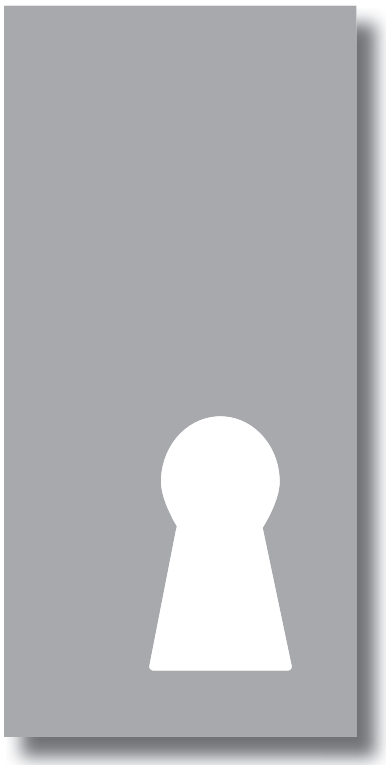
Comptroller of the Currency
Administrator of National Banks

Privacy Rule

Small Bank Compliance Guide



Office of the Comptroller of the Currency

December 2001

Index

Privacy Compliance Pointers for Community Bankers

The OCC is publishing the Small Bank Compliance Guide (the Guide) to help community bankers comply with the Gramm-Leach-Bliley Act privacy rule.[1] The Guide consists of:

- Part I, a summary of the privacy rule.

- Part II, a privacy preparedness checklist that the OCC first issued in January 2001 as Advisory Letter 2001-2. Although initially designed to help banks prepare for the privacy rule's mandatory compliance date, July 1, 2001, the checklist can assist you in deciding where to devote your compliance resources.

- Part III, a series of frequently asked questions and answers prepared by an interagency group to address issues the group believed would interest community banks and other small financial institutions.[2]

In complying with the privacy rule, you should note several important considerations about your basic obligations, marketing arrangements, and customer opt out rights. These are discussed briefly as follows and cross-reference the relevant sections of the Guide so that you may learn more about them.

Your basic obligations

You have an obligation to:

- Develop a privacy notice that explains how you collect, safeguard, and share nonpublic personal information about your customers.

---

[1] 12 CFR 40. The privacy rule was published jointly on June 1, 2000 by the OCC, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision to implement subpart A of Title V of the Gramm-Leach-Bliley Act. The National Credit Union Administration, the Federal Trade Commission, the Securities and Exchange Commission, and the Commodity Futures Trading Commission each published substantially similar rules to those issued by the banking agencies.

The Guide satisfies our obligations under the Small Business Regulatory Enforcement Fairness Act of 1996. Pub. L. 104-121, Mar. 29, 1996, 110 Stat. 857-862.

[2] The OCC is issuing this series of Frequently Asked Questions jointly with the Federal Reserve Board, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. In preparing these questions and answers, staff of the agencies consulted with the Securities and Exchange Commission, the Federal Trade Commission, and the Commodity Futures Trading Commission.

- Make privacy notices *clear and conspicuous*. The information in your notices should be easy to find and to understand.

- Deliver notices to your customer. The method of delivery you choose for any customer must be reasonable for that person. It would be unreasonable, for instance, to send electronic notices to customers who conduct their transactions with you in person.

NOTE: The following techniques are effective in providing clear and conspicuous notices:

- Use simple language instead of regulatory or legal terms.
- Use short sentences and precise explanations.
- Use an easy to understand question-and-answer format to explain key concepts.
- Explain at the beginning of the notice the customers' opt out rights.
- Use captions that describe the materials in plain language, such as "You Have a Right To Opt Out."
- Use boldface sparingly or for emphasis.
- Use easy-to-read typefaces and sizes.
- Place electronic links to privacy notices at the top of your Web site pages.

- You may be able to give your customers *simplified privacy notices* and reduce your compliance burdens significantly under the rule. A simplified notice is one that contains only three disclosures:
  - The categories of nonpublic personal information that you collect.
  - Your policies for safeguarding nonpublic personal information.
  - A statement that you share nonpublic personal information with third parties as permitted by law.

- In general, you can use this kind of simplified privacy notice if you share your customers' nonpublic personal information only for routine business purposes. Some examples of information sharing for routine business purposes are to:
  - Maintain or service consumer accounts.
  - Process credit cards or checks.
  - Collect debts.
  - Print customer checks.

  Other examples include sharing information with:
  - Law enforcement officials.
  - Regulators.
  - Credit bureaus.

NOTE: Marketing is not a routine business purpose. If you share customer information for marketing, your privacy notices will be more complex, and you may have to provide your customers with opt out rights.

For additional information about privacy notices, see the Summary of OCC Privacy Rule, pages 7-14, and Frequently Asked Questions, beginning on page 23. You can find a discussion of the exceptions that permit you to share information for routine business purposes without providing your customers with opt out rights in the Summary of OCC Privacy Rule, page 13, and Frequently Asked Questions, section I.

- Marketing arrangements You may share your customers' nonpublic personal information with marketing partners without offering consumer opt out rights, only if:
  - The product or service you provide with your marketing partner is financial.
  - Your marketing partner is a financial institution.
  - You have a contract with your partner that shows that you will jointly offer, endorse, or sponsor the financial product or service.
  - Your contract limits your partner's use or further sharing of your customers' nonpublic personal information.
  - You provide your customers with a complete privacy notice, rather than a simplified one. This will include a separate statement about your information sharing arrangements with your marketing partners.

- If your marketing arrangements do not qualify for the exception in the rule, you must provide your customers with an opt out notice, in addition to giving them a complete privacy notice.

NOTE: You may not share customer account numbers with marketers (unless they are your *agents* offering *your* own products or services to your customers and you do not allow them to process charges to your customers' accounts). This prohibition extends to your arrangements with marketing partners. You may not give customer account numbers to a marketer either to conduct the initial solicitation or to process a charge for the product or service marketed.

For further discussion about information sharing arrangements with marketing partners and the prohibition against disclosing customer account numbers, see the Summary of OCC Privacy Rule, pages 13-14, and Frequently Asked Questions, sections H and J.

Opt out rights

- You must provide your customers with opt out rights if you share your customers' nonpublic personal information with third parties in situations other than for routine business purposes or in connection with qualifying marketing arrangements. Opt out rights include:
  - A clear and conspicuous notice describing the right and method to opt out.
  - A reasonable means for customers to opt out.
  - A reasonable opportunity for customers to opt out.

- Examples of *reasonable means* include a toll-free telephone number, a check-off box on a relevant form, or a process at the bank's Web site for customers who agree to electronic delivery of notices. You may not require your customers to write their own letter as their only way to opt out.

- You provide a *reasonable opportunity* to opt out, for example, if you give your customer 30 days to opt out from the date you mailed the notice.

NOTE: Your customer has the right to opt out at *any time*. That means that even if your customer does not opt out within the initial 30-day period, you must still process his or her opt out election anytime you receive it. You must process your customer's opt out election as soon as it is *reasonably practicable*.

For further information about opt out rights, see the Summary of OCC Privacy Rule, pages 11-12, and Frequently Asked Questions, sections E and F.

Part I — Summary of OCC Privacy Rule

The Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision issued an interagency final regulation (rule) to implement provisions of the Gramm-Leach-Bliley Act (GLBA) that protect the privacy of consumers' nonpublic personal information. The rule was the product of an interagency working group, and similar rules were issued by the Federal Trade Commission, the Securities and Exchange Commission, the Commodity Futures Trading Commission and the National Credit Union Administration.

Nonpublic personal information

The rule implements the requirements of the GLBA that banks (and other types of "financial institutions," including securities firms, insurance agents, and insurance underwriters) notify consumers about their privacy policies and allow consumers to opt out of information sharing between the bank and certain nonaffiliated third parties.

The notice requirement and opt out right pertain to "nonpublic personal information" about consumers. Generally, nonpublic personal information is "personally identifiable financial information" that is not "publicly available."

The rule treats *any* information as "personally identifiable financial information," if it is provided by a consumer to obtain a financial product or service, results from a transaction with a bank involving a financial product or service, or is obtained by the bank in connection with providing a financial product or service to the consumer.

The rule excludes from the definition of "nonpublic personal information" information that is "publicly available." Information will be treated as publicly available if a bank has a "reasonable basis" to believe that the information is made available lawfully to the general public from government records, widely distributed media, or disclosures required by law. A bank may not assume that a consumer's information is publicly available, but must determine that the information is of the type available to the general public and whether a person can direct that the information not be publicly available (for example, an unlisted telephone number). If a person can prevent information from being made publicly available, a bank must determine whether the consumer has done so.

Under the rule, information obtained over the Internet will be considered publicly available if it is made available lawfully on a site that is accessible to the general public on an unrestricted basis. The payment of a fee or the use of a password does not necessarily restrict access to a Web site as long as access is

available to the general public. A site, such as a "look up" service, that makes available personal information (that may combine publicly available and confidential information on a particular person) compiled in response to a specific request, is not available to the general public on an unrestricted basis.

Publicly available information, however, is treated as "nonpublic personal information" when it is included on a list, description, or other grouping of consumers, if derived from personally identifiable financial information that is not publicly available. For example, the rule would cover all of the information on a list of depositors provided by the bank. This would include publicly available information, such as names and addresses. In this example, the list and information are derived from account numbers or the existence of the customer relationship, both of which are personally identifiable financial information that is not publicly available.

Distinction between "consumer" and "customer"

All *customers* covered by the rule are *consumers*, but not all *consumers* are *customers*.[1] A bank must give to a *customer*, when it establishes the customer relationship and annually, thereafter, a notice informing the customer of the bank's privacy policies and practices. The bank must also give the privacy notice to a *consumer* along with a notice of the right to opt out of sharing nonpublic personal information with nonaffiliates (opt out notice), before the bank discloses the information to a nonaffiliated third party. In other words, c*onsumers* who are not *customers* get the privacy and opt out notices, *only if* their bank wants to share their nonpublic personal information with certain nonaffiliated third parties.

A *consumer* is anyone who obtains from a bank any financial product or service to be used primarily for personal, family, or household purposes. A financial service includes a bank's evaluation of an application for a financial product or service from the bank. Thus, a person who submits an application will be considered a *consumer*, even if the application is denied.

A *customer*, by contrast, is defined as any *consumer* who has a "customer relationship" with the bank. A "customer relationship" is defined as a continuing relationship between a bank and a consumer to provide a financial product or service to the consumer. This would include a deposit, credit, or investment account. A one-time transaction may come within the definition, such as the purchase of an insurance policy, because of the ongoing nature of the product. By contrast, use (including repeated use) of an automated teller machine of a bank at which a consumer has no account would not create a "customer relationship."

[1] Business customers are not covered by the rule.

Time of establishing a customer relationship

The rule provides that a *customer* relationship is established at the time a bank and a consumer enter into a continuing relationship. This allows a bank to provide the privacy notice when it must give other notices, such as those required under the Truth-in-Lending Act.

In general, for customer relationships that are contractual in nature, a *customer* relationship is established when a *consumer* executes the contract that is necessary to conduct the transaction in question. For transactions that do not involve contracts, a customer relationship is established when the consumer pays or agrees to pay a fee or commission for the product or service.

Time by which the privacy notices must be provided

Initial privacy notice

GLBA provides that the initial privacy notice must be provided "at the time of establishing a customer relationship." The rule requires a bank to provide the initial privacy notice *no later than* when the bank and a consumer establish a customer relationship, e.g., before a consumer enters into a binding contract. In the case of a mortgage loan, for instance, the relationship would be established when a consumer executes the loan documents. For credit card accounts, the relationship is established when the consumer opens the account.

The rule also requires a bank to provide the initial privacy notice to a *consumer* prior to sharing nonpublic information about the consumer with nonaffiliated third parties. For example, if a bank wants to disclose information it collects about a person who uses the bank's ATM but otherwise has no relationship with the bank, the bank must provide the initial privacy notice as part of the ATM transaction.

Annual notices

The rule requires a bank to provide its customers with a copy of the privacy notice at least once during any 12-month period. The obligation ceases when a customer no longer has a continuing relationship with the bank. The rule provides several examples of how a customer relationship may terminate, such as when the bank and its customer have not communicated for 12 months.

Opt out notices

A bank must furnish an opt out notice to a consumer before sharing nonpublic personal information about the consumer with nonaffiliated third parties. The notice must inform the consumer that the bank may disclose this

information and that the consumer has the right to direct that the bank not share the information with nonaffiliated third parties. The notice must either provide the consumer with a reasonable means of opting out (such as a detachable reply form or a toll-free telephone number), or inform that person of another reasonable means (such as designating an electronic mail address if the consumer agrees to electronic delivery of the notice). It would *not* be a reasonable means of opting out if the customer had to write a notification letter, or if the only means provided to the customer was a check-off box in the initial privacy notice that was not included with subsequent revised or annual notices.

The bank need not provide opt out notices if it shares nonpublic personal information with nonaffiliated third parties only under specific regulatory exceptions.

Content of disclosures

Initial and annual privacy notices

The rule requires a bank to address each of the following specific types of information in its initial and annual privacy notices, as applicable. However, a bank may provide to *consumers* who are not *customers* a "short form" initial notice together with an opt out notice, stating that the bank's privacy notice is available upon request and explaining a reasonable means for the consumer to obtain it.

Categories of information a bank may collect. A bank's notice must disclose the *categories* of nonpublic personal information that it *collects*. This requirement may be satisfied if the bank categorizes the information according to its *sources,* such as information from consumers, transaction information, and credit report information.

Categories of information a bank may disclose. The bank's notice also must identify the categories of nonpublic personal information that a bank may *disclose — either to affiliated or nonaffiliated third parties.* A bank may categorize this information according to its source and provide illustrative examples of its content. For example, a bank's notice may state that it discloses application information (such as name, address, social security number, assets, and income), transaction information (such as account balance, payment history, parties to transactions, and credit card usage), and information from a consumer reporting agency (such as creditworthiness and credit history). If a bank makes disclosures to nonaffiliated third parties only under the exceptions in sections 40.14 and 40.15, it may state merely that it makes disclosures permitted by law.

Categories of parties to whom a bank may disclose. The notice also must disclose the categories of parties — *both affiliated and nonaffiliated* — to whom the bank discloses or intends to disclose nonpublic personal information about

consumers. The bank may satisfy this requirement if it identifies the types of businesses in which those affiliates and nonaffiliates engage. For example, a bank could state that it discloses information to a company offering financial products or services and provide illustrative examples of the types of business of those companies.

Information about former customers. The bank's initial and annual privacy notices must indicate its policies for disclosing nonpublic personal information about persons who have ceased to be customers.

Information disclosed to service providers and joint marketers. GLBA permits a bank to disclose nonpublic personal information about a consumer to a nonaffiliated third party to enable that party to perform services for the bank, including marketing the bank's own products or those offered jointly by the bank and another financial institution. The consumer has no right to opt out of this type of disclosure, but the bank must inform consumers that it will disclose their information in these circumstances. The rule requires that if a bank discloses nonpublic personal information to a nonaffiliated third party in this way, the bank must include in its privacy notices a separate description of the categories of information disclosed and the categories of third parties providing the services.

Right to opt out. The bank's initial and annual privacy notices must inform the bank's customers of their right to opt out and explain the methods by which they can do so. The notices may either provide the full set of opt out disclosures or refer the customer to the bank's opt out notice.

Disclosures required under the Fair Credit Reporting Act. A bank's initial and annual notices also must include any opt out disclosures the bank makes under the Fair Credit Reporting Act about sharing information with its *affiliates*.

Disclosures for confidentiality and security of information. The bank's privacy notices also must disclose its policies for protecting the confidentiality and security of nonpublic personal information. The information need not be technical, but should address who has access to the information, and whether the bank has security practices and procedures in place to maintain the confidentiality of consumer information.

Opt out notices

A bank must inform a consumer about the right to opt out *if* it intends to disclose nonpublic personal information about the consumer to certain nonaffiliated third parties. The opt out notice should identify all of the categories of nonpublic personal information that the bank discloses to nonaffiliated third parties *as described in its initial and annual privacy notices,* and describe the means by which consumers may opt out. It should be clear to the consumer

whether the opt out notice applies to the consumer's entire relationship with the bank or to specific accounts.

Standards governing delivery and clarity of notices

The rule requires that privacy and opt out notices be reasonably understandable and designed to call attention to the nature and significance of their content. The notices also must accurately reflect the bank's privacy practices. This requirement that disclosures be accurate enables the banking agencies to evaluate whether a bank is actually complying with its stated privacy policies and take appropriate action if it is not.

Notices must be provided so that each recipient can reasonably be expected to receive actual notice. Notices may be delivered in writing, or if the consumer agrees, electronically. A consumer must be able to retain an electronic notice or access it at a later time. Examples of acceptable delivery include mailing a copy to the consumer's last known address, or sending it by electronic mail *to a consumer who obtains a financial product or service from the bank electronically.* It is not sufficient for a bank to post a copy of its privacy notices in a lobby, or provide an *initial privacy* notice only on a Web page unless the consumer is required to acknowledge receipt of the notice to obtain the product or service in question. A bank may satisfy the *annual notice* requirement by posting the privacy notice on a transaction page on its Web site for customers who use the site to access financial products or services and who agree to receive notices at the site.

Reasonable opportunity to opt out

The rule requires that a consumer have a reasonable opportunity to opt out before a bank discloses nonpublic personal information to nonaffiliated third parties. An example of a reasonable opportunity is 30 days from the date a bank mails a notice to a consumer. The rule does not, however, mandate a specific waiting period before a bank may disclose nonpublic personal information to third parties. Instead, the examples in the rule indicate that "reasonableness" depends on the circumstances. Regardless of the length of time a bank waits before sharing that information, a consumer may always opt out of the information sharing at any time.

Limits on redisclosure and reuse of information

The rule limits a third party's (including a bank's) use and disclosure of the nonpublic personal information it receives from a nonaffiliated financial institution. When a nonaffiliated third party receives information under an exception (discussed under the heading "Section 502(e) exceptions"), the third party may only use and disclose the information in the ordinary course of business to carry

out the activity for which it received the information. When the third party receives information that was subject to notice and opt out, the third party may disclose the information consistent with the privacy policy of the financial institution that provided it (subject to a consumer's opt out election) and may disclose it according to an exception.

Exceptions

Service providers and joint marketers

GLBA permits a bank to disclose nonpublic personal information about a consumer to a nonaffiliated third party to enable that party to perform services for the bank, including marketing products offered jointly by the bank and another financial institution. A consumer has no right to opt out of this disclosure, but the bank must satisfy certain requirements to qualify for this exception. First, before it shares the information, the bank must disclose to the consumer that it will provide this information to the nonaffiliated third party. Second, the bank must enter into a contract with the third party that requires it to maintain the confidentiality of the information. The rule requires that the contract generally prohibit the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.

"Section 502(e) exceptions"

Section 502(e) of GLBA lists several exceptions to the requirements that would apply otherwise to a bank's disclosure of nonpublic personal information to nonaffiliated third parties. These exceptions, contained in sections 40.14 and 40.15 of the OCC's rule, generally are intended to permit a bank to continue sharing information as needed to conduct routine business transactions, such as disclosures made in connection with administration, processing, servicing, or sale of a consumer's account. When a bank shares information under any of these exceptions, it need not provide a *consumer* with a privacy notice or opportunity to opt out of the information sharing. However, even if a bank's disclosures to nonaffiliated third parties are limited to those permitted under the exceptions, the bank still must provide privacy notices to its *customers*. The rule states that a bank may describe its information disclosures under the exceptions merely as disclosures "permitted by law."

Disclosures of account numbers for marketing purposes

The rule restates the statutory prohibition against a bank disclosing, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer, to any nonaffiliated party for use in

telemarketing, direct mail marketing, or other marketing to the consumer through electronic mail.

The rule provides two exceptions to this prohibition and clarifies further its scope. A bank may provide an account number to an agent or service provider to market solely the bank's own products or services, *provided the bank does not authorize the agent or service provider to initiate charges to a consumer's account*. A bank may also disclose a consumer's account number to a participant in a private label credit card program or an affinity program when the participants are identified to the consumer.

An encrypted account number is not considered an account number for purposes of the prohibition, if the bank does not provide the third party with the key to decode the number and the third party cannot access the account. The rule also provides that the term "transaction account" does not pertain to an account to which third parties cannot initiate charges.

Effective date and transition rule

The rule was effective November 13, 2000 and extended the time for compliance until July 1, 2001. Thus, by July 1, 2001, banks must have provided an initial privacy notice to existing customers and, when necessary, an opportunity for them to opt out. By that time banks must have established a system for providing initial notices to new customers.

Effect of State laws

Consistent with the GLBA, the rule provides that the regulation does not preempt state laws that provide greater consumer protection than is provided under the GLBA privacy provisions. Determinations whether a particular state law provides greater protection are made by the Federal Trade Commission. (Note that the Fair Credit Reporting Act preempts state laws pertaining to information sharing among *affiliated* parties until 2004.)

Part II — Privacy Preparedness Checklist[1]

TO: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Purpose

This advisory is to help prepare you for the implementation of the new Privacy of Consumer Financial Information regulation, 12 CFR 40. The regulation becomes fully effective on July 1, 2001, and it affects all national banks, large and small, including most of their subsidiaries. A questionnaire is attached to assist you in your preparations and in performing a self-assessment. During the 2001 quarterly reviews conducted with your bank, your examiner-in-charge or bank portfolio manager will include a discussion of this advisory, the results of your self-assessment, and your progress toward full compliance with the provisions of 12 CFR 40. The extent of that discussion will be determined by the size of the institution involved, the nature of its information collection and sharing practices, and any concerns the examiner may have regarding the state of the bank's preparedness.

Background

Title V of the Gramm–Leach–Bliley Act (GLBA) of 1999 sets forth provisions addressing the obligations of a financial institution with respect to the privacy of consumers' nonpublic personal information. The Office of the Comptroller of the Currency's (OCC's) implementing regulation, 12 CFR 40, Privacy of Consumer Financial Information, provides for disclosures to consumers of a financial institution's privacy policy and the rights of consumers to direct their financial institution not to share their nonpublic personal information with third parties (opt out). A copy of the regulation is included in OCC Bulletin 2000-21 ("Privacy of Consumer Financial Information"), issued June 20, 2000. In addition, OCC Bulletin 2000-25 ("Privacy Laws and Regulations"), issued September 8, 2000, provides information and guidance regarding the various federal laws and regulations relating to the disclosure of consumer financial information.

Many who commented on the proposed rule stated that they needed more time than was provided in the statute to comply with the regulation. Commenters noted that they needed extra time to assess existing information practices; prepare new disclosures; develop software to track opt outs; train employees; and create management oversight, internal review, and auditing systems to ensure compliance. As a result of the comments, the agencies exercised their

[1] This checklist initially was published as OCC Advisory Letter 2001-2.

authority under section 510(1) of the GLBA and extended the mandatory compliance date. Financial institutions are expected to be in full compliance with the regulation by July 1, 2001. Full compliance means that an institution has delivered a privacy notice to its customers and, where applicable, has afforded its customers with a reasonable opportunity to opt out of information sharing before July 1, 2001. These institutions may continue to share nonpublic personal information after that date for customers who do not opt out.

PRIVACY PREPAREDNESS MEASURES

Senior management and the boards of directors of national banks and their subsidiaries are strongly encouraged to ensure that their institutions take all appropriate steps before the mandatory compliance date so that their institutions will comply fully with the privacy regulation by the July 1, 2001 deadline. The term "bank" in this advisory includes national banks, federal branches and agencies of foreign banks, and subsidiaries of a national bank or federal branch or agency, except subsidiaries that are brokers, dealers, persons providing insurance, investment companies, investment advisers, and entities subject to regulation by the Commodity Futures Trading Commission.[2] These steps should include:

- Assessing existing information practices by conducting an inventory of information collection, disclosure, and security practices.

- Evaluating agreements with nonaffiliated third parties that involve the disclosure of consumer information.

- Where necessary, establishing mechanisms to permit and process opt-out elections by consumers.

- Developing or revising existing privacy policies to reflect the new regulatory requirements.

- Determining how to deliver privacy notices to consumers.

- Establishing employee training and compliance programs.

- Developing an implementation plan.

Assessing Existing Information Practices. Banks are encouraged to assess their existing practices with respect to nonpublic personal information in order to (1) accurately represent them in their privacy policies; (2) determine the extent to

[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.

which disclosures to third parties fall within the statutory exceptions; (3) evaluate which information disclosures, if any, would trigger opt-out rights for consumers; and (4) determine whether any practices are prohibited, *e.g.*, impermissible sharing of account numbers with third parties. This exercise should also assist banks in evaluating the desirability of continuing or altering existing practices.

Evaluating Agreements with Nonaffiliated Third Parties that Involve Disclosure of Consumer Information. Banks should determine whether their agreements with nonaffiliated third parties that involve the disclosure of nonpublic personal information meet the regulatory requirements for maintaining the confidentiality of the bank's consumer information. For instance, if a bank discloses customer lists to a nonaffiliated third-party service provider to market the bank's own products or services, or to a nonaffiliated financial institution pursuant to a joint marketing agreement, section 40.13 of the regulation requires the bank to enter into a contract limiting the third party's use or disclosure of that information. Additionally, banks should consider how best to maintain the confidentiality of the consumer information they disclose pursuant to other nonaffiliated third-party arrangements, such as routine service agreements. Under the regulation, any nonaffiliated third party that receives nonpublic personal information from a bank is limited in its ability to use or disclose the information. Banks are encouraged to inform their service providers to familiarize themselves with these limitations. Moreover, banks that obtain nonpublic personal information from other nonaffiliated financial institutions also face limits on their use or disclosure of this information.

Establishing Mechanisms to Handle Opt-Out Elections. Banks that disclose information to nonaffiliated third parties outside the statutory exceptions must provide their consumers with a mechanism to opt out of that information sharing. Banks must ensure that they meet the regulatory requirements of providing consumers with a clear and conspicuous opt-out notice and a reasonable means to do so (*e.g.*, a convenient mechanism for opting out and a reasonable period of time (*e.g.*, 30 days)). In addition, banks must devise the means to record, maintain, and effectuate opt-out elections by consumers.

Developing a Privacy Policy. The regulation requires that all banks, even those that do not share nonpublic personal information, provide privacy notices to customers. Institutions must develop or revise existing privacy notices to conform them to the new privacy requirements. The notices must meet the clear and conspicuous standards, and they must accurately reflect the bank's privacy practices. In developing their privacy practices and notices, banks may want to evaluate the competitive aspects of their policies and obtain consumer input (*e.g.*, as to whether consumers understand and accept the policy).

Delivering Privacy Notices. Banks must determine the mechanism to deliver initial, annual, and revised privacy notices and opt-out notices to customers, consumers, and joint account holders. Methods of delivery may include hand

delivery, mail, and electronic delivery where the consumer is conducting business with the bank electronically and agrees to electronic disclosures. Banks should deliver privacy notices to customers, and where applicable, afford them a reasonable opportunity to opt out of information sharing before July 1, 2001.

Establishing Training Programs. All bank employees should have a general understanding of the bank's privacy policies; however, certain employees require more detailed knowledge. Customer service personnel, personnel who process requests for consumer information or who provide such information to third parties, and other employees in contact with consumers must have a thorough understanding of the bank's privacy policies and practices. They should be prepared to answer questions about the bank's privacy policies and practices, address whether an individual consumer's records are shared, direct consumers through the bank's complaint process, and if applicable, provide notices to consumers. Bank training programs should be customized for the audience, should be ongoing, and should provide follow-up when problems are noted.

Establishing Compliance Programs. Banks should ensure that their compliance personnel are involved in the privacy preparations. Compliance should evaluate the bank's privacy practices and measures undertaken to ensure regulatory conformance. Internal controls, policies, and audit procedures should be developed, and audits/compliance reviews scheduled, in time for the July 1, 2001, implementation date. Implementation problems and compliance deficiencies identified by the compliance staff should receive immediate attention by senior management.

Developing an Implementation Plan. To ensure timely and adequate compliance with the new privacy requirements, banks should develop a privacy action plan that takes into consideration the above measures, as appropriate. The plan should be approved by senior management and the board, and should include target dates, goals, and responsible parties. Also, it should call for testing and progress reports.

Attached to this advisory is a privacy preparedness questionnaire that may be used to perform a privacy self-assessment. It sets forth measures for implementation and compliance. The questionnaire is a general guide that addresses a broad scope of application, and as a result, some questions may not be applicable to your financial institution. During the 2001 quarterly reviews of your bank, examiners will inquire about your privacy policies and preparations, and the results of any self-assessment. They will use the attached questionnaire to ask applicable questions about your privacy readiness and may also offer suggestions to improve your compliance efforts. Results of these reviews will allow the OCC to determine which national banks may be at higher risk for noncompliance requiring priority in examination scheduling.

Questions concerning this advisory may be directed to your supervisory office or the Community and Consumer Policy Division at (202) 874-4428.

_____

Ralph E. Sharpe,
Deputy Comptroller for Community and
Consumer Policy

Privacy Preparedness Questionnaire

Assessing Existing Information Practices

1. What are your information-sharing practices?

- What information is shared with affiliates and nonaffiliates (including sharing within and outside of the regulatory exceptions contained in 12 CFR 40.13, 40.14, 40.15), what is the purpose of the sharing, and is information shared on former customers?
- Are account numbers or access numbers/codes disclosed to nonaffiliated third parties?
- What information do you share on consumers who are not customers?
- Do you route requests for nonpublic personal information to a central point or use other control measures?
- Will any of your current information-sharing practices be prohibited by the regulation?

2. What kinds of information do you collect from consumers and customers for the various financial products and services offered by the bank?

3. Do you obtain information about consumers and customers from other financial institutions? If so, do you use or share the information for other purposes?

4. Are your safeguards for protecting customer information consistent with Section 501(b) of the Gramm–Leach–Bliley Act?

- Has the board approved the written information security program?
- Are your safeguards adequate to: a) ensure security and confidentiality of customer records and information, b) protect against any anticipated threats or hazards to the security or integrity of customer records and information, and c) protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer?
- Has your information security program been tested in accordance with the regulatory guidelines?

Evaluating Agreements with Nonaffiliated Third Parties that Involve Disclosure of Consumer Information

5. What arrangements, agreements, or contracts exist with nonaffiliated third parties that involve disclosing consumer information? Do contracts or

agreements detail responsibilities regarding the use, disclosure, and protection of consumer information?

6. What changes need to be made to conform the arrangements, agreements, or contracts to the regulation?

Establishing Mechanisms to Handle Opt-Out Elections

7. If applicable, how will you administer the opt-out provisions of the regulation?

- Is the opt-out mechanism reasonably convenient for the consumer to use?
- How will you document those consumers who opt out or later change their opt-out status, and how will you segregate their information?
- How much time will you allow for consumers to opt out and how quickly will you process opt-outs?
- What are your opt-out arrangements for consumers who jointly hold a financial product or service?
- Will you allow partial opt-outs? If so, under what circumstances, and are your record- keeping systems capable of handling that level of complexity?

Developing a Privacy Policy

8. Have you developed a privacy policy? If so, what is it?

- Does the policy contain all relevant disclosures required by the privacy regulation?
- Is the information in the privacy policy stated clearly and in a way that consumers are likely to understand? Is it presented in a way that is likely to call the consumer's attention to the nature and significance of the information in the notice?
- Has the policy been reviewed by the board and senior management, the compliance officer, and legal counsel?
- Does it reflect your actual practices?
- Do you think your customers will accept your privacy policy?
- Does the institution have a process to ensure that privacy policies are kept current?

Delivering Privacy Notices

9. How will you deliver initial, annual, and revised privacy notices, and opt-out notices to customers, consumers, and customers who jointly hold a financial product or service?

- Will you hand deliver notices to individuals conducting transactions in person?
- Will you mail the notices, and if so, will you mail them with other information, such as account statements, or separately?

- Do you intend to deliver any notices electronically? If so, how will you obtain the consumer's/customer's agreement to receive electronic delivery?

Establishing a Training Program

10. Describe your plan to train employees on privacy.

- Who will be trained, when, and what information will be covered?
- Will there be different levels of training depending upon job responsibilities?

Establishing a Compliance Program

11. Describe audit's/compliance review's role in developing and implementing the bank's privacy program.

12. Have internal controls, policies, procedures, and audit programs been established to ensure a satisfactory level of compliance?

Developing an Implementation Plan

13. Describe your implementation plan.

- Has the plan been approved by senior management and the board?
- Does it contain target dates, responsibilities, responsible parties, testing procedures, and progress reports?
- Is the plan on schedule?
- Does the plan ensure delivery of the privacy policy prior to July 1, 2001, and afford customers a reasonable time to exercise any opt-out rights before that date?

Part III — Frequently Asked Questions for the Privacy Regulation

December 2001

Table of Contents

Staff of the OCC has developed the following Frequently Asked Questions (FAQs) to assist financial institutions within our jurisdiction in complying with the privacy provisions of the Gramm-Leach-Bliley Act (GLB Act) and the OCC's implementing regulation, 12 C.F.R. Part 40. These FAQs illustrate how select provisions of the regulation apply to specific situations a financial institution may confront. However, they do not necessarily address all provisions that may apply to any given situation. Additionally, this staff guidance addresses a financial institution's obligations only under sections 502-509 of the GLB Act and 12 C.F.R. Part 40 and does not address the applicability of the Fair Credit Reporting Act or any other federal or state law that may pertain to the questions and answers. Staff may supplement or revise these FAQs as necessary or appropriate in light of further questions and experience.

A. Financial institutions, products, and services that are covered under the Privacy Rule

1. Q. Who must comply with the Privacy Rule?

A. Any financial institution that provides financial products or services to consumers must comply with the privacy provisions of Title V of the Gramm-Leach-Bliley Act ("GLB Act") (15 U.S.C. §§ 6801-09) and the Privacy Rule. Under the banking agencies' rules,[1] you are a financial institution if you engage in an activity that is financial in nature or incidental to a financial activity, as described in § 4(k) of the Bank Holding Company Act of 1956 ("BHC Act") (12 U.S.C. § 1843(k)). For purposes of the banking agencies' rules, activities "described in § 4(k) of the BHC Act" include the activities specifically listed in § 4(k) and any additional activities the Board, in consultation with the Secretary of the Treasury, determines to be financial in nature or incidental to a financial activity in accordance with § 4(k).

Section 225.86 of the Board's Regulation Y lists or otherwise references the activities that are financial in nature as of the date of this Compliance Guide. *See* 12 C.F.R. 225.86. Note, however, that additional activities the Board authorizes in the future, such as activities approved by Board order, may not necessarily be listed at § 225.86.

Authorized financial activities as of the date of this Compliance Guide include but are not limited to the following:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities;
- Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, either as principal, agent, or broker; and
- Providing financial advice, underwriting, dealing in, or making a market in securities.

You have consumers if you provide your financial products or services to individuals to be used primarily for their personal, family, or household purposes.

[1] The scope of the privacy regulation promulgated by the Federal Trade Commission ("FTC") is more limited than that of the other agencies. Under the FTC's privacy regulation, financial institution means "any institution the business of which is engaging in financial activities as described in § 4(k) of the Bank Holding Company Act of 1956." *See* 16 C.F.R. 313.3(k)(1). Moreover, an institution is not a financial institution unless it is *significantly engaged* in financial activities. *Id.* In addition, the FTC's regulation does not automatically apply to institutions significantly engaged in activities that the Board determines, after November 12, 1999, to be financial in nature. *See* 16 C.F.R. 313.18(a)(2).

Additionally, the Privacy Rule restricts the use and disclosure of nonpublic personal information obtained from a nonaffiliated financial institution, as discussed below.

2. Q. I am a small financial institution with no affiliates. I do not disclose information about my customers or consumers to anyone, except as permitted by an exception under §§ 40.14 and 40.15 of the Privacy Rule.[2] Does the Privacy Rule apply to a small operation like mine?

A. Yes. You have responsibilities under the Privacy Rule regardless of your size, affiliate relationships, or information collection and disclosure practices. The Privacy Rule is focused not only on regulating the disclosure of financial information about customers and consumers, but also on requiring each financial institution to provide initial and annual notices of its policies to its customers. You may, however, provide notice in a simplified form, as illustrated by the notice described in § 40.6(c)(5).

3. Q. I provide trust services. In this capacity, I serve as the trustee of trusts whose beneficiaries are individuals. Does the Privacy Rule apply to my trust operations?

A. When you act as a trustee, you have a relationship with the trust. Because the trust itself is not an individual, it is not a consumer under the Privacy Rule. Even if the grantor and all the beneficiaries are individuals, neither the grantor nor any of the beneficiaries are your consumers solely because of their relationship to the trust. If, for example, the trust requires you, as trustee, to transfer money to a beneficiary, you provide that financial service to the trust rather than the individual who is the beneficiary. In other words, grantors and beneficiaries of a trust are not your consumers unless they directly obtain a financial product and service from you for their personal, family, or household purposes. Accordingly, you do not have any obligations under the Privacy Rule with respect to the trust. Your duties as a fiduciary, however, may require you to maintain the confidentiality of information about the trust, its grantor, and its beneficiaries.

4. Q. I act as a custodian for Individual Retirement Arrangements ("IRAs"). Are the individuals who own the IRAs my customers?

A. Yes. An individual who establishes an IRA account for which you act as a custodian has obtained a financial product or service that is to be used primarily for personal, family, or household purposes; therefore, he or she is a consumer. When an individual selects you to act as custodian for his or her IRA, the individual enters into a continuing relationship with you and becomes your customer under the Privacy Rule. By contrast, an individual who is a participant

[2] All subsequent section references are to the Privacy Rule unless otherwise noted.

or a beneficiary of an employee benefit plan that you sponsor or for which you act as trustee or fiduciary is *not* your customer because your relationship in that case is with the plan.

5. Q. I am a tax return preparer and I understand that I may be subject to the Privacy Rule concerning the disclosure of my clients' nonpublic personal information. However, I also am subject to section 7216 of the Internal Revenue Code, which restricts the use and disclosure of my customers' federal tax return information. Do the privacy provisions of the GLB Act and the Privacy Rule supersede the restrictions in section 7216? May I now disclose my customers' federal income tax return information after I provide them with the proper notices and give my customers a reasonable opportunity to opt out?

A. No. The Privacy Rule does not supersede the restrictions in section 7216. The GLB Act and the Agencies' implementing regulations do not authorize a financial institution to disclose nonpublic personal information in a way that is prohibited by some other law. Therefore, you may not avoid the restrictions of section 7216 by providing your customers with an opt out notice and a reasonable opportunity to opt out.

B. Individuals who are entitled to receive notices

1. Q. Why does the Privacy Rule sometimes refer to consumers and other times to customers? Aren't customers also consumers?

A. All customers are consumers, but not all consumers are customers.

A consumer is an individual who obtains a financial product or service from you that is primarily for personal, family, or household purposes. A financial product or service includes the evaluation or brokerage of information collected in connection with a request or application, such as a bank's review of loan application materials to determine whether an applicant qualifies for a loan. A customer is a type of consumer, namely, an individual who has an ongoing relationship with you under which you provide a financial product or service. Note that neither a business nor an individual who obtains a financial product or service for business purposes is a consumer or a customer under the Privacy Rule.

The rule distinguishes consumers from customers because your responsibilities to provide notices to consumers and to customers differ in several respects.

- You must give all your customers initial privacy notices.
- You must give initial notices (or short form notices) to consumers who are not your customers *only* if you intend to disclose nonpublic personal information about those consumers to nonaffiliated third parties (unless

an exception in §§ 40.14 or 40.15 applies such that no initial notice is required prior to the disclosure).

- You must give annual privacy notices to your customers as long as they remain your customers.
- You are *never* required to send annual notices to consumers who are not your customers.

It is important to remember that all consumers are entitled to the same protection from disclosures of nonpublic personal information under this regulation regardless of whether they are customers. You therefore must not disclose the nonpublic personal information of any consumer or any customer to any nonaffiliated third party outside of the exceptions in §§ 40.13 – 40.15 unless you provide a privacy notice and a reasonable opportunity to opt out, and the consumer or customer does not opt out.

2. Q. I occasionally make business loans to sole proprietors. Do I have to provide them with a privacy notice?

A. Although a sole proprietor is an individual, if the sole proprietor obtains a loan from you for business purposes he or she is not a "consumer" for purposes of the Privacy Rule. Therefore, you do not have to provide any privacy notices to the sole proprietor.

3. Q. Is a guarantor or an endorser of a consumer loan considered my consumer or customer?

A. A guarantor or endorser of a consumer loan is your customer because the individual assumes secondary liability on the loan he or she guarantees or endorses and thereby receives an extension of credit from you. You may, however, treat the primary borrower and the guarantor or endorser as joint account holders. As a result, you may deliver a single privacy notice to the joint account holders in accordance with § 40.9(g). If you disclose information to nonaffiliated third parties outside of the exceptions in §§ 40.13, 40.14, and 40.15, you must also provide the primary borrower and the guarantor/endorser with an opportunity to opt out. You may deliver a single opt out notice to the joint account holders under § 40.7(d).

4. Q. Non-U.S.-resident consumers conduct business at my U.S. offices. Do the privacy regulations apply in cases where consumers live in another country?

A. Yes. The privacy regulations apply to all United States offices of entities for which the federal financial institution regulators have primary supervisory authority, regardless of where the consumer lives.

5. Q. Is a person who only browses my web site my consumer?

A. No. The person does not obtain a financial product or service from you merely by browsing your web site.

C. Delivering your privacy notices

1. Q. I issue credit cards to consumers. Very often, I take credit card applications by telephone and approve them within minutes. My customers wish to begin using their new accounts right away. When must I deliver initial notices in these cases?

A. You cannot deliver your privacy notice solely by explaining it over the telephone. However, you may provide an initial notice within a reasonable time after establishing a customer relationship if (i) providing it when you establish that relationship would substantially delay the customer's transaction, and (ii) the customer agrees to a later delivery. In the case of approving a credit card application by telephone, waiting until you have time to mail the notice would substantially delay the customer's use of a new credit account. As long as your new customer agrees to receive the notice later, you may deliver it within a reasonable time after establishing the customer relationship.

Notwithstanding that exception, delayed delivery of an initial notice does not alter the restrictions on disclosing nonpublic personal information. That is, if you delay delivering your initial notice to a customer, you may not disclose that customer's nonpublic personal information to any nonaffiliated third party (except as permitted by the exceptions under §§ 40.14 and 40.15) before you provide the notices and a reasonable opportunity to opt out, in accordance with §§ 40.7 and 40.10.

2. Q. I am a financial institution with several subsidiaries. Must each affiliated financial institution issue a separate privacy notice? If affiliated financial institutions are permitted to combine their notices, how may we identify them in the notice?

A. You and your subsidiaries may share common privacy policies and practices and you may combine your respective privacy notices into a joint notice. However, any joint notice must be accurate as to each institution, must be clear and conspicuous, and must identify which institutions it covers.

You do not have to list each financial institution by its particular legal name. Instead, if each institution shares the "ABC" name, then the joint notice could state that it applies to "all institutions with the ABC name" or "in the ABC family of companies." Conversely, if an affiliated institution does not have ABC in its name, then your notice must separately identify that institution.

3. Q. My privacy notice must identify "categories" of nonpublic personal information I collect and categories of affiliates and nonaffiliated third parties with which I share that information. How detailed do the categories need to be?

A. The Privacy Rule does not require your privacy notices to describe in detail the information you collect or disclose. Moreover, you are not required to identify by name parties to whom you may make disclosures. Rather, you may describe the types, or categories, of information you collect and disclose, and the types of third parties to whom you disclose the information. These categories must be representative of your policies and practices. Because the examples in the rule that describe categories of information and parties to whom you disclose information are not exclusive, you may describe the items in § 40.6(a)(1)-(9) that apply to you by using other reasonably understandable language that informs a consumer about your privacy policies and practices. You also may use different language and may provide additional detail as appropriate to explain your policies and practices to your consumers. In addition, the Privacy Rule requires you to address only those items that apply to you. Your initial notice must accurately describe your policies and procedures as of the time you provide the notice to a consumer or customer. A notice also may be accurate even if it reflects anticipated as well as current policies and practices.

4. Q. Won't my annual notice look just like my initial notice?

A. The initial and annual notices may be identical because the required contents for your initial notice are the same as those for your annual notice. You must, of course, incorporate any revisions you make to your privacy policy into your annual notice.

Your annual notice, like your initial notice, must describe any right of consumers to opt out of disclosures you may make and must describe how consumers may opt out. If the only opt out method you allow is for consumers to send you a specific opt out form, then you must include that form with your initial and annual notices.

5. Q. After I provide an initial privacy notice to my customer, the Privacy Rule requires me to deliver privacy notices to that customer not less than annually during the continuation of the customer relationship. What does "annually" mean?

A. "Annually" means at least once in any period of 12 consecutive months during which a customer relationship exists. If you use the calendar year as your notice period, you have the flexibility to give the first annual notice to a customer at any point in the calendar year following the year in which the customer relationship is established. Thereafter, you are expected to provide annual notices on a consistent basis. Any period of more than 12 consecutive

months between annual notices should have an appropriate business justification.

6. Q. Can I combine my privacy notice with other consumer disclosures, such as those under the Truth in Lending Act (Regulation Z) or the Truth in Savings Act (Regulation DD)?

A. The Privacy Rule does not prohibit you from combining your privacy notices with other information. However, you still must comply with all applicable requirements, such as those governing form, content, and delivery of notices. For example, if you combine your privacy notice with a disclosure under Regulation Z or Regulation DD, each component of the combined notice/disclosure must comply with the "clear and conspicuous" requirements in the regulation governing that component.

7. Q. I do not disclose any nonpublic personal information about my customers to any affiliates or nonaffiliated third parties, except under the conditions described in §§ 40.14 and 40.15 (exceptions to notice and opt out requirements). What aspects of my privacy policies and practices must my notice address?

A. In this case, you may use a simplified notice. A simplified notice is sufficient if it:

- Describes the categories of nonpublic personal information you collect;
- States the fact that you do not share nonpublic personal information about your customers or former customers to affiliates or nonaffiliated third parties, except as authorized by law; and
- Describes your policies and practices for protecting the confidentiality and security of consumers' nonpublic personal information (under § 501(b) of the GLB Act).

8. Q. I own and operate several ATMs. Many consumers who use them are not my customers. I disclose to nonaffiliated third parties nonpublic personal information about those consumers other than as permitted by the exceptions in §§ 40.14 or 40.15, so I must provide them with the required notices when they use my ATMs. But ATM screens are very small. Am I required to purchase machines with screens large enough to hold my privacy policy? Must I make consumers click through dozens of tiny screens of information?

A. Neither new machines nor multiple screens are necessary. You must provide an opt out notice, as required under § 40.7. This notice must state that you disclose nonpublic personal information about the consumer to nonaffiliated third parties, state that the consumer has a right to opt out of that disclosure, and provide a reasonable opportunity for the consumer to opt out (such as by requiring the consumer to decide whether to opt out as a necessary

part of the transaction). § 40.10(a)(3)(iii). In addition to the opt out notice, you must provide an initial privacy notice. For consumers who are not your customers, you may provide a short-form initial notice with an opt out notice. § 40.6(d). This short-form notice must state that your privacy policy is available upon request and it must describe a reasonable means for the consumer to get your privacy notice. As with any privacy notice, the opt out notice and the short-form initial notice must be clear, conspicuous, and accurate. These notices must be delivered in a manner so that the consumer can agree to receive the notices electronically, such as by acknowledging receipt of the notices as a necessary step to completing the transaction at the ATM. § 40.9(a).

9. Q. I'm a small bank. I want to offer credit cards to my customers, but I am too small to handle a credit card operation. Instead, I contract with others to help me. When my customer indicates an interest in getting a credit card, I supply an application form. That form makes clear that the lender is a large bank ("Large Bank"). I am not affiliated with the Large Bank. The customer sends the completed form directly to the Large Bank, so that I do not "collect" the application information within the meaning of § 40.3(c). The Large Bank issues the credit card for approved applicants, with its name on the back. My name and logo are prominent on the front of the credit card. Who must provide the initial privacy notice?

A. When a financial institution makes a consumer loan, as the Large Bank does in this case, it has a customer relationship with that consumer. The Large Bank, therefore, must provide an initial privacy notice and must provide annual notices as long as the credit card relationship continues. You are not required to send any new notices to your customers because you do not appear to be providing any financial product or service to them in connection with this credit card product.

D. Providing notices to joint account holders

1. Q. I have two depositors who hold one account jointly. The depositors share the same address. When notice is required, may I mail just one privacy notice?

A. Yes, you may mail one notice to two or more joint account holders at the same address. § 40.9(g).

2. Q. What if those same account holders have different addresses?

A. You still may mail one notice to all accountholders jointly at one account holder's address. § 40.9(g).

3. Q. One account holder, A, maintains with me a single account and a joint account with another consumer, X. What are my obligations to send privacy notices to A and X? Can I satisfy the initial privacy notice requirement by sending just one notice?

A. In some cases, one notice may be sufficient. For example, if A and X open the joint account first and A subsequently opens an individual account, you need not provide an additional initial notice to A if the most recent notice you provided to A as part of the joint account is accurate as to the individual account. § 40.4(d). If A already has an individual account with you but X becomes your customer at the time the joint account is opened, you must provide an initial notice to X with respect to the joint account. § 40.4(a). However, you may deliver the initial notice either to A or to X by providing one notice to those consumers jointly. § 40.9(g). For example, you may deliver one notice addressed to both A and X. You subsequently may satisfy the annual and revised notice requirements by sending one notice regarding the joint account either to A or X.

4. Q. One depositor, A, has two different joint accounts, one with X and the other with Y. When annual or revised notices are required as to both accounts, how many notices must I provide?

A. Annual and revised notices pertaining to each of the joint accounts may be provided either to A or to both of the other account holders respectively. Thus, one notice to A is sufficient, as long as the notice is accurate as to both accounts. § 40.9(g). The Privacy Rule does not require you to mail two identical notices to A, one for each account.

However, you must neither disclose to X that A has a joint account with Y nor disclose to Y that A has a joint account with X, unless these facts are publicly available. The fact that a consumer is a financial institution's customer is nonpublic personal information, unless you have a reasonable basis to believe that the customer relationship is a matter of public record.

5. Q. Assume the same facts as Question D.4. What if the two joint account holders with A, X and Y, have different addresses?

A. You still may provide one notice to A. However, in any communications with X and Y, you must not disclose to X the fact that A has a joint account with Y, nor may you disclose to Y that A has a joint account with X, unless you have a reasonable basis to believe this information is publicly available.

E. Complying with the opt out provisions for joint account holders

1. Q. I have two depositors who hold one account jointly. Must I deliver a separate opt out notice to each account holder and allow each of them to opt out individually? Suppose I mail only one opt out notice for that account, and one of the joint holders checks "I opt out" and returns it to me. To whom does the opt out decision apply?

A. You may deliver either a single opt out notice to one of the account holders or a separate notice to each account holder. In either case, the notice must permit one joint account holder to opt out on behalf of all holders of the account. So long as your notice fulfills this requirement, you also may permit joint account holders to opt out individually.

The answer to your second question depends upon how you have designed your opt out notice. Your notice must permit one joint account holder to opt out on behalf of all holders of that account. However, you have several ways to do this. For example, your notice may contain one box that, when checked, will result in an opt out by the person checking the box and all other individuals on the account. Alternatively, the opt out notice may provide boxes that enable each individual on the account to opt out separately, as well as a box that permits one account holder to opt out on behalf of everyone on the account.

With either option your opt out notice must clearly and conspicuously describe how each applicable opt out selection will be treated. For example, the opt out selection for all account holders should disclose that the customer making that selection is opting out for all account holders with respect to information concerning that joint account. Similarly, the "individual" opt out selection should explain that the selection applies only to the customer making the selection.

If you already are disclosing nonpublic personal information because you did not receive an opt out direction after sending your initial notice, each joint account holder still may choose to opt out at a later date. You must abide by any subsequent opt out decision as soon as reasonably practicable after you receive it, and you must not delay complying with one individual account holder's opt out direction until the remaining account holder(s) opt out.

Once a consumer opts out, whether during the initial opt out period or subsequently, you must not share the consumer's nonpublic personal information to which the opt out applies unless and until the consumer subsequently revokes his or her opt out direction. § 40.7(g)(1).

2. Q. I allow joint account holders X and Y to make independent opt out elections. For opt outs, I use reply forms with check-off boxes. Must I mail two opt out response forms for one joint account?

A. No, only one is necessary. However, you must allow each account holder a reasonable amount of time to opt out before disclosing any nonpublic personal information about him or her. For example, suppose you normally allow each consumer thirty days to opt out, and you immediately receive an opt out instruction from X but not from Y. You still must allow Y the standard thirty days to opt out before you may disclose any nonpublic personal information relating to the joint account. You may disclose nonpublic personal information about Y if Y does not opt out within the reasonable opt out period, but only to the extent such a disclosure would not reveal nonpublic personal information about X.

3. Q. I allow joint account holders to make independent opt out elections. May I require each account holder to opt out in a separate response?

A. No. You must allow both account holders a reasonable opportunity to opt out in one response, such as one opt out form or in one call to your toll-free opt out line.

4. Q. I allow joint account holders, X and Y, to make independent opt out elections. Suppose that X opted out, but Y did not respond. What nonpublic personal information about X and Y may I disclose?

A. Because X has opted out, you must not disclose any nonpublic personal information about X, except as permitted by an exception at §§ 40.13, 40.14, or 40.15. In addition, you must not disclose nonpublic personal information about Y except as permitted by an exception if the disclosure of that information also would disclose nonpublic personal information about X.

For example, suppose that X and Y are married, share the same surname, reside at the same address, and jointly hold a savings account with you. You may disclose nonpublic personal information relating to that account about Y, such as the average monthly balance in the account, as long as that disclosure does not include any nonpublic personal information about X. Furthermore, you must not disclose the fact that Y holds the joint account together with X.

F. Delivering opt out notices and providing consumers with a reasonable opportunity to opt out of disclosures

1. Q. Must I provide opt out notices if I do not disclose nonpublic personal information to nonaffiliated third parties, except as permitted under one of the exceptions under §§ 40.13, 40.14, or 40.15?

A. No. If you disclose nonpublic personal information only under one or more of those exceptions, you need not provide any opt out notices.

Nonetheless, be aware that if you disclose nonpublic personal information under § 40.13, then you must provide an initial notice that includes a separate statement that describes that disclosure. Also, you must provide an annual notice to your customers regardless of your disclosure policies and practices. § 40.5.

2. Q. What are some reasonable means of allowing consumers an opportunity to opt out?

A. You may provide various opt out methods that are reasonable, depending on the circumstances surrounding the financial product or service. For example, for new customers who open credit card accounts, you may deliver a form with a check-off box that they can check and return to you. If you use this method, you must deliver the check-off form with your opt out notice. You also may provide a toll-free telephone number that consumers can call to opt out. §§ 40.7(a)(2)(ii), 40.10(a)(3)(i).

The Privacy Rule provides that you may require a consumer to opt out through a specific means if that means is reasonable for that particular consumer. § 40.7(a)(2)(iv). For example, you may require a consumer who has agreed to the electronic delivery of notices to opt out by using a process available on your web site if that consumer uses your web site to access financial products or services. You also may require a consumer who conducts an isolated transaction at your branch, ATM, or office in person to decide whether to opt out as a necessary part of completing the transaction and to use the means you specify to effect his or her opt out direction. § 40.10(a)(3)(iii).

Note that you may *allow* any consumer to opt out by e-mail or by using a process available on your web site, but you may not *require* the consumer to use an electronic method if the consumer has not agreed to electronic delivery of notices. Under these circumstances, you must provide other reasonable methods for the consumer to opt out.

No particular method described in an example in the Privacy Rule is strictly required and there may be other reasonable methods for allowing a consumer to opt out of disclosures. Some methods to opt out, however, are unreasonable. For instance, you must *not* require consumers to write their own letters to opt out as the only opt out method. § 40.7(a)(2)(iii)(A).

3. Q. If I allow my customers to mail a form to indicate their opt out election, am I required to provide my customers with a postage-paid envelope so they can mail the form back?

A. No. You are not required to provide an individual with a postage-paid envelope to meet the requirement that you provide a reasonable means for consumers to opt out.

4. Q. In our initial and annual notices, our bank would like to provide a tear-off opt out form and its privacy policies on the front and back of a single sheet of paper. Is this permissible?

A. Yes, provided the opt out form may be detached without removing text from your privacy policy. However, if by detaching the opt out form the customer removes text from the privacy policy, the practice may violate § 40.9(e). This section requires a financial institution to provide its privacy notices in a form in which a customer can retain them or obtain them later. If the customer would remove text from your privacy policy by detaching the opt out notice, then you should either redesign the privacy notice or have procedures in place to provide a customer with the complete text of your privacy notice upon request.

5. Q. I provide consumer credit cards. I would like to disclose to nonaffiliated third parties different types of nonpublic personal information about my customers, such as their addresses and their account information. The nonaffiliated third parties are not financial institutions with which I have a joint agreement. I realize that I must allow my customers to opt out of all these disclosures, but may I give them the choice to opt out of disclosures of certain categories of information as well as all categories of information to nonaffiliated third parties?

A. Yes. You must allow your customers to opt out of all these disclosures to nonaffiliated third parties. Additionally, you may allow your customers to choose to opt out of some types of disclosures, rather than simply all of those disclosures. For example, you may allow your customers to opt out of disclosures of account information and provide a separate opportunity for customers to opt out of disclosures of their addresses. § 40.10(c).

6. Q. I make consumer loans. I would like to disclose my customer list to nonaffiliated clothing retailers and to nonaffiliated automobile dealers. These nonaffiliated third parties are not financial institutions with which I have a joint agreement. I realize that I must allow my customers to opt out of all these disclosures. But may I also give them the choice to opt out of disclosures to certain kinds of nonaffiliated third parties without having to opt out of disclosures to all kinds of third parties?

A. Yes. You must allow your customers to opt out of all these disclosures. Additionally, you may allow your customers to choose to opt out of disclosures to some kinds of nonaffiliated third parties instead of simply all of those parties. For example, you may allow your customers to opt out of disclosures to clothing retailers and allow a separate opportunity for the same customers to opt out of disclosures to automobile dealers.

7. Q. We deliver opt out notices by mail and allow our new customers 30 days to opt out before we begin sharing their information with nonaffiliated third parties. Section 40.7(e) provides that a financial institution must comply with a consumer's opt out direction as soon as reasonably practicable after the financial institution receives it. It may take our bank up to five weeks to process an opt out direction. If we mail a new customer a privacy and opt out notice on September 1 and we receive the customer's opt out direction on September 15, may we share that individual's nonpublic personal information between September 15 and October 22 -- the date by which we can process the opt out?

A. No. Because your question concerns a new customer rather than an existing one, the standard in § 40.10(a)(1) rather than that in § 40.7(e) applies. Section 40.10(a)(1) of the Privacy Rule provides that a financial institution may not share a consumer's nonpublic personal information unless the institution has given the consumer an initial privacy notice, an opt out notice, and a reasonable opportunity to opt out, and the consumer has not opted out. If your customer opts out at any point within the 30-day period in your example, then you would not be able to disclose that individual's information to nonaffiliated third parties unless the customer subsequently revoked the opt out direction. § 40.7(g)(1).

Section 40.7(e) applies only where the financial institution is already lawfully disclosing nonpublic personal information of existing customers or consumers to nonaffiliated third parties. Because the Privacy Rule permits consumers to opt out at any time, § 40.7(e) provides an institution with a reasonable period of time to process an existing consumer's opt out election before the institution must cease disclosing the consumer's information. The institution must process the opt out election as soon as reasonably practicable. For example, following the 30-day period that you provide initially for your customers to opt out, you may disclose the nonpublic personal information of those individuals who have not exercised their right to opt out. However, you must honor any subsequent opt out election by any of those customers "as soon as reasonably practicable."

G. Complying with the limitations on redisclosure and reuse of nonpublic personal information

I. Nonpublic personal information disclosed under an exception

I am a consumer lender, but a nonaffiliated third party ("Servicer") services my loans. I disclose nonpublic personal information to the Servicer under an exception for that purpose. I have the following questions.

1. Q. I disclose nonpublic personal information about my customers to the Servicer so the Servicer can process transactions that the customers have

requested. May the Servicer disclose the information it collects from me about my customers to a retail merchant that is not affiliated with me?

A. Generally, no. When the Servicer receives nonpublic personal information about your customers under an exception to the notice and opt out provisions, such as in connection with servicing your loans, the Servicer's use and disclosure of that information is limited. The Servicer must not disclose any nonpublic personal information to a retail merchant not affiliated with you unless the Servicer may do so under an applicable exception in §§ 40.14 or 40.15. For example, the Servicer may not provide information about your customers to the retail merchant for marketing purposes.

2. Q. May the Servicer disclose the nonpublic personal information to my affiliate?

A. Yes. The Privacy Rule explicitly provides that the Servicer may disclose the information to your affiliate. § 40.11(c)(1).

3. Q. May the Servicer disclose the information to the Servicer's affiliate?

A. Yes, but the Servicer's affiliate may disclose and use the information only as the Servicer could disclose and use it. § 40.11(c)(2). The Servicer's affiliate therefore may use the information to service your loans. The affiliate also may disclose the information under an applicable exception in §§ 40.14 or 40.15 in the ordinary course of business to carry out the activity covered by the exception under which the Servicer received the information.

II. Nonpublic personal information disclosed outside of an exception

I am a consumer lender and am affiliated with a property insurer. In my privacy notices I inform consumers that I disclose nonpublic personal information to my affiliated insurance company. My privacy notice also states that, if a consumer does not opt out, I may disclose nonpublic personal information about the consumer to nonfinancial companies, such as retailers.

Among the nonaffiliated third parties to whom I disclose information are an automobile dealer and a residential plumbing company. The plumbing company is affiliated with a company that sells air conditioning products and services.

I have the following questions about disclosing information about consumers who do not opt out.

4. Q. I disclose information about my customers who do not opt out to a residential plumbing company. Can the plumbing company use the information for marketing purposes?

A. Yes. This is permissible because you disclosed nonpublic personal information to the plumbing company in accordance with the notice and opt out provisions of the GLB Act. § 502(a)-(b) of the Act, codified at 15 U.S.C. § 6802(a)-(b). In other words, you disclosed information about a consumer consistent with your privacy notice and the consumer's choice not to opt out.

As illustrated in the following questions and answers, when the plumbing company receives from you nonpublic personal information about a consumer who has not elected to opt out, the company is free to use the information for marketing or other purposes. However, the plumbing company may disclose the nonpublic personal information it receives from you only if such a disclosure is consistent with the restrictions on disclosure of the information described in your privacy policy. § 40.11(d). The plumbing company therefore is required to honor any subsequent opt out elections made by consumers pursuant to your privacy policy and accordingly must have a mechanism through which it can monitor and implement subsequent opt out elections you receive.

5. Q. One of my affiliates sells insurance. May the plumbing company, who received my customers' information outside an exception, disclose that information to my affiliated insurer?

A. Yes. The Privacy Rule explicitly provides that the plumbing company may disclose the information to your affiliate. § 40.11(d)(1).

6. Q. I disclosed information to the plumbing company outside an exception. The plumbing company is affiliated with an air conditioning company. The air conditioning company is not affiliated with me. May the plumbing company disclose my consumers' nonpublic personal information to that air conditioning company?

A. Yes. The Privacy Rule permits a party that receives nonpublic personal information outside of an exception to disclose that information to its affiliates. In this case, therefore, the plumbing company may disclose the information to its affiliated air conditioning company. However, the affiliated air conditioning company may, in turn, disclose the information only to the extent that the plumbing company may, consistent with your privacy notice. § 40.11(d)(2).

7. Q. I disclosed information to the plumbing company outside an exception. May the plumbing company disclose my consumers' nonpublic personal information to a nonaffiliated automobile parts retailer?

A. Yes. The Privacy Rule permits a party that receives nonpublic personal information outside of an exception to disclose that information to another nonaffiliated third party, provided that it would be lawful for the original financial institution to make that disclosure directly to that party. Under your

privacy notice, it would be lawful for you to disclose nonpublic personal information about those consumers who chose not to opt out to the automobile parts retailer. § 40.11(d)(3). However, the plumbing company could not disclose nonpublic personal information obtained from you to other nonaffiliated retailers if your privacy policy would not permit such disclosures.

H. Complying with the limitation on disclosing account numbers

1. Q. I am a depository institution. I transform my customers' account numbers into encrypted forms that can be used solely to identify those customers. I enter into an arrangement with a third party telemarketing firm whereby I disclose my customers' names, telephone numbers, and encrypted identifying numbers. The third party telemarketing firm uses that information to market products (other than products I offer) to those customers. For those customers who agree to purchase the products, the third party telemarketing firm submits their encrypted identifying numbers to me, and I decrypt them into account numbers. At the end of this process, am I permitted to disclose the customers' actual account numbers to the third party telemarketing firm so that the telemarketing firm can initiate the charges to the customers' accounts?

A. No. Section 40.12 generally prohibits you from disclosing credit card, deposit, or other transaction account numbers "for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." Accordingly, you must not provide your customers' account numbers to the third party telemarketing firm "for use in telemarketing."

The primary reason a marketer seeks access to a customer's account number is to allow the marketer to initiate a charge to the customer's account as part of the transaction. Section 40.12 prohibits you from disclosing customer transaction account numbers to the third party telemarketing firm to initiate a charge to a customer's account even after a customer accepts the product. Moreover, the general exceptions for notice and opt out under §§ 40.14 and 40.15, including the exception for disclosing information with the consent or at the direction of the consumer, do not apply to disclosures of account numbers for use in marketing that are prohibited by § 40.12.

Section 40.12 provides only three exceptions. A financial institution may disclose its customers' account numbers to: (i) a consumer reporting agency; (ii) its agent to market the institution's own products or services, provided that the agent is not authorized to directly initiate charges to the account; or (iii) another participant in a private label credit card or an affinity or similar program involving the institution. Because none of these exceptions applies in your case, you must not provide your customers' account numbers to a third party telemarketing firm so that it can initiate the charges to the customers' accounts.

2. Q. I would like to enter into an arrangement with a nonaffiliated insurance agency that markets its products to my customers through direct mail solicitations. The proposed arrangement contemplates that I would disclose a customer's account number to the insurance agency's affiliate. The affiliate then would use the account number to debit the purchase price from my customer's account in response to these solicitations. The affiliate's only role in the arrangement would be initiating the charges. Does the Privacy Rule allow me to disclose a customer's account number to the insurance agency's affiliate under these circumstances?

A. No. The Privacy Rule prohibits you from disclosing your customers' account numbers to *any* nonaffiliated third party for use in marketing. § 40.12(a). Although the affiliate in your hypothetical does not distribute marketing materials but only initiates charges, its conduct of that activity is an integral part of your marketing arrangement with the insurance company. The disclosure of a customer's account number to the insurance company's affiliate under these circumstances therefore would be a disclosure for use in marketing that violates the Privacy Rule.

I. Disclosing nonpublic personal information under the exceptions to the notice and opt out provisions

1. Q. I offer consumer checking accounts. I notify my customers that, among other things, I make disclosures as permitted by law. Merchants sometimes call me and ask whether a particular consumer's checking account has sufficient funds to cover a check to the merchant. How does the Privacy Rule apply to my response to the merchant's question?

A. The Privacy Rule allows you to disclose nonpublic personal information about your consumers without providing them a reasonable opportunity to opt out under certain circumstances. These exceptions to the opt out requirement are described at §§ 40.13 – 40.15 of the Privacy Rule. For example, you do not need to allow your customer to opt out of a disclosure made in connection with processing or clearing checks (§ 40.14(b)(2)(vi)(A)) or for the purposes of preventing actual or potential fraud, unauthorized transactions, claims, or other liability (§ 40.15(a)(2)(ii)). Therefore, if you have notified your customer that you make disclosures as permitted by law, you may disclose whether your customer's checking account has sufficient funds to cover a check, regardless of whether or not the customer has exercised his or her opt out rights.

Be aware of the possibility that the caller may be attempting to obtain information about your customer through false or fraudulent statements to you. Toward this end, you must ensure that you respond to the caller in accordance with the controls you have implemented as part of your information security program, as required by the applicable provisions of the banking agencies' Interagency Guidelines Establishing Standards for Safeguarding

Customer Information (the "security guidelines"). *See* 66 Fed. Reg. 8616 (February 1, 2001).

2. Q. While we may confirm funds availability to a merchant where our customer seeks to pay for merchandise with a check under the exceptions in §§ 40.14 and 40.15, may we confirm funds availability to an individual who is not a merchant for the same purpose? For instance, if our customer wants to use a check to purchase a used car from an individual seller, may we respond to the seller's request about the availability of funds in the customer's account under these exceptions?

A. Whether or not someone is a "merchant" is not material to determining if you may disclose customer information pursuant to the exceptions in §§ 40.14 and 40.15. You should determine whether the third party to whom you intend to disclose information actually is involved in carrying out a financial transaction that is requested or authorized by your customer. Check verification is permitted under the exceptions to the notice and opt out provisions, such as in connection with processing or clearing a check under § 40.14(b)(2)(vi)(A), and under § 40.15(a)(2)(ii) to protect against or prevent actual or potential fraud or unauthorized transactions.

As discussed in the answer above, if you make such a disclosure you should take appropriate measures to ensure that the individual inquiring has a legitimate need for the information and is not engaging in an attempt to obtain customer information fraudulently. Concerns about properly safeguarding customer information are heightened in a situation in which you disclose nonpublic personal information to an individual rather than to a known merchant.

3. Q. I offer consumer checking accounts. I notify my customers that, among other things, I make disclosures as permitted by law. My checking account customers deposit checks made payable to my customer but drawn on a financial institution unaffiliated with me. My practice is to write my customer's account number on the back of the deposited check to facilitate its processing. The check itself then goes to the maker's financial institution, with my customer's account number on the check. Is this a disclosure of nonpublic personal information that would be subject to opt out requirements or the prohibition against sharing account numbers?

A. No. The opt out provisions do not apply to disclosures in connection with servicing or processing a financial product or service that a consumer requests or authorizes. Nor do they apply to disclosures that are required, or are a usual, appropriate, or acceptable method in connection with settling, processing, clearing, transferring, reconciling or collecting amounts charged, debited or otherwise paid. §§ 40.14(a), 40.14(b)(2)(vi)(A). Also, because the account number is added to the check solely for use in processing the check and is not used in connection with marketing by a third party, this

disclosure is not prohibited by the ban on disclosing account numbers for marketing purposes. § 40.12.

4. Q. I made a loan to a consumer who defaulted. In trying to collect the bad loan, I wish to learn information to locate the defaulting borrower. I believe that a financial institution unaffiliated with me may have some helpful information about the borrower. If I were to ask that institution for information, I would disclose nonpublic personal information, such as the fact that I have a loan to a particular consumer. I previously notified my borrower that, among other things, I make disclosures as permitted by law. Must I allow my borrower to opt out of my question to the financial institution?

A. No. You may disclose nonpublic personal information to the financial institution without complying with the opt out provisions as necessary to enforce a consumer loan where the disclosure is required or is one of the lawful or appropriate methods to enforce your rights. § 40.14(b)(1).

5. Q. A financial institution that is not affiliated with me made a loan to a consumer who defaulted. In trying to collect the bad loan, the lender wishes to learn information to locate the defaulting borrower. The lender believes that I may have some helpful information about the borrower and asks me to disclose nonpublic personal information. I notify my consumers that, among other things, I make disclosures as permitted by law. May I disclose nonpublic personal information to help the lender try to collect a bad loan without providing opt out notices?

A. Where you have notified your consumer that you make disclosures as permitted by law, you may make disclosures to "persons holding a legal or beneficial interest relating to the consumer," or under the appropriate circumstances, "to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability," without providing opt out notices and a reasonable opportunity for a consumer to opt out. § 40.15(a)(2)(iv); § 40.15(a)(2)(ii). Thus, disclosures to the lender may be permissible without complying with the opt out provisions.

As stated above, you must be aware of the possibility that the party requesting the information may be attempting to obtain that information about your customer through false or fraudulent statements to you.

6. Q. I make consumer loans. I notify my customers that, among other things, I make disclosures as permitted by law. A state law requires me to disclose to the state the names, addresses, social security numbers, and account balances of individuals the state believes have failed to make required child support payments. Does the Privacy Rule require me to allow my customers to opt out of disclosures to the state under this state law?

A. No. The Privacy Rule exempts from the opt out provisions any disclosures you make "[t]o comply with Federal, State, or local laws, rules and other applicable legal requirements." § 40.15(a)(7)(i).

7. Q. Must I provide a privacy notice to consumers who are not my customers when I have to report information about denied mortgage applicants under the Home Mortgage Disclosure Act ("HMDA")?

A. No. If the information that HMDA requires you to disclose is not personally identifiable, the Privacy Rule would not apply to your disclosure of that information. Alternatively, if you disclose nonpublic personal information to comply with the law, you may disclose the information under § 40.15(a)(7)(i) without providing a privacy notice to consumers who are not your customers.

8. Q. We often receive phone calls from auto dealers or other financial institutions requesting loan pay-off amounts on our customers. May we respond to these requests without providing those customers with a reasonable opportunity to opt out of that kind of disclosure?

A. Yes, if the disclosure is in connection with servicing or processing a financial product or service from the third party that the customer has requested or authorized. In your case, for example, you may disclose loan pay-off information to a third party lender where your customer seeks to refinance the bank loan with the other lender. Alternatively, you may disclose nonpublic personal information that is required, or is a usual, appropriate or acceptable method to carry out the transaction that the customer has requested or authorized § 40.14(a). This would be the case, for example, if the car dealer accepts your customer's car as partial consideration for the purchase of another vehicle and wants to know the outstanding amount on the customer's car loan with you.

As discussed in response to several of the questions above, you should be aware of the possibility that the caller may be attempting to obtain information about your customer through false or fraudulent statements to you. Toward this end, you must ensure that you respond to the caller in accordance with the controls you have implemented as part of your information security program.

9. Q. During the ordinary course of business, I may request proof of insurance from a nonaffiliated insurance agency on an automobile that serves as our collateral on a customer's loan. May I disclose customer information to the insurance agency in order to obtain this information without triggering specific notice and opt out requirements?

A. Yes, you may disclose nonpublic personal information, such as the existence of your relationship with a particular customer, to a nonaffiliated

insurance agency in order to obtain proof of insurance under the exceptions to the specific notice and opt out requirements in § 40.14. For example, you could disclose nonpublic personal information under the exception in § 40.14(b)(1) as a lawful or appropriate method to enforce your rights in providing the loan.

10. Q. I make wire transfers for consumers who are not otherwise my customers. Do I have to provide an initial privacy notice to these consumers when I only make a wire transfer for them?

A. No. Processing a wire transfer for a consumer on a one-time basis would not create a customer relationship, even if the consumer repeatedly requests that one-time service. Accordingly, you do not owe the consumer an initial notice on that basis. Furthermore, this disclosure would fall under the exception for processing a transaction that a consumer has requested or authorized. § 40.14(a)(1). Consequently, you would not be required to provide any privacy notices unless you also disclosed nonpublic personal information about the consumer to nonaffiliated third parties outside of an exception under § 40.14 or § 40.15. *See* § 40.4(a)(2).

11. Q. I use a nonaffiliated third party to service consumer loans, and in this arrangement I disclose to the servicer nonpublic personal information about my borrowers. This arrangement seems to qualify for an exception from both the notice and opt out requirements, under § 40.14(a)(1). At the same time, this arrangement seems to qualify for an exception from opt out requirements—but not from notice requirements—under § 40.13(a)(1). The latter exception requires me to provide notice to consumers of the disclosures, and requires language in our contract that restricts the servicer's further disclosure and use of the nonpublic personal information. When a servicing arrangement qualifies for two differing exceptions, which applies?

A. When a disclosure qualifies for both the § 40.13 exception and a § 40.14 or § 40.15 exception, you do not need to comply with the notice and confidentiality provisions under § 40.13. Instead, you may make that disclosure solely in accordance with an exception under § 40.14 or § 40.15.

12. Q. A community bank has an agreement with a mortgage company to prequalify mortgage loan applicants prior to referring them to the mortgage company for underwriting. As part of this agreement, the community bank, among other things, (1) educates applicants about home buying and about different types of loan products available; (2) collects financial information and related documents; (3) assists the applicant in understanding and resolving credit problems; and (4) maintains regular contact with the applicant during the loan process to apprise the applicant of the status of the application.

The community bank forwards the completed loan application to the mortgage company for underwriting, origination and servicing. After the loan is

approved, the community bank has no further contact with the applicant with respect to the applicant's loan.

Does the bank have to provide an initial privacy notice to the applicant? If so, does the bank have to disclose this information sharing arrangement in its privacy notice, or is it covered by an exception in § 40.14 or § 40.15?

A. If the bank does not already have a customer relationship with the loan applicant, the services that the bank performs pursuant to this program appear to give rise to a customer relationship between the applicant and the bank as described in § 40.3(i)(2)(i)(F), at least until the applicant has completed the loan process. As a result, the bank would have to provide an initial privacy notice. Whether the bank must disclose the information sharing arrangement with the mortgage company in its privacy notice depends on whether the disclosure is permitted under one of the exceptions in §§ 40.13, 40.14, or 40.15.

If the bank and the mortgage company have an agreement to jointly offer, endorse, or sponsor the mortgage company's loan product as described in § 40.13 and otherwise comply with the confidentiality requirements of this section, the bank would have to describe this arrangement in its privacy notice in accordance with § 40.6(a)(5).

Where the bank discloses to the applicant that the mortgage loan will be made by the mortgage company and not the bank, the bank's disclosure of the applicant's nonpublic personal information to the mortgage company would fall within the exception in § 40.14(a)(1), to service or process a financial product the consumer has requested. The bank would not have to specifically describe this information sharing arrangement in its privacy notice as long as the notice states that the bank makes disclosures to nonaffiliated third parties as permitted by law. § 40.6(b).

Finally, the bank could obtain the applicant's specific consent to disclose the applicant's nonpublic personal information to the mortgage company so the applicant may obtain the loan. In that event, the disclosure would fall within the exception in § 40.15(a)(1). The bank's privacy notice may refer to this disclosure as "permitted by law." § 40.6(b).

Where the disclosure of information may be made pursuant to an exception under both § 40.13 and either § 40.14 or § 40.15, the bank may rely on the latter exceptions, and therefore would not have to specifically describe in its privacy notice its disclosure arrangements under § 40.6(a)(5).

The mortgage company also will establish a customer relationship with any applicant for whom it originates a loan, and will have to provide a notice of its privacy policies not later than when it establishes the customer relationship.

J. Complying with the exception to the opt out provisions for joint marketing arrangements

1. Q. I disclose my consumer borrowers' names and addresses to a nonaffiliated insurance company. The insurance company sends the borrowers a letter, on my letterhead, offering insurance. I do not sell insurance. Does this arrangement qualify for the § 40.13 joint marketing agreement exception? Must the products described in the marketing materials be our products?

A. The exception to the opt out requirement in § 40.13 applies to disclosures you make to nonaffiliated third parties pursuant to a joint written agreement between you and one or more financial institutions under which you and the other financial institution(s) jointly offer, endorse, or sponsor a financial product or service. You may disclose your consumer borrowers' names and addresses to the insurance company under § 40.13 because (i) the insurance company is a financial institution, (ii) insurance is a financial product or service, and (iii) you and the insurance company market the insurance together. The financial product you offer, sponsor or endorse under a joint agreement with another financial institution need not be your product.

You and the insurance company must have a written agreement that restricts the insurance company from disclosing or using the borrowers' nonpublic personal information for any purpose other than selling insurance to the borrowers. Furthermore, you must describe this type of arrangement in your privacy notice in accordance with § 40.6(a)(5).

2. Q. I disclose my consumer borrowers' names and addresses to a nonaffiliated retail merchant that sells household goods, hardware, and clothing. The retail merchant wants to send notices, on my letterhead, offering household products. Would this arrangement qualify for the § 40.13 joint marketing agreement exception?

A. No. To qualify for the § 40.13 exception, a joint marketing arrangement must be an agreement between financial institutions for offering, endorsing, or sponsoring financial products or services.

3. Q. Each month I mail account statements to my customers. May I include marketing materials for a third party vendor's products in my mailings to my customers? I do not have a joint marketing agreement under § 40.13 with the vendor.

A. Yes. However, you must be careful not to facilitate your customer's unwitting disclosure of his or her nonpublic personal information to the vendor by virtue of a response to the marketing materials. For example, the vendor may

have printed a reference code on its marketing materials that indicates that the offer for that product was sent to your customers who share certain financial characteristics. From this code, the vendor would be able to determine that the individual who responds to the marketing materials that you delivered is your customer or holds certain kinds of assets. In that case, you would have disclosed nonpublic personal information about the customer to the vendor.

To comply with the Privacy Rule under these circumstances, you must either describe these types of marketing arrangements in your initial, annual, or revised privacy notice and provide your customer with a reasonable opportunity to opt out or obtain your customer's specific consent to such arrangements. Alternatively, you may structure the marketing materials so your customer knows that by responding he or she would be disclosing certain categories of nonpublic personal information about himself or herself.

4. Q. I am a bank. I have a financial advisory center on my premises that is operated by people employed both by me and by an insurance company. The shared employees do not sell bank products. They sell insurance products and services offered by the insurance company pursuant to a third-party arrangement. We provide the employees with information about our customers so that they may solicit our customers on behalf of the insurance company. Do we have to provide our customers with an opportunity to opt out of these disclosures?

A. You must provide a reasonable opportunity for your customers to opt out of any disclosure of their nonpublic personal information to a nonaffiliated third party unless one of the exceptions applies. Although a dual employee himself or herself is not a "nonaffiliated third party," providing customer information to a dual employee for purposes of marketing the insurance company's products and services to your customers is deemed to be providing the information directly to the insurance company. Because the insurance company is a nonaffiliated third party, you must provide your customers a reasonable opportunity to opt out of disclosure of their nonpublic personal information prior to disclosing such information to the dual employees unless the disclosure is covered by an exception.

The exception at § 40.13 specifically permits you to disclose nonpublic personal information about your customer to the nonaffiliated insurance company without providing the customer an opportunity to opt out if three requirements are met:

- The insurance company must market financial products or services offered under a joint agreement between you and the insurance company. The joint agreement must be a written agreement under which you and the insurance company "jointly offer, endorse, or sponsor" a financial product or service. Simply agreeing to share customer

information with the insurance company would not satisfy this contractual requirement. Rather, your agreement with the insurance company must provide for the joint offering, endorsement, or sponsorship of the financial product or service. For example, a third-party agreement that provides the insurance company will use your name in its marketing materials or offer insurance products and services on your premises would demonstrate that you are jointly offering, endorsing, or sponsoring the products or services with the insurance company;

- You must have provided your customers with an initial privacy notice, including a separate statement describing your joint marketing that satisfies § 40.6(a)(5); and
- You must have a written contract that restricts the insurance company from disclosing or using your customer's nonpublic personal information for any purpose other than to offer insurance products and services to those customers.

In addition to the foregoing requirements, the prohibition against disclosing a consumer's account number for use in telemarketing, direct mail marketing, or other marketing through electronic mail, as set forth in § 40.12, applies to your arrangement with the insurance company.

5. Q. Must I have a confidentiality and security clause in all my contracts with service providers who have access to customer information?

A. Both the privacy regulations and the banking agencies' security guidelines require financial institutions to enter into contracts with service providers that address customer information in particular circumstances. The requirements differ, however, and those differences are as follows:

Under § 40.13 of the Privacy Rule, you may share nonpublic personal information with a servicer, without providing a consumer with the right to opt out of this disclosure, if you have a contract with the servicer that *limits the servicer's ability to further use or disclose this information.* The Privacy Rule does not require you to have such a contract clause in place prior to disclosing information to any servicer —only those servicing arrangements that fall within § 40.13. If the servicing arrangement is within the scope of the exceptions in §§ 40.14 and 40.15, you may disclose information to the servicer without a contract that limits the servicer's ability to use or disclose nonpublic personal information. In those instances, the servicer will be subject to the limits on reuse and redisclosure under § 40.11.

Under III.D.2 of the security guidelines, you must provide by contract with each of your service providers that has access to customer information that it *undertakes security measures that will protect your customer information*. The supplementary materials to the guidelines explain that a service

provider must implement controls that satisfy the objectives of the guidelines, yet need not have a security program that is identical to the program that financial institutions themselves must implement under the guidelines.

There is a different transition rule for each of these contract clauses. Section 40.18 of the Privacy Rule states that a contract entered into on or before July 1, 2000, must be brought into compliance with the provisions of § 40.13 by July 1, 2002. Contracts entered into after July 1, 2000, should have been brought into compliance by July 1, 2001. The security guidelines provide that a contract entered into on or before March 5, 2001, between a bank and service provider must be brought into compliance with the security guidelines by July 1, 2003. Contracts entered into after March 5, 2001, should have been brought into compliance by July 1, 2001.