OCC Staff Responses to Questions from February 13-14, 2001, Telephone Seminar on Privacy Regulation Compliance

[Most recent questions and answers appear in bold text]

Scope of the rule -- Section 40.1

- Is a bank required to provide privacy notices to customers who live in another country? (Q12, 25)

  Yes. Part 40 applies to all United States offices of entities for which the OCC has primary supervisory authority, regardless of where the customer lives. (Posted 5/29/01)

Clear and conspicuous -- Section 40.3(b)

- Are banks required to provide a privacy notice in Braille to visually impaired customers or in an alternative language to consumers who do not speak English? (Q14)

  The regulations require that all privacy notices (initial, annual, revised and opt out notices) be clear and conspicuous. Section 40.3(b)(1) defines a clear and conspicuous notice as one that is reasonably understandable and designed to call attention to the nature and significance of the information in the notice. If for example, the bank provides loan documents in Spanish to Spanish-speaking customers, we encourage the bank to provide its privacy and opt out notices to those customers in Spanish. However, this is not a requirement under the regulations. (Posted 5/29/01)

Definition of consumer and financial institution -- Sections 40.3(e); 40.3(k)

- Are business customers of a bank covered by the privacy rule? (Q8)

  No, business customers are not covered by the privacy regulations. A bank's obligations under the regulations are only to those customers who are consumers, meaning, individuals who obtain a financial product or service from the bank primarily for personal, family, or household purposes. (Posted 5/29/01)

- Are sole proprietors exempt from the regulations? (Q30)

  This question raises three related issues:

  1. Will a sole proprietor who conducts business with a financial institution be deemed a "consumer" and therefore subject to the regulations? No, sole proprietors will not be "consumers" under the rule. A "consumer" is defined as an individual who obtains or has obtained a financial product or service from a bank that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

Thus, the disclosure of information relating to business customers of a bank, including sole proprietorships, generally would not be restricted by the rule, because the information does not relate to a consumer.

2. If sole proprietors are not consumers, are there instances in which information obtained about the individual may be protected under the privacy rule? Yes. For instance, if a bank received nonpublic personal information about an individual who has both a consumer and commercial relationship with the bank, the privacy rule protects all the nonpublic personal information the bank has obtained in connection with providing the consumer financial products or services. The protection afforded an individual consumer's nonpublic personal information under the rule is not lost because a bank may have collected the same information in connection with providing the individual a commercial product or service.

3. May sole proprietors be "financial institutions" and, therefore, subject to the regulations? This depends on whether the sole proprietor is significantly engaged in activities that are financial in nature or incidental to such financial activities as described in §4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). For further guidance on this question, you should consult the privacy regulations of the Federal Trade Commission, which has primary jurisdiction under Title V of the Gramm-Leach-Bliley Act over financial institutions that are not subject to the jurisdiction of any of the other agencies or authorities with rulemaking responsibility under this Title. *See* 16 C.F.R. Part 313. (Posted 5/29/01)

Definition of customer relationship -- Section 40.3(i)

- If a consumer applies for and receives a credit card, and includes in the application two authorized users (such as a spouse and a child), is the bank obligated under the rule to provide any privacy notices to the authorized users? May the bank assume that an applicant's (account holder's) opt out of information disclosures would also apply to the authorized users? (Q23)

  Assuming the authorized users are not liable to the bank for their use of the credit card, the bank's customer relationship for purposes of the regulations is only with the applicant. Therefore, the bank needs to provide a privacy notice and opt out notice only to the applicant. However, any nonpublic personal information that the bank obtains in connection with the account, including information about the authorized users, would be considered the account holder's information and subject to the same requirements under the rule as other information the bank collects about the account holder. (Posted 5/29/01)

- **Is a guarantor or an endorser of a consumer loan considered a bank's consumer or customer? (Q9)**

  A guarantor or endorser of a consumer loan is a bank's customer, because the person receives an extension of credit from the bank. A bank may, however, treat the primary borrower and the guarantor/endorser as joint account holders. As a result, the bank may deliver a single privacy notice to the joint account holders in accordance with §40.9(g). If the bank discloses

information to nonaffiliated third parties outside of the exceptions in §§40.13, .14, and .15, the bank must also allow the primary borrower and the guarantor/endorser to opt out. The bank may deliver a single opt out notice to the joint account holders under §40.7(d). (Posted 8/28/01)

Definition of nonpublic personal information X Section 40.3(n)

- **A bank's Web site has a portal link to a Web site of a nonaffiliated third party that offers products and services. Visitors to the bank's Web site (bank customers, consumers, or a person merely browsing the bank's site) may access this third party Web site. If a bank customer or consumer clicks onto this site from the bank's Web site, would the bank be disclosing nonpublic personal information? (Q15)**

  A bank does not disclose nonpublic personal information if it only provides a link to a third party's Web site that is available to anyone who browses the bank's site and the bank does not identify its customers and consumers to the third party or discloses any other nonpublic personal information about those customers or consumers. (Posted 8/28/01)

Initial privacy notices -- Section 40.4

- If a bank discloses information about its *customers* only under the exceptions in §§40.13, .14, and .15, and discloses information about its *consumers* only under the exceptions in §§40.14 and 40.15, must the bank provide a privacy notice on or at its ATM? (Q26)

  A bank is under no obligation to provide its consumers who do not have customer relationships with the bank with any privacy notices, *unless* the bank intends to disclose the consumers' nonpublic personal information to nonaffiliated third parties outside the exceptions in §§40.14 and 40.15. If the bank discloses information about *consumers* only under these exceptions, the bank has no obligation to provide them with a privacy notice. Of course, a bank must provide a privacy notice to each of its *customers* and deliver the notice in accordance with §40.9 even if it discloses information about its customers only under the exceptions in §§40.13, .14, and .15. (Posted 5/29/01)

- Is it necessary to provide an individual consumer who is not a customer of the bank a privacy notice when the bank sells and redeems savings bonds for the individual? (Q45)

  No. Under these circumstances, a bank is not obligated to provide a privacy notice to an individual for whom it performs this service. The bank does not establish a customer relationship with the individual solely by selling or redeeming U.S. savings bonds and thus acting as an agent for the U.S. Treasury Department. Accordingly, if the bank submits this information only to the U.S. Treasury to process the transaction, the bank has no disclosure obligations to its consumers. (Posted 5/29/01)

- Is it necessary to provide an individual consumer who is not a customer of the bank an initial privacy notice when the bank makes a wire transfer on the individual's behalf for a fee? (Q45)

  No. Processing a wire transfer for a consumer would not create a customer relationship, and would fall under the exception provided in §40.14(a)(1) (processing a financial product or service that the consumer requests or authorizes). As a result, if the information disclosure were limited to processing the transaction, the bank would not have to provide any privacy notices to consumers for whom they provide this service. (Posted 5/29/01)

- Must a small bank that does not disclose nonpublic personal information to any nonaffiliated third party except as allowed by law for customary operations (and that therefore has a very simple privacy policy) send an initial privacy notice to existing consumer loan and time deposit customers?

  Yes. The bank must provide an initial privacy notice to its existing customers by July 1, 2001. The bank is required to provide an initial notice, for example, to a customer who has a deposit or investment account, or obtains a loan from the bank for which the bank retains ownership of the servicing rights. If the bank does not retain servicing rights to a loan, however, the bank would not have to provide an initial privacy notice -- even if the bank retains the asset -- except in two circumstances. The first is when the bank wants to disclose nonpublic personal information about the recipient of the loan pursuant to §40.13. In that case, the bank would have to provide an initial notice that includes a separate statement about its disclosure arrangements under §40.13. The second is when the bank wants to disclose nonpublic personal information to nonaffiliated third parties outside of the exceptions. In that case, the bank would have to provide both an initial notice and an opt out notice. (Posted 5/29/01)

- If a bank discloses nonpublic personal information to nonaffiliated third parties only under the exceptions in §§40.14 and 40.15, but its notice indicates that the bank *may* disclose nonpublic personal information outside of these exceptions in order to preserve its options, must the bank send the first initial privacy notice to all of its customers (including former customers)? (Q46)

  The bank must provide an initial privacy notice to all current bank customers. Additionally, before it discloses customer information outside of the regulatory exceptions, the bank must provide its customers with an opt out notice and a reasonable opportunity to opt out. A bank has no obligation to provide its former customers with an initial notice by July 1 unless the bank plans to disclose their information outside of the exceptions in §§40.14 and 40.15. In those instances, the bank must provide the required notices to its former customers prior to disclosing their nonpublic personal information -- i.e., a privacy notice containing a separate statement about the bank's information disclosure arrangements under §40.13, or a privacy notice and opt out notice if the bank discloses information

outside of the exceptions in §§40.13, 40.14, and 40.15. (Posted 5/29/01)

- Must a bank provide a privacy notice to consumers (who are not customers) if the bank discloses information about those consumers as required by federal law, such as information about denied mortgage applicants under the Home Mortgage Disclosure Act? (Q15)

  No. If the information that the bank is required to disclose is not personally identifiable, Part 40 would not apply. Alternatively, if the bank discloses nonpublic personal information to comply with the law, the bank may disclose the information without providing consumers a privacy notice under §40.15(a)(7) (to comply with federal, state, or local laws). The privacy rule does not require a bank to provide privacy notices to consumers who are not customers if the bank makes disclosures only as permitted by §§40.14 and 40.15. (Posted 5/29/01)

Termination of customer relationship -- Section 40.5(b)

- Does a financial institution need to send an initial privacy notice by July 1, 2001 to credit card holders whose accounts have been written off, who no longer have the right to use the credit card, and whose only written contact from the financial institution is through collection correspondences? (Q4)

  No, provided the institution is disclosing information about these individuals only under §§40.14 and 40.15. If the institution's only communication with the card holder is for the collection of a debt that has been charged off, that is not a statement or notice for the purposes of §40.5(b)(2)(iii) and the card holder may be considered a former customer.

  Note that former customers are considered consumers under the regulations. The definition of consumer (§40.3(e)(1)) includes an individual who *has obtained* a financial product or service from a bank. Accordingly, if an institution discloses information about its former customers only under the exceptions in §§40.14 and 40.15, the institution does not have to provide them with a privacy notice. If the institution also discloses nonpublic personal information about its former customers under §40.13, the institution does have to provide its former customers with a privacy notice. If the disclosure is outside of the exceptions, the institution must provide those former customers an initial privacy notice, an opt out notice, and a reasonable opportunity to opt out of the disclosure. (Posted 5/29/01)

Simplified notice -- Section 40.6(c)(5)

- The supplementary material to the rule includes "Guidance for Certain Institutions" (p. 35186 of the Federal Register). This guidance states that a bank may use a simplified notice if the bank does not have any affiliates and only discloses nonpublic personal information to nonaffiliated third parties under the routine business exceptions in §§40.14 and 40.15. May a bank also use a simplified notice if it has

affiliates but doesn't share any nonpublic personal information with them? (Q9)

Yes. A bank may use the simplified notice if the bank does not disclose nonpublic personal information to its affiliates outside of the exceptions in §§40.14 or 40.15, and if the bank is not required to include a disclosure in its privacy notice about affiliate information sharing under the FCRA. (Posted 5/29/01)

Opt out -- Section 40.7

- If a bank's privacy notice allows the customer to mail in a form indicating the customer's opt out election, is the bank required to include a pre-paid postage mailer with the form? (Q10)

  No. A bank is not required to provide an individual with a pre-paid mailer to meet the requirement in §40.7(a)(1)(iii) that the bank provide a reasonable means for consumers to opt out. (Posted 5/29/01)

Joint Notice -- Section 40.9(f)

- Where a bank holding company has developed a single privacy notice on behalf of all its subsidiaries, is the company required to list each of the legal entities that are providing the privacy notice by its legal name, or will a more generic "all subsidiaries and affiliates of ABC & Company" satisfy the rule's requirements? (Q61)

  The bank holding company does not have to list each entity by its legal name as long as the notice clearly identifies the institutions covered by the privacy policy. For instance, a privacy notice for ABC & Company could state that it applies to all institutions with the ABC name. Any affiliated company that does not share the ABC name would then need to be separately identified in the notice. (Posted 5/29/01)

- Where a bank has an insurance agency affiliate and a broker-dealer affiliate, must each of these affiliates provide privacy notices to its customers? May the bank provide a single notice on behalf of the bank and these affiliates? (Q41)

  Both the insurance agency affiliate and the broker-dealer affiliate must provide privacy notices to their customers. However, §40.9(f) permits a bank to provide a joint notice with one or more of its affiliates or other financial institutions, as long as the notice is accurate for the bank and the other parties, and the entities using the notice are adequately identified as described in response to Q61. (Posted 5/29/01)

Contract Provisions -- Section 40.13 and Interagency Guidelines Establishing Standards for Safeguarding Customer Information

- What is the difference between the service provider contract provision referenced in § 40.13 of the privacy rules and the contract provision in 12 C.F.R. § 30, Appendix B,

the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (the security guidelines)? (Q55)

Under §40.13 of the privacy rule, a bank may share nonpublic personal information with a servicer, without providing a consumer with the right to opt out of this disclosure, if the bank has a contract with the servicer that *limits the servicer's ability to further use or disclose this information*. The privacy rule does not require a bank 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, a bank 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, all banks must monitor service provider arrangements by entering into contracts with their service providers requiring the providers to *undertake security measures that will protect the bank's customer information*. The preamble to the guidelines explains 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 must be 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 a service provider, must be brought into compliance with the provisions of 12 C.F.R. Part 30, Appendix B, III.D.2, by July 1, 2003. See 12 C.F.R. Part 30, Appendix B, III.G.2. Contracts entered into after March 5, 2001, must be brought into compliance by July 1, 2001. (Posted 5/29/01)

- Is there a sample or generic confidentiality clause for third party contracts under §40.13 to which a bank can refer? (Q21, 43)

  The agencies have not issued such sample clauses. Institutions may wish to consult with bank counsel or contact a bank trade association for assistance. (Posted 5/29/01)

Joint agreement X Section 40.13

- **If a bank's investment center sells only investment products offered by a nonaffiliated brokerage firm, may the bank enter into a joint agreement with that firm, or must the products at issue be bank products to qualify for the exception in §40.13? (Q39)**

The joint marketing agreement under §40.13 applies to bank products as well as financial products or services sold by another financial institution. Thus, the fact that the product in question is not a bank product does not preclude the arrangement from satisfying §40.13. (Posted 8/28/01)

Disclosures under exceptions in Sections 40.14 and 40.15

- In an indirect lending arrangement with a car dealership, if a bank denies a loan that a consumer applies for through the dealership, may the bank disclose the reason for the denial to the dealership? (Q15)

  Where the bank has received an individual's loan application through a dealer, it may be a usual or appropriate practice for a bank to communicate a denial to the consumer through the dealer in order to provide information about the status of the loan. Section 202.9(g) of Regulation B, which implements the Equal Credit Opportunity Act, permits a creditor to disclose reasons for taking an adverse action through a third party where the third party submits an application to a creditor on behalf of the consumer. Accordingly, a bank may disclose to a car dealership the reasons the bank denied a loan to a consumer pursuant to §§40.14(a) and (b)(2)(iii) -- as a usual, acceptable, or appropriate method to provide information on the status of a financial product to the consumer's agent or broker with respect to a product a consumer has requested. If the bank obtains the
  consumer's consent for the specific disclosure, this information also may be disclosed under §40.15(a)(1). Because the dealer receives nonpublic personal information from the bank, and the bank discloses the information under an exception, the dealer's ability to reuse and redisclose the consumer information is limited by the rules. (Posted 5/29/01)

- Where a bank currently processes all its nonpublic personal information in-house using software purchased from a nonaffiliated third party, it may occasionally have an issue that it cannot address on its own and may authorize its software provider to access the bank's system to address the problem. By accessing the mainframe, the software provider would also have access to individual customer account information. Would this disclosure violate the regulations? Is this an issue under the interagency guidelines for safeguarding customer information? (Q17)

  This would not be a violation of the privacy regulations. Providing information to a software provider to assist the bank in maintaining or servicing customer accounts, for instance, would be permitted under §40.14(a)(2) without specific notice to customers about this disclosure or an opportunity to opt out. The sharing of information with a service provider under the circumstances posed may fall within that exception. Also, §40.15 permits a bank to disclose information to protect the confidentiality or security of the bank's records, or for required institutional risk control, without specific notice or opt out. When a bank makes disclosures to nonaffiliated third parties under the exceptions in §§40.14 and 40.15, it may refer to such disclosures in its privacy notice as "permitted by law"

in accordance with §40.6(b). The bank must also comply with the requirements concerning service providers set out in the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (66 Fed. Reg. 8616, February 1, 2001) to ensure the proper safeguarding of customer information. (Posted 5/29/01)

- May a bank disclose nonpublic personal information about its customers in response to a skiptracing call (e.g., a financial institution seeking to locate a consumer who defaulted on a loan from the institution) under any of the exceptions? (Q30, 33, and 57)

  There are exceptions to the notice and opt out requirements that may apply to the disclosure of nonpublic personal information in this situation. Information could be provided to the nonaffiliated lender under §40.15(a)(2)(iv) to "persons holding a legal or beneficial interest relating to the consumer" or where circumstances indicate, under §40.15(a)(2)(ii) to protect against or prevent fraud. However, a bank that makes such a disclosure should take appropriate measures to protect customer information from pretext calling or other fraudulent or unauthorized attempts to obtain customer information. *See* the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Part 30 (66 Fed. Reg. 8616) and OCC Advisory Letter 2001-4 on Identity Theft and Pretext Calling. (Posted 5/29/01)

- **Banks often receive phone calls from auto dealers or other financial institutions requesting loan pay-off amounts on bank customers. May a bank respond to these requests without triggering the customers' opt out rights? (Q13, 51, 57)**

  A bank may disclose nonpublic personal information about its customers to auto dealers or other financial institutions without triggering opt out rights if, for instance, the disclosure is made in connection with servicing or processing a financial product or service from the third party that the customer requested or authorized. The bank may also disclose its customers' information, if necessary, to effect, administer, or enforce a transaction between the customer and the third party, and the customer requested or authorized the transaction. These exceptions to the opt out requirement would be applicable, for example, if the car dealer accepts the bank 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 the bank. A bank may also disclose loan pay-off information to a third party lender, for instance, when the bank's customer seeks to refinance the bank loan with the other lender.

  If the bank is uncertain whether its customer is actually engaged in a transaction with a third party that would warrant disclosure under any of the exceptions in §§40.14 or 40.15, the bank should request that the third party provide evidence of the transaction or contact the customer directly. Additionally, banks that make such disclosures should take appropriate measures to protect customer information from pretext calling or other unauthorized attempts to obtain customer information. *See* the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Part 30 (66 Fed. Reg. 8616), and OCC Advisory Letter 2001-4 on Identity Theft and Pretext Calling. (Posted 8/28/01)

- **May a bank disclose nonpublic personal information to a merchant to verify the availability of funds in a customer's account to cover the customer's check to the merchant without triggering the opt out requirements? (Q42)**

  Yes. A bank may verify the availability of funds to cover a customer's check in response to a request for funds availability from a merchant without triggering the opt out rights. Such a disclosure is permissible for processing or clearing checks, under §40.14(b)(2)(vi)(A), or to prevent actual or potential fraud, under §40.15(a)(2)(ii). When a bank discloses information under these exceptions, its privacy notice may state that the bank makes disclosures to nonaffiliated third parties as permitted by law.

  However, a bank that makes such disclosures should take appropriate measures to protect customer information from pretext calling or other fraudulent or unauthorized attempts to obtain customer information. *See* the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Part 30 (66 Fed. Reg. 8616) and OCC Advisory Letter 2001-4 on Identity Theft and Pretext Calling. (Posted 8/28/01)

- **The exceptions in sections 40.14 and 40.15 permit a bank to confirm funds availability to a merchant when the bank's customer seeks to pay for merchandise with a check. May the bank confirm funds availability to a person who is not a merchant for the same purpose? For instance, if a bank customer wants to use a check to purchase a used car from an individual seller, may the bank respond to the seller's request about the availability of funds in the customer's account under these exceptions? (Q50)**

  Whether or not someone is a "merchant" is not material to determining if a bank may disclose customer information pursuant to the exceptions in §§40.14 and 40.15. The bank should determine if the third party to whom the bank intends to disclose information is actually involved in carrying out a financial transaction that is requested or authorized by the bank's customer. Check verification is permitted under the exceptions to the notice and opt out provisions, for 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 response to Q42, a bank that makes such a disclosure should take appropriate measures ensure that the person who inquires has a legitimate need for the information and is not engaging in a fraudulent attempt to obtain customer information. Concerns about properly safeguarding customer information are heightened when a bank discloses nonpublic personal information to a person rather than to a known merchant. (Posted 8/28/01)

- **A bank may want to request proof of insurance from a nonaffiliated insurance agency on an automobile that serves as the bank's collateral on a customer's loan. May the bank disclose customer information to the insurance agency to obtain proof of insurance without triggering specific notice and opt out requirements? (Q45)**

Yes, the bank may disclose nonpublic personal information, such as the existence of its relationship with a particular customer, to a nonaffiliated insurance agency to obtain proof of insurance under the exceptions to the specific notice and opt out requirements in §40.14. For instance, the bank could disclose nonpublic personal information under the exception in §40.14(b)(1) as a lawful or appropriate method to enforce the bank's rights in providing the loan. (Posted 8/28/01)

Disclosures under the exceptions in sections 40.13, 40.14, and 40.15

- **A community bank offers customers credit cards through a credit card bank. The credit card is issued with the name of the community bank on the front, although the credit card bank extends the credit and sends the monthly statements. The community bank provides customers with the card applications, and customers return the applications to the bank. The application states that the credit card bank is the issuer. The community bank makes recommendations to the credit card bank for approval, but the credit card bank makes the final decision, issues the card, and provides customer service. Does this type of arrangement fall under the exception in §40.14 or some other exception?**

  The community bank's disclosure of customer information to a credit card bank in this situation could fall within either §40.13 or §40.14. For instance, the credit card bank and the community bank may have an agreement to jointly offer, endorse, or sponsor the credit card and otherwise meet the requirements of §40.13. However, the community bank could also disclose the customer's information to the credit card bank pursuant to §40.14(a)(1) to process a financial product that a consumer has requested. (Posted 8/28/01)

- **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. Under the agreement, the community bank: (1) educates applicants about home buying and different types of available loan products; (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 application status. The community bank forwards the completed loan application to the mortgage company for underwriting, origination, and servicing. After that, the community bank has no further contact with the applicant about the applicant's loan. Must the bank provide an initial privacy notice to the applicant? If so, must the bank disclose this information sharing arrangement in its privacy notice, or is it covered by an exception in §40.14 or §40.15? (Q53)**

  If the bank does not already have a customer relationship with the loan applicant, the services that the bank performs pursuant to this program give rise to a customer relationship between the applicant and the bank as described in §40.3(i)(2)(i)(F). 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, .14, or .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).

When 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 describe specifically 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).

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

The mortgage company will also establish a customer relationship with any applicant for whom it originates a loan, and must provide a notice of its privacy policies no later than when it establishes the customer relationship. (Posted 8/28/01)

Compliance program

- **How should a bank monitor compliance with the privacy regulations?**

  An effective privacy monitoring/audit program will test the bank's compliance with the privacy regulations and ensure that its actual privacy practices are consistent with its stated policies and procedures. A bank should consider putting controls in place for monitoring: (1) the delivery of initial and annual notices to customers; (2) the delivery of initial notices to consumers who are not customers, if applicable; (3) compliance with opt out directions, if applicable; and (4) the accuracy of privacy notices.

  The bank must also monitor state laws, because it may be subject to additional restrictions or requirements for information shared with unaffiliated third parties, if applicable state laws provide greater consumer protections than the federal requirements.

  The FFIEC privacy examination procedures should be a useful tool in developing a privacy monitoring/audit program. (Posted 8/28/01)

- **Is a bank required by the privacy regulations to have both a board-approved written information security program and privacy compliance program?**

This question deals with two separate, but related, issues. The written "information security program" is a requirement of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 C.F.R. Part 30), which address the requirements to safeguard customer records and information. The written "information security program" should include administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The board of directors, or an appropriate committee thereof, must approve the program and oversee the development, implementation, and maintenance of the institution's information security program.

The privacy rule (12 C.F.R. Part 40) requires an institution to issue privacy notices and provide consumers with an opportunity to opt out of certain types of information sharing. A board-approved privacy compliance program to ensure compliance with the privacy rule is not required by the rule, but strongly recommended. The compliance program can be an effective way to communicate to the entire organization the institution's commitment to, and strategy for, complying with the privacy regulations. All institutions, regardless of size, should incorporate adherence to consumer privacy requirements into their compliance program. The formality of the compliance program will be determined by the nature, scope, and complexity of the institution's operations. (Posted 8/28/01)