

(6) *Confidentiality and security.* A bank describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if it does both of the following:

(i) Describes in general terms who is authorized to have access to the information; and

(ii) States whether the bank has security practices and procedures in place to ensure the confidentiality of the information in accordance with the bank's policy. The bank is not required to describe technical information about the safeguards it uses.

(d) *Short-form initial notice with opt out notice for non-customers.* (1) A bank may satisfy the initial notice requirements in §§ 40.4(a)(2), 40.7(b), and 40.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as the bank delivers an opt out notice as required in § 40.7.

(2) A short-form initial notice must:

- (i) Be clear and conspicuous;
- (ii) State that the bank's privacy notice is available upon request; and
- (iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) The bank must deliver its short-form initial notice according to § 40.9. The bank is not required to deliver its privacy notice with its short-form initial notice. The bank instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the bank's short-form notice requests the bank's privacy notice, the bank must deliver its privacy notice according to § 40.9.

(4) *Examples of obtaining privacy notice.* The bank provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the bank:

- (i) Provides a toll-free telephone number that the consumer may call to request the notice; or
- (ii) For a consumer who conducts business in person at the bank's office, maintain copies of the notice on hand that the bank provides to the consumer immediately upon request.

(e) *Future disclosures.* The bank's notice may include:

(1) Categories of nonpublic personal information that the bank reserves the

right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or non-affiliated third parties to whom the bank reserves the right in the future to disclose, but to whom the bank does not currently disclose, nonpublic personal information.

(f) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

§ 40.7 Form of opt out notice to consumers; opt out methods.

(a) (1) *Form of opt out notice.* If a bank is required to provide an opt out notice under § 40.10(a), it must provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice must state:

- (i) That the bank discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;
- (ii) That the consumer has the right to opt out of that disclosure; and
- (iii) A reasonable means by which the consumer may exercise the opt out right.

(2) *Examples.* (i) *Adequate opt out notice.* A bank provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the bank:

(A) Identifies all of the categories of nonpublic personal information that it discloses or reserves the right to disclose, and all of the categories of non-affiliated third parties to which the bank discloses the information, as described in § 40.6(a)(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

(B) Identifies the financial products or services that the consumer obtains from the bank, either singly or jointly, to which the opt out direction would apply.

(ii) *Reasonable opt out means.* A bank provides a reasonable means to exercise an opt out right if it:

(A) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;

(B) Includes a reply form together with the opt out notice;

§ 40.7

12 CFR Ch. I (1-1-06 Edition)

(C) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the bank's web site, if the consumer agrees to the electronic delivery of information; or

(D) Provides a toll-free telephone number that consumers may call to opt out.

(iii) *Unreasonable opt out means.* A bank does not provide a reasonable means of opting out if:

(A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the bank provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* A bank may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

(b) *Same form as initial notice permitted.* A bank may provide the opt out notice together with or on the same written or electronic form as the initial notice the bank provides in accordance with § 40.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If a bank provides the opt out notice later than required for the initial notice in accordance with § 40.4, the bank must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(d) *Joint relationships.* (1) If two or more consumers jointly obtain a financial product or service from a bank, the bank may provide a single opt out notice. The bank's opt out notice must explain how the bank will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5) of this section).

(2) Any of the joint consumers may exercise the right to opt out. The bank may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(ii) Permit each joint consumer to opt out separately.

(3) If a bank permits each joint consumer to opt out separately, the bank must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A bank may not require all joint consumers to opt out before it implements any opt out direction.

(5) *Example.* If John and Mary have a joint checking account with a bank and arranges for the bank to send statements to John's address, the bank may do any of the following, but it must explain in its opt out notice which opt out policy the bank will follow:

(i) Send a single opt out notice to John's address, but the bank must accept an opt out direction from either John or Mary.

(ii) Treat an opt out direction by either John or Mary as applying to the entire account. If the bank does so and John opts out, the bank may not require Mary to opt out as well before implementing John's opt out direction.

(iii) Permit John and Mary to make different opt out directions. If the bank does so:

(A) It must permit John and Mary to opt out for each other;

(B) If both opt out, the bank must permit both of them to notify it in a single response (such as on a form or through a telephone call); and

(C) If John opts out and Mary does not, the bank may only disclose non-public personal information about Mary, but not about John and not about John and Mary jointly.

(e) *Time to comply with opt out.* A bank must comply with a consumer's opt out direction as soon as reasonably practicable after the bank receives it.

(f) *Continuing right to opt out.* A consumer may exercise the right to opt out at any time.

(g) *Duration of consumer's opt out direction.* (1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the non-public personal information that the bank collected during or related to

that relationship. If the individual subsequently establishes a new customer relationship with the bank, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When a bank is required to deliver an opt out notice by this section, the bank must deliver it according to § 40.9.

§ 40.8 Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this part, a bank must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a non-affiliated third party other than as described in the initial notice that the bank provided to that consumer under § 40.4, unless:

(1) The bank has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The bank has provided to the consumer a new opt out notice;

(3) The bank has given the consumer a reasonable opportunity, before the bank discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

(b) *Examples.* (1) Except as otherwise permitted by §§ 40.13, 40.14, and 40.15, a bank must provide a revised notice before it:

(i) Discloses a new category of nonpublic personal information to any nonaffiliated third party;

(ii) Discloses nonpublic personal information to a new category of nonaffiliated third party; or

(iii) Disclose nonpublic personal information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if the bank discloses nonpublic personal information to a new nonaffiliated third party that the bank adequately described in its prior notice.

(c) *Delivery.* When a bank is required to deliver a revised privacy notice by this section, the bank must deliver it according to § 40.9.

§ 40.9 Delivering privacy and opt out notices.

(a) *How to provide notices.* A bank must provide any privacy notices and opt out notices, including short-form initial notices, that this part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(b) (1) *Examples of reasonable expectation of actual notice.* A bank may reasonably expect that a consumer will receive actual notice if the bank:

(i) Hand-delivers a printed copy of the notice to the consumer;

(ii) Mails a printed copy of the notice to the last known address of the consumer;

(iii) For the consumer who conducts transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service;

(iv) For an isolated transaction with the consumer, such as an ATM transaction, posts the notice on the ATM screen and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

(2) *Examples of unreasonable expectation of actual notice.* A bank may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(i) Only posts a sign in its branch or office or generally publishes advertisements of its privacy policies and practices;

(ii) Sends the notice via electronic mail to a consumer who does not obtain a financial product or service from the bank electronically.

(c) *Annual notices only.* A bank may reasonably expect that a customer will receive actual notice of the bank's annual privacy notice if:

(1) The customer uses the bank's web site to access financial products and services electronically and agrees to receive notices at the web site and the bank posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or