

§ 160.5 Annual privacy notice to customers required.

(a)(1) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the life of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

(2) *Example.* You provide notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

(b)(1) *Termination of customer relationship.* You are not required to provide an annual notice to a former customer.

(2) *Examples.* Your customer becomes a former customer when:

(i) The individual's commodity interest account is closed;

(ii) The individual's advisory contract or subscription is terminated or expires; or

(iii) The individual has redeemed all of his or her units in your pool.

(c) *Delivery of notice.* When you are required by this section to deliver an annual privacy notice, you must deliver it in the manner provided by § 160.9.

§ 160.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 160.4, 160.5 and 160.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

(1) The categories of nonpublic personal information that you collect;

(2) The categories of nonpublic personal information that you disclose;

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 160.14 and 160.15;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 160.14 and 160.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 160.13 (and no other exception applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the consumer's rights under § 160.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

(7) Any disclosures that you make under § 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that you make under paragraph (b) of this section.

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under §§ 160.14 and 160.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 160.4 and 160.5. When describing the categories with respect to those parties, it is sufficient to state that you make disclosures to other nonaffiliated companies:

(1) For your everyday business purposes, such as *[include all that apply]* to process transactions, maintain account(s), respond to court orders and

§ 160.6

17 CFR Ch. I (4–1–11 Edition)

legal investigations, or report to credit bureaus; or

(2) As permitted by law.

(c) *Examples*—(1) *Categories of nonpublic personal information that you collect.* You satisfy the requirement to categorize the nonpublic personal information that you collect if you list the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with you or your affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal information you disclose.* (i) You satisfy the requirement to categorize the nonpublic personal information you disclose if you list the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If you reserve the right to disclose all of the nonpublic personal information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal information you disclose.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information if you list the following categories, as applicable, and a few examples to illustrate the types of third parties in each category:

(i) Financial service providers;

(ii) Non-financial companies; and

(iii) Others.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in §160.13 to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:

(i) List the categories of nonpublic personal information you disclose,

using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) State whether the third party is:

(A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or

(B) A financial institution with which you have a joint marketing agreement.

(5) *Simplified notices.* If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information to affiliates or nonaffiliated third parties except as authorized under §§160.14 and 160.15, you may simply state that fact, in addition to information you must provide under paragraphs (a)(1), (a)(8), (a)(9) and (b) of this section.

(6) *Confidentiality and security.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you do both of the following:

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

(ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

(d) *Short-form initial notice with opt out notice for non-customers.* (1) You may satisfy the initial notice requirements in §§160.4(a)(2), 160.7(b) and 160.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in 160.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that your privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain your privacy notice.

(3) You must deliver your short-form initial notice according to §160.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply

provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to §160.9.

(4) *Examples of obtaining privacy notice.* You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:

(i) Provide 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 your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

(e) *Future disclosures.* Your notice may include:

(1) Categories of nonpublic personal information that you reserve the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates and non-affiliated third parties to whom you reserve the right in the future to disclose, but to whom you do not currently disclose, nonpublic personal information.

(f) *Model privacy form.* Pursuant to §160.2(a) of this part, a model privacy form that meets the notice content requirements of this section is included in appendix A of this part.

(g) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in appendix B of this part. Use of a sample clause in a privacy notice provided on or before December 31, 2010, to the extent applicable, constitutes compliance with this part.

[66 FR 21252, Apr. 27, 2001, as amended at 74 FR 62974, December 1, 2009]

EFFECTIVE DATE NOTE: At 74 FR 62974, December 1, 2009, §160.6 was amended by removing (g), effective January 1, 2012.

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

(a)(1) *Form of opt out notice.* If you are required to provide an opt out notice under §160.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:

(i) That you disclose or reserve the right to disclose nonpublic personal information about your 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.* You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of non-affiliated third parties to which you disclose the information, as described in §160.6(a)(2) and (3), and state that the consumer can opt out of the disclosure of that information; and

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

(ii) *Reasonable means to opt out.* You provide a reasonable means to exercise an opt out right if you:

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

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

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

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

(iii) *Unreasonable opt out means.* You do 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 you provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* You may require each consumer to opt out