation by the consumers on the list, and (3) in accordance with appropriate exceptions under sections 14 and 15.

Other Matters

Fair Credit Reporting Act

The regulations do not modify, limit, or supersede the operation of the Fair Credit Reporting Act.

State Law

The regulations do not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that it is inconsistent with the regulations. A state statute, regulation, order, etc. is consistent with the regulations if the protection it affords any consumer is greater than the protection provided under the regulations, as determined by the FTC.

Grandfathered Service Contracts

Contracts that a financial institution has entered into, on or before July 1, 2000, with a nonaffiliated third party to perform services for the financial institution or functions on its behalf, as described in section 13, will satisfy the confidentiality requirements of section 13(a)(1)(ii) until July 1, 2002, even if

the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information.

Guidelines Regarding Protecting Customer Information

The regulations require a financial institution to disclose its policies and practices for protecting the confidentiality, security, and integrity of nonpublic personal information about consumers (whether or not they are customers). The disclosure need not describe these policies and practices in detail, but instead may describe in general terms who is authorized to have access to the information and whether the institution has security practices and procedures in place to ensure the confidentiality of the information in accordance with the institution's policies.

The four federal bank and thrift regulators have published guidelines, pursuant to section 501(b) of the Gramm-Leach-Bliley Act, that address steps a financial institution should take in order to protect customer information. The guidelines relate only to information about customers, rather than all consumers. Compliance examiners should consider the findings of a 501(b) inspection during the compliance examination of a financial institution for purposes of evaluating the accuracy of the institution's disclosure regarding data security.