



LEGAL EASE

New Federal Privacy Regulations May Affect Some NeighborWorks® Organizations

BY DANIEL EHRENBERG

Q: I am an executive director of a community-based organization that engages in home ownership, rehab and lending activities. I understand I may be subject to some disclosure requirements to our customers about privacy issues: specifically, the collection and use of information about them. Can you tell me whether I am and, if so, what the requirements may be?

A: When Congress in 1999 passed financial-modernization legislation (commonly referred to as the Gramm-Leach-Bliley Act or GLB Act, named after its three key sponsors, Senator Gramm and Representatives Leach and Bliley), one of the issues that Congress was concerned about was the use and sharing of customer personal information by financial institutions and other businesses.

To address this issue, Congress in the GLB Act added a section on the privacy of consumer financial information. It can be found at Title V of the GLB Act at Title 15 of the United States Code, Sections 6801 through 6810. This “privacy act” section limits the ability of a financial institution to disclose nonpublic personal information about its customers to nonaffiliated third parties; requires initial and annual notices, in certain circumstances, to its consumers and customers about its privacy policies and practices; and provides consumers and customers with an opportunity to not have their nonpublic personal information disclosed to others.

The federal financial institution regulators and the Federal Trade Commission in time issued final rules on the “privacy act” section. On May 24, 2000, the Federal Trade Commission (FTC) published a final rule on Privacy of Consumer Financial Information in Volume 65 of the Federal Register, beginning at page 33646. A copy of the pertinent sections of the GLB Act and the FTC’s final rule can be found at <http://www.ftc.gov/privacy/glbact/index.html>. Full compliance with the “privacy rule” was required of all financial institutions by July 1, 2001.

Unfortunately, Congress in the GLB Act did not distinguish between for-profit companies and nonprofit entities. It also used a very expansive definition of “financial institution.” Thus, not only are traditional banks, lenders and insurance companies required to comply with the rule’s requirements, but also many travel agencies, lawyers and others, including nonprofits, who provide financial services. If an organization is “significantly engaged” in financial activities, it would be considered a financial institution and would have to comply with the privacy rule.

The type of activities that would be considered financial activities include lending money, as well as providing financial services, brokering or servicing loans, engaging in credit counseling activities, and some community development or advisory activities. (The complete list of what constitutes a financial activity is found in Section 4(k) of the Bank Holding Company Act of 1956, at Title 12 of the United States Code at Section 1843(k).)

Thus, I would suspect there is a good chance, depending on the volume of your loan, rehab and home-ownership activities, that your organization would be considered a financial institution and would need to comply with the privacy rule. Because your organization is not a depository institution, it would be regulated by the FTC and its privacy rule.

Definitions

Before touching on the main requirements of the privacy rule, you should understand how the rule defines a few key terms. These include:

Consumer – A person who applies for, obtains or has obtained a personal, family or household financial product or service from you.

Customer – A person who is a consumer, but with whom you have a continuing or ongoing rela-

tionship, such as someone for whom you are helping obtain a loan or whose loan you are servicing.

Nonaffiliated third party – Any person or entity who you are not affiliated with, such as a subsidiary or parent corporation.

Nonpublic personal information – Personally identifiable financial information that is not publicly available, such as that which a consumer provides on an application form, account balance information, payment history, etc.

Opt-out – A directive by a consumer that the financial institution shall not disclose nonpublic personal information about the consumer to a nonaffiliated third party, other than as permitted by certain exceptions.

The privacy rule basically forbids you from disclosing any nonpublic personal information about a consumer to any nonaffiliated third party before you have provided a clear and conspicuous notice of your privacy policies and practices to that consumer and given that consumer an opportunity to opt-out of any such disclosure.

In addition, you must provide a customer with an initial privacy notice when you establish a “customer relationship” and then annually as long as the person continues as your customer.

Privacy Notice

The required privacy notice must be delivered so that each consumer can reasonably be expected to receive it in writing or, if the consumer agrees, electronically. The notice must be clear and conspicuous. In other words, it must be reasonably understandable and designed to call attention to the nature and significance of the information it contains. Many banks have been criticized for delivering privacy notices that were neither very readable nor intelligible.

The privacy notice should clearly set out your privacy collection and disclosure practices. It needs to answer the following questions and include the answers in the notice.

- 1) What categories of nonpublic personal information do you collect?
- 2) What categories of nonpublic personal information do you disclose to others?

- 3) To what categories of affiliates and nonaffiliated third parties do you disclose nonpublic personal information, other than parties to whom such information is disclosed under one of the privacy rule’s exceptions?

- 4) What categories of nonpublic personal information about former customers do you disclose and to what categories of affiliates and nonaffiliated third parties do you disclose such information, other than parties to whom such information is disclosed under one of the privacy rule’s exceptions?

- 5) Do you disclose nonpublic personal information to nonaffiliated third parties that you use to perform marketing services, and not pursuant to any of the other privacy rule’s exceptions, and, if so, what categories of third parties have you contracted with?

- 6) What is your consumer’s right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties and by what method(s) can a consumer exercise that right at any time?

- 7) What disclosures, if any, do you make under the Fair Credit Reporting Act of information to affiliates?

- 8) What are your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information?

- 9) Pursuant to which privacy rule exceptions do you disclose nonpublic personal information to nonaffiliated third parties (which may simply be a statement that you make disclosures to nonaffiliated third parties “as permitted by law.”

Your privacy notice only has to disclose the category of information that you disclose and the category of parties to whom you disclose it, not the specific information or individual parties to whom such information is disclosed.

If you do not disclose and do not wish to reserve the right to disclose, you can use a simplified privacy notice that states you only make disclosures pursuant to the privacy rule’s exceptions, and includes: a) the categories of nonpublic personal information you collect, b) your policies and practices with respect to protecting confidentiality and security of nonpublic personal information, and

c) if you disclose information pursuant to the privacy rule's exceptions, a disclosure of such practices (which may simply be a statement that you make disclosures to nonaffiliated third parties "as permitted by law." You obviously do not need to provide an opt-out notice.

Opting Out

If you do share nonpublic personal information with a nonaffiliated third party, even if with a funder (such as a NeighborWorks® organization sharing data with Neighborhood Reinvestment), you must give the consumer or customer a reasonable opportunity to opt-out. The opt-out notice, again, must be clear and conspicuous, accurately explain the right to opt-out, identify all categories of nonpublic personal information that you reserve the right to disclose and all categories of nonaffiliated third parties to whom you reserve the right to disclose such information.

A reasonable means of opting-out would include : a) designating check-off boxes in a prominent position on the relevant forms with the opt-out notice, b) including a reply form that contains the address to which the form should be mailed, c) providing an electronic means to opt-out, such as a form that can be e-mailed or a process at a Web site, if the consumer agrees to the electronic delivery of information, or d) providing a toll-free telephone number consumers may call to opt-out. It is not a reasonable means to opt-out if the consumer has to write his or her own letter in order to exercise the opt-out right. Finally the opt-out notice must be delivered in the same manner as you delivered the privacy notice. If you use the mail, you should give your consumers at least 30 days from the date you mailed the opt-out notice.

If a consumer does opt-out, you must honor his or her opt-out request as soon as reasonably practicable. The request remains effective until revoked in writing, and continues to apply even after the customer relationship ends. A consumer can choose to opt-out at any time.

Identifying the Exceptions

Three major types of exceptions exist to the notice and opt-out requirements. The first is a limited exception that pertains to service providers and joint

marketing arrangements. Under this exception, if a nonaffiliated third party performs services for you or functions on your behalf, you provide your consumers with an initial privacy notice and you enter into a contractual arrangement with the nonaffiliated third party that prohibits the third party from using the information that you provided for any purpose other than carrying out your directions, you can disclose nonpublic personal information to that third party.

The second exception is termed the administrative exception. You do not have to provide a privacy or opt-out notice to your consumer to share information in order to process a transaction that your consumer has requested or authorized. In addition, any secondary-market sales (including sales of servicing rights) are exempted from the requirements of the privacy rule. Therefore, you and the secondary-market maker can share nonpublic personal information in order to allow you sell your loans on the secondary market and to have you continue to service the loans.

The last exception is a catch-all exception that covers a number of situations, such as to comply with laws and subpoenas and/or other requests for information from federal, state or local authorities.

For examples of electronic privacy and opt-out notices, see the Bank of America Web site at www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr.cfm or the Wells Fargo Bank Web site at www.wellsfargo.com/privacy/privacy.jhtml. For more information on the privacy rule, go to the FTC's Web site at <http://www.ftc.gov/privacy/glbact/index.html>. ■

Daniel Ehrenberg (dehrenberg@nw.org) is deputy general counsel, Neighborhood Reinvestment Corporation.

This article is for general purposes only and does not represent legal advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised as to relevant legal developments. If you have a question involving your community development organization, or any of its activities, and the law, please send it to Allan Martin (amartin@nw.org), Neighborhood Reinvestment's publishing director.