

Section One:

Overview of privacy rule requirements

The privacy rule governs when and how banks may share nonpublic personal information about consumers with nonaffiliated third parties.

The rule embodies two principles—notice and opt out. In summary:

- **All banks must develop initial and annual privacy notices.** The notices must describe in general terms the bank's information sharing practices.
- Banks that share nonpublic personal information about consumers with nonaffiliated third parties (outside of opt out exceptions delineated in the privacy rule) must also provide consumers with:
 - an opt out notice
 - a reasonable period of time for the consumer to opt out

*A few **key terms** used throughout the privacy rule are critical to understanding the rule's scope and application. Refer to **Section Four** of this guide for an explanation of:*

- *nonpublic personal information*
- *the distinction between consumers and customers*
- *nonaffiliated third party*

Exceptions to opt out: A consumer cannot opt out of all information sharing. First, the privacy rule does not govern information sharing among affiliated parties. Second, the rule contains exceptions to allow transfers of nonpublic personal information to unaffiliated parties to process and service a consumer's transaction, and to facilitate other normal business transactions. For example, consumers cannot opt out when nonpublic personal information is shared with a nonaffiliated third party to:

- market the bank's own financial products or services
- market financial products or services offered by the bank and another financial institution (joint marketing)
- process and service transactions the consumer requests or authorizes
- protect against potential fraud or unauthorized transactions
- respond to judicial process
- comply with federal, state, or local legal requirements

Applying exceptions: A bank may have to satisfy disclosure and other requirements to make the rule's opt out exceptions applicable. For example, the **joint marketing exception** requires a **contractual agreement** between two nonaffiliated financial institutions to:

- a) jointly offer, endorse, or sponsor the financial product or service, and
- b) limit further use or disclosure of the consumer information transferred

In addition, the bank must include a separate statement in the privacy notice disclosing the joint marketing agreement.

Prohibition on sharing account numbers: The privacy rule prohibits a bank from disclosing an account number or access code for credit card, deposit, or transaction accounts to any nonaffiliated third party for use in marketing. The rule contains two narrow exceptions to this general prohibition. A bank may share account numbers in conjunction with marketing its **own products** as long as the service provider is not authorized to directly initiate charges to the accounts. A bank may also disclose account numbers to a participant in a private label or affinity credit card program when the participants are identified to the customer. **An account number does not include a number or code in encrypted form as long as the bank does not also provide a means to decode the number.**

Limits on reuse and redisclosure: The privacy rule limits reuse and redisclosure of nonpublic personal information received from a nonaffiliated financial institution or disclosed to a nonaffiliated third party. The specific limitations depend on whether the information was received pursuant to or outside of the notice and opt out exceptions.

State Law: A provision under a State law that provides greater consumer protection than provided under the GLBA privacy provisions will supercede the Federal privacy rule. The bank will be obligated to comply with the provisions of that State law to the extent those provisions provide greater consumer protection than the Federal privacy rule. The Federal Trade Commission determines whether a particular State law provides greater protection.

Privacy Notices

Every bank must develop initial and annual privacy notices—even if the bank does not share information with nonaffiliated third parties.

Content of notices: The initial, annual, and revised notices include, as applicable:

- **categories of information a bank collects** (all banks)
- **categories of information a bank may disclose** (all banks, except a bank that does not intend to make any disclosures or only makes disclosures under the exceptions may simply state that)
- **categories of affiliates and nonaffiliates to whom a bank discloses nonpublic personal information** (all banks sharing nonpublic personal information with an affiliate or with a nonaffiliated third party)
- **information sharing practices about former customers** (all banks)
- **categories of information disclosed under the service provider/joint marketing exception** (only those banks relying on this exception)
- **consumer's right to opt out** (only those banks that disclose outside of exceptions)
- **disclosures made under the Fair Credit Reporting Act** (only those banks providing the FCRA opt out notice)
- **disclosures about confidentiality and security of information** (all banks)

A revised notice may be required when a bank changes its information sharing practices.

The following table reflects the rule's requirements for delivering initial, annual, and revised notices to consumers and customers.

Type of notice	Who gets it	Delivery
Initial privacy notice (all banks)	<ul style="list-style-type: none"> • all existing bank customers • all new bank customers after July 1, 2001 • consumers who are not customers 	<ul style="list-style-type: none"> • no later than July 1, 2001 • when the customer relationship is established • only if the bank intends to share nonpublic personal information about the consumer with a nonaffiliated third party
Annual privacy notice (all banks)	<ul style="list-style-type: none"> • customers 	<ul style="list-style-type: none"> • at least once in any period of 12 consecutive months while the customer relationship continues
Revised privacy notice (as applicable)	<ul style="list-style-type: none"> • customers and consumers who are not customers 	<ul style="list-style-type: none"> • before the bank shares nonpublic personal information in a manner not described in the most recent notice delivered to the customer or consumer

Opt Out Notice

The final rule provides that an **opt out notice** is adequate if it:

- identifies all the categories of nonpublic personal information the bank intends to disclose to nonaffiliated third parties
- states the consumer can opt out of the disclosure
- provides a reasonable method for the consumer to opt out, such as a toll-free telephone number

The table below summarizes the rule's requirements for delivering an opt out notice.

Type of notice	Who gets it	Delivery
Opt out notice (only banks that share outside of exceptions)	<ul style="list-style-type: none"> • customers and consumers who are not customers 	<ul style="list-style-type: none"> • before the bank shares nonpublic personal information about the customer or consumer (and the information sharing is not permissible under the privacy rule opt out exceptions)

The opt out right: If a bank intends to share nonpublic personal information outside the exceptions, it must also:

- provide consumers with a **reasonable opportunity to opt out**. Examples in the privacy rule give consumers **30 days** to respond to the opt out notice when the bank delivers the notice by mail or electronically
- **comply** with a consumer's opt out direction **as soon as reasonably practicable** when the direction is received after the initial opt out period elapses
- **comply** with the opt out direction until revoked in writing by the consumer

Delivering notices: The initial, annual, revised, and opt out notices may be delivered in writing or, if the consumer agrees, electronically. An oral description of the notice is not sufficient.

Section Two

Get Ready for July 1, 2001

A bank's strategy for achieving full compliance by July 1, 2001, will vary depending on the complexity of the bank and the progress it has already made in complying with the requirements of the rule. The level of effort a bank will expend depends in large part on:

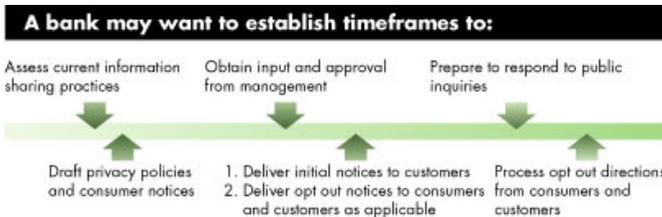
- the bank's previous efforts to assess or disclose information sharing practices
- the bank's decisions about sharing nonpublic personal information after July 1, 2001
- the volume, if any, of consumers and customers who must receive an opportunity to opt out before information sharing with nonaffiliated third parties can take place.

Nearly all banks, however, can take the following four steps to create a comprehensive and effective privacy compliance strategy:

- establish a timeline for compliance
- develop privacy policies and notices
- deliver notices
- prepare to respond to consumers

1. Establish a timeline for compliance

A timeline designating important checkpoints prior to July 1, 2001, is a good place to start and can be instrumental to ensuring timely compliance.



A specific process for certifying completion of the various steps identified in the bank's privacy compliance strategy will help managers keep track of progress. When establishing due dates for specific activities, build in time to receive input and feedback from senior management and other stakeholders. Every bank should consider:

- **Involving the Board of Directors:** A board-approved privacy policy is not required by the rule, but it can be an effective way to involve the board of directors in developing a privacy compliance strategy. A board-sanctioned privacy policy can be useful in communicating the bank's overall privacy commitment and strategy to the entire organization.
- **Involving representatives from each bank department:** Most likely a senior bank officer will oversee development and implementation of the privacy compliance strategy. Nevertheless, participation from each department in the bank will help ensure nothing is overlooked. This approach will also help policy makers identify information sharing practices or consumer privacy issues unique to a specific department or to a financial product or service.

2. Develop privacy policies and notices

Use this opportunity to evaluate and establish institutional privacy objectives, and communicate to potential customers and consumers the bank's customer service philosophy.

- Create a comprehensive inventory of information collection and information sharing practices at the bank. The inventory will help ensure practices are properly disclosed in the bank's privacy notices. For every department, review:
 - all applications and forms used to collect information about consumers
 - marketing practices
 - vendor contracts
 - electronic banking and Internet activities
 - fee income accounts
 - record retention policies

Affiliates: If a bank has any affiliates, the inventory should include information-sharing practices with affiliates. Although the privacy rule does not place any restrictions on information sharing with affiliates, it does require disclosure of these practices in the initial and annual notices. Furthermore, the privacy rule requires the initial and annual notices to include applicable **Fair Credit Reporting Act** affiliate information sharing opt out notices.

- **Assess current information collection and information sharing practices** in light of the privacy rule obligations and the bank's objectives. Determine which practices should continue after July 1, 2001. This may be a good time to involve the bank's Board of Directors. Consider:
 - whether any current practices would be prohibited under the rule
 - which practices must be disclosed in the privacy notices and whether opt out rights apply
 - whether account numbers are shared only as permitted by the rule
 - whether information received from other financial institutions is shared only as permitted by the rule's reuse and redisclosure limitations
 - whether to adopt voluntary privacy standards developed by relevant trade associations. Those standards could be good indicators of industry norms and consumer expectations
- **Draft privacy notice(s)**. Create a list of information collection and information sharing practices that must be disclosed to consumers. This list can help you categorize practices per the rule requirements and decide how to structure notices. The privacy rule provides a variety of disclosure options. For example, banks may develop:
 - one initial privacy notice that covers all the information sharing practices of the bank
 - an assortment of initial notices for different customer relationships or different types of financial products or services
 - one initial notice that covers the practices of the bank along with one or more of its affiliates. Likewise, the opt out notice may be structured in a variety of ways.

When drafting privacy notices, consider:

- **Sample clauses** provided in Appendix A in the rule. Banks may use the sample clauses to the extent they accurately reflect the bank's practices.

Most likely, the initial and annual privacy notices will be identical. If required, the opt out notice may be combined with the initial and annual notices.

- **Fair Credit Reporting Act requirements and information security standards.** The federal banking agencies have issued two **proposed rules** that may affect the compliance strategy and the content of privacy notices.

The **Proposed Security Standards for Customer Information** describe the agencies' expectations for implementing technical and physical safeguards to protect customer information. **The Proposed Fair Credit Reporting Regulations** cover the opt out provisions of the Fair Credit Reporting Act.

Both proposals will be finalized in the near future. When issued, the final rules will be available on the FDIC's Web site: www.fdic.gov. In the meantime, the proposals are posted on the Web site.

3. Deliver notices

- Identify consumers and customers who must receive the initial and opt out notices. It is important to identify all groups of existing customers, consumers, and former customers who must get the initial privacy notice and opt out notification. Some banks may need to coordinate several databases and a variety of departments to identify everyone who must receive a notice.

***Opt out notices for joint account holders:** The privacy rule allows banks to provide a **single** privacy and opt out notice when two or more consumers **jointly** obtain a financial product or service. However, any of the joint consumers may exercise the right to opt out. The opt out notice provided to joint account holders must explain how the bank will treat an opt out direction by a joint consumer and must give one joint consumer the ability to opt out on behalf of all the joint consumers.*

- **Establish timeframes for mailing or otherwise delivering notices.** Remember:
 - **All existing bank customers must receive an initial privacy notice no later than July 1, 2001.**
 - **Existing bank customers, consumers who are not customers, and former bank customers** have the right to opt out if the bank is sharing nonpublic personal information about them with nonaffiliated third parties outside the exceptions.
 - Information sharing subject to opt out cannot continue after July 1, 2001, until the initial and opt out notices are delivered and a reasonable opt out period has elapsed. Therefore, banks that intend to share nonpublic personal information outside the exceptions after July 1, 2001 should deliver notices well before July 1.

4. Prepare to respond to consumers

- **Develop opt out procedures.** All banks sharing nonpublic personal information outside of the exceptions will need to develop procedures for consumers to exercise an opt out, as well as procedures for processing and complying with opt out directions. The opt out procedures should include:
 - tracking the initial opt out opportunity (e.g., the first 30 days after the initial notice is delivered)
 - recording opt outs received from consumers
 - maintaining the opt out mechanism(s), such as a toll-free telephone number, electronic mail, or an opt out form with boxes to check

- o complying with opt out directions received after the initial opt out opportunity elapses

- **Respond to public inquiries.** Customer service representatives and other bank employees should be prepared to answer questions from consumers about the new privacy notices. Depending on the number of employees answering consumer phone calls, it may be a good idea to provide scripts to help employees respond to questions from the public. In addition, it may be helpful to have extra copies of the privacy notice readily available for mailing or handing out to consumers.

Section Three:

Maintaining Compliance Beyond

July 1, 2001

The following activities can help a bank achieve and maintain compliance with the privacy rule.

- Develop controls to monitor ongoing compliance. Consider mechanisms for monitoring:
 - o delivery of initial and annual notices to customers
 - o delivery of initial notice to consumers who are not customers, if applicable
 - o compliance with opt out directions, if applicable
 - o accuracy of privacy notices, including prior approval for:
 - new marketing arrangements
 - new or renewed vendor contracts
 - disclosure of account numbers
 - affiliate-referral programs
 - reuse of consumer information received from another financial institution
- Train employees. All employees should understand the bank's policies and procedures for complying with the privacy rule. Some employees will need to be able to explain the bank's privacy policies to customers and to businesses providing services to the bank.
- Audit for compliance. Periodic audits will help management assess risk and verify the effectiveness of the compliance program. The Federal Financial Institutions Examination Council (FFIEC) will release interagency privacy examination procedures before July 1, 2001. The exam procedures will be a useful tool in developing a privacy audit program.

The interagency exam procedures will be mailed directly to insured depository institutions as soon as they are finalized. The procedures will also be available on the FDIC's Web site at www.fdic.gov when complete.

Section Four:

Learn the Lingo

Learning the lingo will help you understand and comply with the privacy rule. This section provides an explanation of key terminology.

Who must comply with the FDIC's privacy rule?

The FDIC's privacy rule refers to financial institutions that must comply with the rule as "you." For example, when the rule states that "you must provide a notice" it means all entities subject to this rule must provide a notice. The following definition of "you" explains the types of entities subject to the rule:

You: The banks that must comply with the FDIC's rule are -

- (1) FDIC-supervised banks
- (2) insured state branches of foreign banks
- (3) subsidiaries of FDIC-supervised banks and insured state branches of foreign banks, with certain exceptions, such as insurance and securities or brokerage subsidiaries

Although the FDIC's rule only applies to certain banks and some of their subsidiaries, all financial institutions must comply with similar privacy rules adopted by their supervisory agencies. For example, although securities subsidiaries of FDIC-supervised banks do not have to comply with the FDIC's privacy rule, they do have to comply with a similar privacy rule adopted by the Securities and Exchange Commission.

Who is protected by the privacy rule?

The privacy rule protects "consumers." **All consumers receive the same privacy protections.**

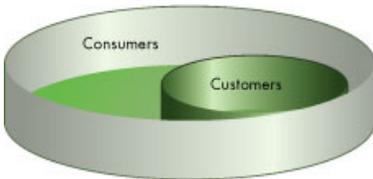
However, a subset of consumers defined as **customers** must receive certain disclosures, such as an annual privacy notice, that need not be provided to consumers who are not customers.

Thus, it is important to know the distinction between consumers and customers to understand the different disclosure requirements under the privacy rule.

Consumer: Any individual who is seeking to obtain or has obtained a financial product or service from a bank for personal, family, or household purposes is a consumer of that bank. The definition of consumer includes individuals who:

- **apply for** a financial product or service (e.g., a loan or a deposit account) for personal, family, or household purposes
- **actually obtain** a financial product or service (e.g., a loan or a deposit account) for personal, family, or household purposes

Customer: As the following diagram reflects, customers are a subset of consumers. A customer is a consumer with whom a bank has a **continuing relationship**. Although the rule does not define "continuing relationship," it provides examples of transactions that are and are not considered continuing relationships. Consumers who have a deposit account, obtain a loan, or obtain an investment advisory service are considered customers. See Section 332.3(i).



Additional guidance regarding the customer relationship can be found in the Supplemental Information (the preamble) of the rule, which notes that a continuing relationship is established "where a consumer typically would receive some measure of continued service following, or in connection with, a transaction." See page 35168, Federal Register, Vol. 65, No. 106.

The next diagram depicts the relationship between all individuals who do business with a bank and those who meet the regulatory definitions for **consumers** and **customers**. As the diagram shows, only a portion of the individuals who conduct business with a bank are consumers under the privacy rule. For example, individuals are not considered consumers under this rule if they are commercial clients, grantors or beneficiaries of trusts for which the bank is trustee, or participants in an employee benefit plan that the banks sponsors.



What type of information is protected by the privacy rule? The rule identifies three primary categories of information:

- publicly available information
- personally identifiable financial information
- nonpublic personal information

Nonpublic personal information is the category of information protected by the privacy rule. The definitions for publicly available information and personally identifiable financial information work together to describe and define nonpublic personal information.

- **Publicly available information** is any information a bank reasonably believes is lawfully publicly available. The **nature** of the information, **not the source** of the information, determines whether it is publicly available information for purposes of the privacy rule. For example, even if a bank obtains customers' telephone numbers or the assessed value of their residences directly from the consumers, this information will be considered publicly available if the bank has a reasonable basis to believe the information could have been lawfully obtained from a public source. A reasonable belief exists if a bank has determined that (a) the information is of the type that is generally available to the public and (b) the individual has not blocked such information from public disclosure. This means, for example, that a bank can consider a customer's phone number to be publicly available, **but only** if the bank takes steps to determine the phone number is not unlisted.
- **Personally identifiable financial information** is any information a bank collects about a consumer in conjunction with providing a financial product or service. This includes:
 - information provided by the consumer during the application process (e.g., name, phone number, address, income)
 - information resulting from the financial product or service transaction (e.g., payment history, loan or deposit balances, credit card purchases)
 - information from other sources about the consumer obtained in connection with providing the financial product or service (e.g., information from a consumer credit report or from court records)

Personally identifiable financial information also includes any information that "is disclosed in a manner that

indicates that the individual is or has been your consumer." See Section 332.3(o)(2)(i)(D). **Thus, the very fact that an individual is a consumer of a bank is personally identifiable financial information.**

- **Nonpublic personal information**, the category of information protected by the privacy rule, consists of:
 1. Personally identifiable financial information that is **not** publicly available information; and
 2. Lists, descriptions, or other groupings of consumers that were either
 - a. **created using** personally identifiable financial information that is not publicly available information, or
 - b. **contain** personally identifiable financial information that is not publicly available information.

A list is considered nonpublic personal information if it is **generated** based on customer relationships, loan balances, or other personally identifiable financial information that is not publicly available. A list is also considered nonpublic personal information if it **contains** any nonpublic personal information.

For example, in jurisdictions where mortgage documents are public records, the names and address of all individuals for whom a bank held a mortgage would not be nonpublic personal information since it was generated using publicly available information and contained only publicly available information. The list would become nonpublic personal information, however, if it contained current loan balances or if it was generated using only those customers with current mortgage loan balances in excess of a certain amount.

The two categories of nonpublic personal information are depicted in the following diagram.



Who are nonaffiliated third parties?

The privacy rule restricts information sharing with nonaffiliated third parties. The rule defines nonaffiliated third parties as persons or entities except affiliates and persons jointly employed by a bank and a nonaffiliated third party. Affiliates generally include a bank's subsidiaries, its holding company, and any other subsidiaries of the holding company. See Section 332.3(a), Section 332.3(d), and Section 332.3(g).

The privacy rule does not impose limitations on information sharing with affiliates. It does, however, require disclosure of such information sharing policies and practices. (Note: The rules governing the sharing of information between a bank and its affiliates are set forth in the Fair Credit Reporting Act.)

Although the privacy rule most commonly uses the term "nonaffiliated third parties," there are some instances in which a distinction is made between nonaffiliated financial institutions and all other nonaffiliated third parties. Readers should pay particular attention to these distinctions. See Section 332.13.

Other Resources

A variety of resources are available to help banks understand the privacy rule and related issues. Some of the most significant are listed below. All FDIC material can be found at www.fdic.gov.

FDIC Financial Institution Letter titled **Final Rule on the Privacy of Consumers' Financial Information**, (FIL-34-2000 dated June 5, 2000).

FDIC Financial Institution Letter titled **Proposed Regulations Implementing the Fair Credit Reporting Act**, (FIL-71-2000 dated October 26, 2000).

FDIC Financial Institution Letter titled **Proposed Security Standards for Customer Information**, (FIL-43-2000 dated July 6, 2000).

FDIC Financial Institution Letter titled **Internet Web Site Privacy Survey Report**, (FIL-113-99 dated December 27, 1999).

FDIC Financial Institution Letter titled **Online Privacy of Consumer Financial Information**, (FIL-86-98 dated August 17, 1998).

Transcript of **"Is It Any of Your Business? Consumer Information, Privacy, and the Financial Services Industry,"** an interagency public forum hosted by the FDIC, March 23, 2000.

Office of the Comptroller of the Currency's Bulletin titled **Privacy Laws and Regulations**, (September 8, 2000) available at www.occ.treas.gov.

Office of Thrift Supervision's Memorandum to Chief Executive Officers titled **Privacy Preparedness Check-up**, (September 29, 2000) available at www.ots.treas.gov.