

COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 160

RIN 3038-AB68

Privacy of Consumer Financial Information

AGENCY: Commodity Futures Trading Commission.

ACTION: Final rule.

SUMMARY: The Commodity Futures Trading Commission is adopting part 160, privacy rules promulgated under section 5g of the Commodity Exchange Act, which directs the Commission to prescribe regulations under Title V of the Gramm-Leach-Bliley Act. Title V requires certain federal agencies to adopt rules implementing notice requirements and restrictions on the ability of financial institutions to disclose nonpublic personal information about consumers to nonaffiliated third parties. Under section 503 of the Gramm-Leach-Bliley Act, a financial institution must provide its customers with a notice of its privacy policies and practices, and must not disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure. Section 505 of the Gramm-Leach-Bliley Act further requires certain federal agencies to establish for financial institutions appropriate standards to protect customer information. The part 160 rules implement these requirements of the Gramm-Leach-Bliley Act with respect to futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers that are subject to the jurisdiction of the Commission under the Commodity Exchange Act as amended.

DATES:

Effective Date: These rules are effective June 21, 2001.

Compliance Date: Compliance will be mandatory as of March 31, 2002. Joint marketing and service agreements in effect as of March 31, 2002 must be brought into compliance with section 160.13 by March 31, 2003.

FOR FURTHER INFORMATION CONTACT:

Susan Nathan, Assistant General Counsel, or Bella Rozenberg, Attorney, Office of General Counsel; Nancy E. Yanofsky, Assistant Chief Counsel, Division of Economic Analysis; or Ky Tran-Trong, Attorney, Division of Trading and Markets, Commodity

Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW., Washington, DC 20581. Telephone: (202) 418-5000, E-mail: (SNathan@cftc.gov), (BRozenberg@cftc.gov), (NYanofsky@cftc.gov), or (KTran-Trong@cftc.gov).

SUPPLEMENTARY INFORMATION: The Commodity Futures Trading Commission today is adopting new part 160, 17 CFR 160, under Subtitle A of Title V of the Gramm-Leach-Bliley Act (Pub. L. No. 106-102, 113 Stat. 1338 (1999)), to be codified at 15 U.S.C. 6801-6809 and section 5g of the Commodity Exchange Act, 7 U.S.C. 7b-2, as amended by the Commodity Futures Modernization Act of 2000 (Pub. L. No. 106-554, 114 Stat. 2763).

Table of Contents

- I. Background
 - II. Overview of Comments Received
 - III. Section-by-Section Analysis
 - IV. Cost-Benefit Analysis
 - V. Related Matters
 - A. Paperwork Reduction Act
 - B. Regulatory Flexibility Act
- Text of Final Rules
Appendix—Sample Clauses

I. Background

Subtitle A of Title V of the Gramm-Leach-Bliley Act (GLB Act),¹ captioned “Disclosure of Nonpublic Personal Information” (Title V), limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose to all of its customers the institution’s privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties.² The Commodity Futures Trading Commission (Commission) and entities subject to its jurisdiction originally were excluded from Title V’s coverage.³ The agencies that were covered by Title V—the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation, Office of Thrift Supervision (collectively, the Banking Agencies), Secretary of the Treasury,

¹ Pub. L. No. 106-102, 113 Stat. 1338 (1999) (to be codified in scattered sections of 12 U.S.C. and 15 U.S.C.)

² GLB Act §§ 501-510 (to be codified at 15 U.S.C. 6801-6809). As discussed in more detail below, the GLB Act distinguishes “consumers” from “customers” for purposes of its notice requirements. Generally speaking, a customer is a consumer with whom a financial institution has established a “customer relationship.” See *id.* §§ 502(a), 503(a) and 509(9) and (11).

³ See *id.* § 509(3)(B).

Securities and Exchange Commission (SEC), National Credit Union Administration, and Federal Trade Commission (FTC) (collectively with the Banking Agencies, the Agencies)—have each adopted implementing regulations under Title V.⁴

The Commodity Futures Modernization Act of 2000 (CFMA) amended the Commodity Exchange Act (CEA or Act) to provide that certain entities subject to the Commission’s jurisdiction—specifically, futures commission merchants (FCMs), commodity trading advisors (CTAs), commodity pool operators (CPOs) and introducing brokers (IBs)—shall be treated as financial institutions for purposes of Title V. At the same time, Congress also amended the CEA to make the Commission a federal functional regulator within the meaning of Title V and to require the Commission to prescribe regulations under Title V within six months.

The Commission has consulted with representatives from the Agencies throughout this rulemaking process, including during the comment period. The rules that we are adopting today are, to the extent possible, consistent with and comparable to the rules adopted by the Agencies. The rules include examples that illustrate the application of the general rules and an appendix of sample clauses that may, to the extent applicable, be used by FCMs, CTAs, CPOs and IBs to comply with the notice and opt-out requirements. These examples and sample clauses differ from those used by the Agencies in order to provide more meaningful guidance to the financial institutions subject to the Commission’s jurisdiction. Furthermore, in order to minimize compliance burdens, the rules permit those firms that are registered with both the Commission and the SEC to comply with part 160 by complying with the privacy rules of the SEC, which are found at 17 CFR part 248. Similarly, the Commission has determined to permit CTAs that are also registered or required to be registered as an investment advisor with a state securities regulator to comply with part 160 by complying with the privacy rules of the FTC, 16 CFR part 313.

⁴ See 65 FR 40334 (June 29, 2000) (SEC); 65 FR 35162 (June 1, 2000) (Secretary of the Treasury and the Banking Agencies); 65 FR 33646 (May 24, 2000) (FTC); 65 FR 31722 (May 18, 2000) (National Credit Union Administration). See also 66 FR 8616 (Feb. 1, 2001) (Secretary of the Treasury and the Banking Agencies); 66 FR 8152 (Jan. 30, 2001) (National Credit Union Administration); 65 FR 54186 (Sept. 7, 2000) (FTC—advance notice of proposed rulemaking) (Guidelines for Establishing Standards for Safeguarding Customer Information).

Title V also requires the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction to safeguard customer records and information. The rules that we are adopting today require FCMs, CTAs, CPOs and IBs to adopt appropriate policies and procedures that address safeguards to protect this information.

II. Overview of Comments Received

On March 19, 2001, the Commission issued a notice of proposed rulemaking (the proposal" or "proposed rules").⁵ The Commission received a total of four comments in response to the proposal.

Managed Futures Association (MFA), a trade association, commented on the following aspects of the proposal: The proposed compliance date; exemptions for unregistered entities; and substituted compliance for dual registrants and affiliated financial institutions. MFA expressed support for the Commission's statement regarding its jurisdiction under the privacy rules over entities that are either registered or exempt from registration, and its belief that the rules are consistent with Congressional intent as expressed in the CFMA and with the privacy rules adopted by the other federal functional regulators.

The Futures Industry Association (FIA) wrote generally in support of the proposed rules, endorsing the Commission's proposal to permit those Commission registrants who are also registered with the SEC to comply instead with the SEC's parallel rules. In this regard, FIA suggested that the Commission's final rules clarify the scope of its substituted compliance provision and expressed support for an expansion of the substituted compliance provision. FIA also recommended that the Commission's proposal to exclude from compliance non-U.S. entities that are exempt from registration pursuant to an order issued under Commission rule 30.10. Finally, FIA requested that the Commission expand the subsequent delivery exceptions to the initial notice requirement in proposed rule 160.4(e) to permit an FCM that accepts customer accounts in a bulk transfer pursuant to Commission rule 1.65 to provide its initial privacy notice subsequent to the establishment of a relationship with such customers.

Southwest Futures, Inc., an IB, objected to the ability of an FCM to share with others confidential information regarding an IB's customers. A member of the public expressed general support for rules to facilitate the

privacy of citizens' nonpublic information but suggests that the definition of "consumer" be expanded.

These comments, and the Commission's responses, are discussed in greater detail below.

III. Section-by-Section Analysis

Section 160.1 Purpose and Scope

Paragraph (a) of section 160.1 identifies three purposes of the rules. First, the rules require a financial institution to provide notice to customers about the institution's privacy policies and practices. Second, the rules describe the conditions under which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party. Third, the rules provide a method for a consumer to "opt out" of the disclosure of that information to nonaffiliated third parties, subject to certain exceptions discussed below.

Paragraph (b) sets out the scope of the Commission's rules and identifies the financial institutions covered by the rules. The Commission proposed including all FCMs, CTAs, CPOs and IBs within the scope of part 160, whether or not such entities were required to register with the Commission. The Commission, however, specifically solicited comment on whether it should seek to exempt some or all categories of unregistered CTAs and CPOs from part 160's coverage. MFA commented that the Commission should exempt, or alternatively create a safe harbor permitting more limited compliance for, unregistered CTAs and CPOs that do not provide nonpublic information to nonaffiliated third parties outside those permitted under the service provider exception. MFA asserted that Congress did not intend to subject all financial institutions subject to the Commission's jurisdiction to the privacy rules, that the Commission had proposed exempting foreign unregistered FCMs from part 160's scope, and that an exemption for unregistered CTAs and CPOs would be consistent with Congress's intent to the extent that such unregistered entities are not sharing nonpublic consumer information with nonaffiliated third parties.

The Commission has carefully considered MFA's comment and has decided not to amend the proposed rules to exempt or create a safe harbor for unregistered CTAs and CPOs. From the face of the statute, it appears that Congress intended to treat all CTAs and CPOs as financial institutions,

irrespective of their registration status.⁶ The Commission also believes that it would be inconsistent with Title V of the GLB Act to exempt unregistered CTAs and CPOs from part 160 because that title is a consumer protection law that appears designed to afford privacy protection to all consumers.⁷ For these reasons, the Commission believes that all CTAs and CPOs should be required to comply with the requirements of part 160 and notes the limited nature of those requirements for CTAs and CPOs that do not share nonpublic personal information with nonaffiliated third parties.

Paragraph (b) also provides that part 160 does not apply to any foreign (or non-resident) FCM, CTA, CPO or IB that is not registered or required to be registered with the Commission. The Commission believes that it would be impracticable to apply part 160 to those foreign unregistered entities and, further, that subjecting these unregistered foreign entities to the obligations to provide the privacy and opt out notices under part 160 would not add to the protections provided to customers under the GLB Act. If a foreign financial institution conducts activities through U.S. interstate commerce in a manner that subjects it to the registration requirements of the Act, and such foreign financial institution has not been exempted from registration requirements by the Commission, it is subject to the part 160 requirements and any other applicable protections to customers, such as anti-fraud protections. The Commission expressly sought comment on the application of this approach to firms that have been exempted from registration requirements pursuant to a rule 30.10 order. FIA observed that it would be difficult, if not impossible, for the Commission to assure compliance

⁶ Section 5g of the Act states in relevant part that "any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker that is subject to the jurisdiction of the Commission with respect to any financial activity shall be treated as a financial institution for purposes of Title V [of the GLB Act] with respect to such financial activity." (emphasis added) The SEC also has applied its privacy regulations to unregistered brokers, dealers and funds. 65 FR at 40335 n.12. In accordance with section 505(a)(5) of the GLB Act, however, the SEC's privacy rules do not apply to investment advisers that are not registered with the SEC. *Id.*

⁷ MFA correctly notes that the Commission is exempting foreign unregistered FCMs from the scope of part 160. *See infra*. This approach maintains consistency with the approach taken by the other federal functional regulators with regard to offshore financial institutions. To the Commission's knowledge, the other federal functional regulators have not exempted any domestic entities from the scope of their privacy rules.

⁵ Privacy of Customer Information, 66 FR 15550 (Mar. 19, 2001).

by such entities with its privacy rules and, moreover, that these entities may be subject to privacy laws in their home countries that are different from, and may be stricter than, the Commission's rules. While the Commission supports consistent protections for consumers regardless of the entity from whom a financial product or service is obtained, at this stage the Commission does not believe that it is appropriate to attempt to apply the rule to offshore offices of financial institutions. Accordingly, the Commission has adopted the rule as proposed, but will continue to consider this question.

We note that other federal, State, or applicable foreign laws may impose limitations on disclosures of nonpublic personal information in addition to those imposed by the GLB Act and the privacy rules the Commission is adopting today. Thus, financial institutions will need to monitor and comply with relevant legislative and regulatory developments that affect the disclosure of consumer information. Paragraph (b) also makes clear that nothing in the rules is intended to supercede rules relating to medical information that have been issued by the Secretary of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d-1320d-8.⁸

Section 160.2 Rule of Construction

Paragraph (a) of section 160.2 sets out a rule of construction intended to clarify the effect of the examples used in the rules and the sample clauses in the appendix to the rules. Given the wide variety of transactions that Title V covers, new part 160 includes rules of general applicability and provides examples that are intended to assist financial institutions in complying with the rule. The examples are not intended to be exhaustive; rather, they are intended to provide guidance on how the rules would apply in specific situations. The rule also states that compliance with the examples will constitute compliance with the rule.⁹ The Commission believes that, when read together, these provisions give financial institutions sufficient flexibility to comply with the regulation and sufficient guidance about the use of the examples. FIA endorses this approach and has asked that the Commission consider publishing additional guidance similar to that published by the federal banking

regulators when they promulgated their privacy rules.

Paragraph (b) of section 160.2 authorizes "substituted compliance" in certain situations. Specifically, paragraph (b)(1) provides that an FCM, CTA, CPO or IB that is also registered with the SEC in an equivalent capacity may comply with part 160 by complying with Regulation S-P, the privacy rules of the SEC, which are found at 17 CFR part 248. Similarly, under this provision, securities broker-dealers registered with the SEC that are also registered with the Commission as an FCM or IB pursuant to a notice registration for the purpose of trading security futures products¹⁰ will also be deemed to be in compliance with part 160 if they are subject to and in compliance with Regulation S-P. Paragraph (b)(2) of section 160.2 provides that a CTA that is a state-registered investment adviser may comply with part 160 by complying with the privacy rules of the FTC, which are found at 16 CFR part 313.¹¹

Section 160.2's authorization of substituted compliance is in no way designed to affect or limit the Commission's authority to enforce its privacy rules against FCMs, CTAs, CPOs and IBs engaged in activities subject to its jurisdiction. Rather, this provision simply authorizes the identified financial institutions to comply with part 160 by complying with certain other substantially similar regulations, and to establish that they have complied with part 160 by establishing that they have complied with those other regulations. In this regard, because the Commission has provided part 160 examples that are tailored to entities under its jurisdiction, the Commission encourages those entities that elect to comply with the substituted compliance provisions in paragraph (b) to look to the Commission's examples for guidance in complying with the privacy rules of the SEC and FTC, respectively.

In its proposal, the Commission requested comment on whether it should provide for a broader form of substituted compliance by permitting an FCM that is affiliated with a financial holding company, a bank holding company, a national bank or a broker-dealer to comply with part 160 by complying with the privacy rules of the

functional regulator for the affiliated entity. Both MFA and the FIA endorsed substituted compliance for affiliated financial institutions. While the Commission believes that permitting broader substituted compliance is a desirable goal, we have decided not to adopt this approach at this time. Rather, we believe it would be preferable to address this issue after we have gained some administrative experience under these rules and have further consulted with the other federal functional regulators.

Section 160.3 Definitions

(a) *Affiliate*. The rules incorporate the definition of "affiliate" used in section 509(6) of the GLB Act. Thus, an FCM, CTA, CPO or IB is considered affiliated with another company if it "controls," is controlled by, or is under common control with the other company.¹² The definition includes both financial institutions and entities that are not financial institutions. The rules also provide that an FCM, CTA, CPO or IB will be considered an affiliate of another company for purposes of the privacy rules if (i) the other company is regulated under Title V by one of the Agencies and (ii) the privacy rules adopted by that Agency treat the FCM, CTA, CPO or IB as an affiliate of the other company.¹³

(b) *Clear and conspicuous*. Title V and the final rules require that various notices be "clear and conspicuous." The Commission has defined that term as it has been defined in the respective rules of the Agencies, with conforming changes.¹⁴ Section 160.3(b) defines the term to mean that the notice must be "reasonably understandable and designed to call attention to the nature and significance of the information in the notice." This phrase is intended to provide meaning to the term "conspicuous." The Commission believes that this standard will result in

¹² We have defined "control" for purposes of an FCM, CPO, CTA or IB to mean the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. In addition, ownership of more than 25 percent of a company's voting securities creates a presumption of control of the company. See *infra* discussion of section 160.3(j). Compare 65 FR at 35207 (Federal Reserve Board).

¹³ Section 160.3(a)(1)-(2). This part of the definition is designed to prevent the disparate treatment of affiliates within a holding company structure. For example, without this provision an FCM in a bank holding company structure might not be considered affiliated with another entity in that organization under the Commission's rules, even though the two entities would be considered affiliated under the privacy rules of the Banking Agencies.

¹⁴ See, e.g., 12 CFR 40.3(b) (OCC rules) and 17 CFR 248.3(c) (SEC rules).

⁸ See 65 FR 82462 (Dec. 28, 2000).

⁹ Compare 65 FR at 35227 (OCC rules) with 65 FR at 40363 (SEC rules).

¹⁰ See CFMA § 252.

¹¹ This provision responds to a comment of NFA seeking broader substituted compliance for investment advisers that are state-registered and therefore subject to the FTC's privacy rules rather than the SEC's privacy rules. Financial institutions that choose to substitute compliance with the FTC's rules should nonetheless refer to the examples provided throughout part 160.

notices to consumers that communicate effectively the information consumers need in order to make an informed choice about the privacy of their information, including whether to open a commodity interest account or enter into an advisory agreement.

Examples of "clear and conspicuous." The rules provide generally applicable guidance about ways in which an FCM, CTA, CPO or IB may make a disclosure clear and conspicuous. We note that the examples do not mandate how to make a disclosure clear and conspicuous. A financial institution must decide for itself how best to comply with the general rule, and may use techniques not listed in the examples.

Combination of several notices. The Commission is aware that a document may combine different types of disclosures that are subject to specific disclosure requirements under different regulations. For example, a CTA that includes a privacy notice in its disclosure document would have to make the privacy notice clear and conspicuous, and would have to prepare the disclosure document according to certain standards under the CEA and Commission regulations.¹⁵ The rule provides an example of how a financial institution may make privacy disclosures conspicuous, including privacy disclosures that are combined in a document with other information.¹⁶ In order to avoid the potential conflicts between two different rules requiring different sets of disclosures that are subject to different standards, the rule does not mandate precise specifications for presenting various disclosures.

Disclosures on Internet web pages. The rule provides guidance on how financial institutions may clearly and conspicuously disclose privacy-related information on their Internet sites. Disclosures over the Internet may present some issues that will not arise in paper-based disclosures. Consumers may view various web pages within a financial institution's web site in a different order each time they access the site, aided by hypertext links. Depending on the hardware and software used to access the Internet, some web pages may require consumers to scroll down to view the entire page. To address these issues, the rule provides an example concerning

Internet disclosures stating that FCMs, CTAs, CPOs and IBs may comply with the rule if they use text or visual cues to encourage scrolling down the page if necessary to view the entire notice, and ensure that other elements on the web site (such as text, graphics, hypertext links, or sound) do not distract attention from the notice.¹⁷ The examples also note that the institution should place a notice or a conspicuous link on a screen that consumers frequently access, such as a page on which consumers conduct transactions.

There is a range of approaches an FCM, CTA, CPO or IB could use based on current technology. For example, an FCM could use a dialog box that pops up to provide the disclosure before a consumer provides information to a financial institution. Another approach would be a simple, clearly labeled graphic located near the top of the page or in close proximity to the financial institution's logo, directing the customer, through a hypertext link or hotlink, to the privacy disclosures on a separate web page.

(c) *Collect.* The GLB Act requires a financial institution to disclose in its initial and annual notices the categories of information that the institution collects. The Commission has defined this term to mean obtaining information that can be organized or retrieved by the name of the individual or by another identifying number, symbol, or other identifying particular assigned to the individual,¹⁸ irrespective of the source of the underlying information. The definition is intended to provide guidance about the information that an FCM, CTA, CPO or IB must include in its notices and to clarify that the obligations arise regardless of whether the institution obtains the information from a consumer or from some other source. This definition is not intended to include information that an FCM, CTA, CPO or IB receives but then immediately passes on without retaining a copy, as such information would not be organized and retrievable.

(d) *Commission.* The term "Commission" means Commodity Futures Trading Commission.

(e) *Commodity pool operator.* The term "commodity pool operator" has the same meaning as in section 1a(5) of the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(f) *Commodity trading advisor.* The term "commodity trading" advisor has the same meaning as in section 1a(6) of

the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(g) *Company.* The rules define "company" to mean any corporation, limited liability company, business trust, general or limited partnership, association or similar organization.

(h) *Consumer.* The rules define "consumer" as an individual (including his or her legal representative) who obtains a financial product or service from an FCM, CTA, CPO or IB that is to be used primarily for personal, family or household purposes. An individual also will be deemed to be a consumer for purposes of a financial institution if that institution purchases the individual's account from some other institution. The GLB Act distinguishes "consumers" from "customers" for purposes of the notice requirements imposed by that Act. As explained in the discussion of section 160.4, a financial institution must give a "consumer" the notices required under Title V only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for a purpose that is not authorized by one of several exceptions set out in sections 160.14 and 160.15. By contrast, a financial institution must give all "customers," not later than the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship, a notice of the institution's privacy policy.

A person is a "consumer" under the rules if he or she obtains a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes. The definition of "financial product or service" in section 160.3(o) includes, among other things, a financial institution's evaluation of an individual's application to obtain a financial product or service. Thus, a financial institution that intends to share nonpublic personal information about a consumer with nonaffiliated third parties outside of the exceptions described in sections 160.14 and 160.15 will have to give the requisite notices, even if the application or request is denied or withdrawn.

The examples that follow the definition of "consumer" explain when someone is a consumer. The examples clarify that a consumer includes someone who provides nonpublic personal information in connection with seeking to obtain commodity interest trading or advisory services, but does not include someone who provides only his or her name, address, and areas of investment interest in order to obtain a

¹⁵ See 7 U.S.C. 6m; 17 CFR part 4.

¹⁶ See section 160.3(b)(2)(ii)(E). Because we believe that privacy disclosures may be clear and conspicuous when combined with other disclosures, this section does not mandate that privacy disclosures be provided on a separate piece of paper. The requirement is not necessary and might significantly increase the burden on financial institutions.

¹⁷ Section 1603.(b)(2)(iii).

¹⁸ The definition uses language from the Privacy Act of 1974, 5 U.S.C. 552a.

brochure or other information about a financial product or service.¹⁹ An individual who has an account with an originating FCM and whose positions are carried by a clearing FCM in an omnibus account in the name of the originating FCM is not a consumer for purposes of the clearing FCM if the clearing FCM receives no nonpublic personal information about the consumer.

Requirements arising from consumer relationship. While the rules define “consumer” broadly, we note that this definition will not result in any additional burden to an FCM, CTA, CPO or IB if (i) no customer relationship is established and (ii) the institution does not intend to disclose nonpublic personal information about the consumer to nonaffiliated third parties. Under this approach, an FCM, CTA, CPO or IB is under no obligation to provide a consumer who is not a customer with any privacy disclosures unless it intends to disclose the consumer’s nonpublic personal information to nonaffiliated third parties outside the exceptions in sections 160.14 and 160.15. The institution may disclose a consumer’s nonpublic personal information to nonaffiliated third parties if it delivers the requisite notices and the consumer does not opt out. Thus, the rule allows a financial institution to avoid all of the rule’s requirements for consumers who are not customers if the institution chooses not to share information about the consumers with nonaffiliated third parties except as provided in the exceptions. Conversely, if an FCM, CTA, CPO or IB chooses to share consumers’ nonpublic personal information with nonaffiliated third parties, the financial institution is free to do so, provided it notifies consumers about the sharing and affords them a reasonable opportunity to opt out. In this way, the rule attempts to strike a balance between protecting an individual’s nonpublic personal information and minimizing the burden on a financial institution.

(i) *Consumer reporting agency.* The rules incorporate the definition of “consumer reporting agency” in section 603(f) of the Fair Credit Reporting Act (FCRA).²⁰ The term is used in sections 160.12 and 160.15.

(j) *Control.* The rules define “control” for purposes of FCMs, CTAs, CPOs or IBs to mean the power to exercise a

controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. In addition, ownership of more than 25 percent of a company’s voting securities creates a presumption of control of the company. This definition is used to determine when companies are affiliated, and results in financial institutions being considered as affiliates regardless of whether the control is exercised by a company or individual.

(k) *Customer.* The rules define “customer” as any consumer who has a “customer relationship” with a particular financial institution. Thus, a consumer becomes a customer of a financial institution when he or she enters into a continuing relationship with the institution. For example, a consumer would become a customer when he or she completes the documents needed to open a commodity interest account or enters into an advisory agreement (whether in writing or orally).

The distinction between consumers and customers determines the notices that a financial institution must provide. If a consumer never becomes a customer, the institution is not required to provide any notices to the consumer unless the institution intends to disclose nonpublic personal information about that consumer to nonaffiliated third parties (outside of the exceptions as set out in sections 160.14 and 160.15). By contrast, if a consumer becomes a customer, the institution must provide a copy of its privacy policy no later than at the time it establishes the customer relationship and at least annually during the continuation of the customer relationship.

(l) *Customer relationship.* The rules define “customer relationship” as a continuing relationship between a consumer and a financial institution in which the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes. Because the GLB Act requires annual notices of the financial institution’s privacy policies to its customers, we have interpreted that Act as requiring more than isolated transactions between a financial institution and a consumer to establish a customer relationship, unless it is reasonable to expect further contact about that transaction between the institution and consumer afterwards. Thus, the rules define “customer relationship” as one that generally is of a continuing nature. As noted in the examples that follow the definition, this

would include a commodity interest account or an advisory relationship. An FCM would have a customer relationship with a consumer when the FCM regularly enters orders for the customer, even if the FCM holds none of the customer’s assets.

A one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. The examples that follow the definition of “customer relationship” clarify that an individual’s purchase or sale of a futures or options contract through an FCM with whom the customer opens an account would be sufficient to establish a customer relationship because of the continuing nature of the service. By contrast, an individual who is merely referred by an IB to an FCM would not be the IB’s customer if the IB does not enter orders for the individual.²¹

(m) *Federal functional regulator.* The rules define the term “federal functional regulator” to include the Commission and each of the Agencies. This term is used in two places. First, it is used in section 160.3(a), the definition of affiliate. Second, it is used in section 160.15(a)(4) for disclosures to law enforcement agencies, “including federal functional regulators.”

(n) *Financial institution.* The rules define “financial institution” as (i) an FCM, CTA, CPO or IB that is registered with the Commission as such or is otherwise subject to the Commission’s jurisdiction, and (ii) any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (BHCA).²² The rules exempt from the definition of “financial institution” those entities specifically excluded by the GLB Act, except to the extent those entities were brought within the scope of Title V by section 5g of the CEA.

The GLB Act excludes “any person or entity” that is subject to the Commission’s jurisdiction from Title V’s coverage.²³ Section 5g of the CEA partially reverses that exclusion by providing that certain entities subject to

²¹ The individual would, however, be a consumer of the IB for purposes of the privacy rules, which would require the IB to provide notices if it intends to disclose nonpublic personal information about the consumer to nonaffiliated third parties outside of the exceptions.

²² 12 U.S.C. 1843(k).

²³ Section 509(3)(B) of the GLB Act provides:

Notwithstanding subparagraph (A), the term “financial institution” does not include any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act.

¹⁹ Individuals may provide this information, for example, on “tear-out” cards from magazines, or in telephone or Internet requests for brochures or other information.

²⁰ 15 U.S.C. 1681a(f).

the Commission's jurisdiction—specifically, FCMs, CTAs, CPOs and IBs—shall be covered by Title V with respect to their financial activity.²⁴ The rule retains the exclusion of the GLB Act, to the extent that it has not been superseded by section 5g of the CEA, to make clear that floor brokers and various trading facilities and clearing organizations that are subject to the Commission's jurisdiction are not “financial institutions” for purposes of the GLB Act.

(o) *Financial product or service.* The rules define “financial product or service” as a product or service (i) that an FCM, CTA, CPO or IB could offer that is subject to the Commission's jurisdiction, or (ii) that a financial institution could offer that is financial in nature, or incidental to such a financial activity, under section 4(k) of the BHCA. An activity that is complementary to a financial activity, as described in section 4(k), is not included in the definition of “financial product or service” under this paragraph.

The Commission's definition of “financial product or service” differs from that of the other Agencies to the extent that it includes any product or service that an FCM, CTA, CPO or IB could offer that is subject to the Commission's jurisdiction and that is not otherwise included as a financial activity under section 4(k) of the BHCA. The other Agencies have defined financial product or service as any product or service that a financial institution could offer that is financial in nature, or incidental to such a financial activity, under section 4(k) of the BHCA. The Commission's broader definition includes certain activity—such as acting as a CPO—which is not financial in nature, or incidental to such a financial activity, under section 4(k) of the BHCA.²⁵ The Commission's definition of “financial product or service” is designed to implement Congress' intent in section 5g of the CEA that customers of FCMs, CTAs, CPOs and IBs be accorded the same privacy rights as customers of other financial institutions and is solely for purposes of part 160.

²⁴ Section 5g of the CEA provides:

Notwithstanding section 509(3)(B) of the Gramm-Leach-Bliley Act, any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker that is subject to the jurisdiction of the Commission under this Act with respect to any financial activity shall be treated as a financial institution for purposes of title V of such Act with respect to such financial activity.

²⁵ See 12 CFR 225.86 (66 FR 400, 418 (Jan. 3, 2001)).

The definition includes the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service even if the application ultimately is rejected or withdrawn. It also includes the distribution of information about a consumer for the purpose of assisting the consumer to obtain a financial product or service.

(p) *Futures commission merchant.* The term “futures commission merchant” has the same meaning as in section 1a(20) of the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(q) *GLB Act.* The term “GLB Act” means the Gramm-Leach-Bliley Act (Pub. L. No. 106-102, 113 Stat. 1338 (1999)).

(r) *Introducing broker.* The term “introducing broker” has the same meaning as in section 1a(23) of the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(s) *Nonaffiliated third party.* The rule defines “nonaffiliated third party” to mean any person (including natural persons as well as corporate entities) except (i) an affiliate of a financial institution and (ii) a joint employee of a financial institution and a third party. Information received by a joint employee will be deemed to have been given to the financial institution that is providing the financial product or service in question. Thus, for example, if an employee of a broker-dealer is also an employee of an FCM, information that the employee received in connection with a securities transaction conducted with the broker-dealer would be considered as received by the broker-dealer.

(t) *Nonpublic personal information.* Section 509(4) of the GLB Act defines “nonpublic personal information” to mean “personally identifiable financial information” that (i) is provided by a consumer to a financial institution, (ii) results from any transaction with the consumer or any service performed for the consumer, or (iii) is otherwise obtained by the financial institution. The term also includes any “list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any nonpublic personal information that is not publicly available information.” The GLB Act excludes publicly available information (unless provided as part of the list, description, or other grouping described above), as well as any list, description, or other grouping of consumers (and

publicly available information pertaining to them) that is derived without using nonpublic personal information. The GLB Act does not define either “personally identifiable financial information” or “publicly available information.”

The rule implements the definition of “nonpublic personal information” under the GLB Act by restating the categories of information described above. The rule provides that information will be deemed to be “publicly available” and therefore excluded from the definition of “nonpublic personal information” if an FCM, CTA, CPO or IB reasonably believes that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule.²⁶ The examples provided in the rule clarify when an FCM, CTA, CPO or IB has a reasonable belief that information is lawfully made available to the general public. For example, an institution would have a reasonable belief if (i) the institution has confirmed, or the consumer has represented, that the information is publicly available from a public source, or (ii) the institution has taken steps to submit the information, in accordance with its internal procedures and policies and with applicable law, to a keeper of federal, State, or local government records who is required by law to make the information publicly available.²⁷ The examples also state that an FCM, CTA, CPO or IB would have a reasonable belief that a telephone number is publicly available if the institution located the number in a telephone book or Internet listing service or if the consumer told the institution that the number is not unlisted.²⁸ Moreover, the examples make clear that an institution may not assume information about a particular consumer is publicly available simply because that type of information is normally provided to a government record keeper and made available to the public by the record keeper, because the consumer may have the ability to keep that information nonpublic or to screen his or her identity.

The approach of the rule is the same as that taken by the Agencies in their rules²⁹ and is based on the underlying principle that a consumer in many circumstances can control the public availability or identification of his or

²⁶ See section 160.3(v)(1).

²⁷ See section 160.3(v)(2)(i)(B).

²⁸ See section 160.3(v)(2)(i)(C).

²⁹ See, e.g., 65 FR at 35208 (Federal Reserve Board); 65 FR at 35218 (Federal Deposit Insurance Corporation); 65 FR at 40364-65 (SEC).

her information and that a financial institution therefore should not assume that the information about that consumer is in fact publicly available. Thus, even though a lender typically enters a mortgage in public records in order to protect its security interest, when a borrower can maintain the privacy of his or her personal information by owning the property and obtaining the loan through a separate legal entity, the customer's name would not appear in the public record. In the case of a telephone number, a person may request that his or her number be unlisted. Thus, in evaluating whether it is reasonable to believe that information is publicly available, a financial institution must determine whether the consumer has kept the information or his or her identity from being a matter of public record.

To implement the complex definition of "nonpublic personal information" that is provided in the statute, the rule adopts a definition that consists, generally speaking, of (i) personally identifiable financial information, plus (ii) a consumer list or description or grouping of consumers (and publicly available information pertaining to the consumers) that is derived using any personally identifiable financial information that is not publicly available information. From that body of information, the rule excludes publicly available information (except as noted above or if the information is disclosed in a manner that indicates that the individual is the institution's consumer) and any consumer list that is derived without using personally identifiable financial information that is not publicly available information.³⁰ Examples are provided in section 160.3(t)(3) to illustrate how this definition applies in the context of consumer lists.

(u) *Personally identifiable financial information.* As discussed above, the GLB Act defines "nonpublic personal information" to include, among other things, "personally identifiable financial information" but does not define the latter term. As a general matter, the rules treat any personally identifiable information as financial if the financial institution obtains the information in connection with providing a financial product or service to a consumer. We believe that this approach reasonably interprets the word "financial" and creates a workable and clear standard for distinguishing information that is financial from other personal information. This interpretation would cover a broad range of personal

information provided to a financial institution, including, for example, information about the consumer's health, as well as the fact that an individual is a customer of a financial institution.

The rules define "personally identifiable financial information" to include three categories of information. The first category includes any information that a consumer provides a financial institution in order to obtain a financial product or service from the institution. As noted in the examples that follow the definition, this includes information provided on an application to open a commodity trading account, invest in a commodity pool or to obtain another financial product of service. If, for example, a consumer provides medical information on an application to obtain a financial product or service, that information would be considered "personally identifiable financial information" for purposes of the proposed rules. Similarly, information that may be required for financial planning purposes, including details about retirement and family obligations, such as the care of a disabled child, would be covered by the definition.

The second category includes any information about a consumer resulting from any transaction between the consumer and the financial institution involving a financial product or service. This would include, as noted in the examples following the definition, information about account balance, payment or overdraft history, credit or debit card purchases or financial products purchased or sold.

The third category includes any financial information about a consumer otherwise obtained by the financial institution in connection with providing a financial product or service. This would include information obtained through an information-collecting device from a web server, often referred to as a "cookie." It would also include information from a consumer report or from an outside source to verify information a consumer provides on an application to obtain a financial product or service. It would not, however, include information that is publicly available (unless, as previously noted, the information is part of a list of consumers that is derived using personally identifiable financial information).

The examples clarify that the definition of "personally identifiable financial information" does not include a list of names and addresses of people who are customers of an entity that is not a financial institution. Thus, the names and addresses of people who

subscribe, for instance, to a particular magazine would fall outside the definition. The examples also clarify that aggregate information (or "blind data") lacking personal identifiers is not covered by the definition of "personally identifiable financial information."

(v) *Publicly available information.* The rules define "publicly available information" as information the financial institution reasonably believes is lawfully made available to members of the general public from three broad types of sources.³¹ First, it includes information from official public records, such as real estate recordings or security interest filings. Second, it includes information from widely distributed media, such as a telephone book, radio program, or newspaper. Third, it includes information from disclosures required to be made to the general public by federal, State, or local law, such as securities disclosure documents. The rules state that information obtained over the Internet will be considered publicly available information if the information is obtainable from a site available to the general public on an unrestricted basis.³²

The rules treat information as publicly available if it could be obtained from one of the public sources listed in the rules. If an institution reasonably believes the information is lawfully made available to the general public from one of the listed public sources, then the information will be considered publicly available and excluded from the scope of "nonpublic personal information," whether or not the institution obtains it from a publicly available source (unless, as previously noted, it is part of a list of consumers that is derived using personally identifiable financial information). Under this approach, the fact that a consumer has given information to a financial institution would not automatically extend to that information

³¹ We recognize that some information that is available to the general public may have been published illegally. In some cases, such as a list of customer account numbers posted on a web site, the publication will be obviously unlawful. In other cases, the legality of the publication may be unclear or unresolved. The rules provide that information is "publicly available" if the institution reasonably believes that information is lawfully available to the public.

³² The examples further explain that an Internet site is not restricted merely because an Internet service provider or a site operator requires a fee or password as long as access is otherwise available to the general public. This recognizes that the "widely distributed" requirement focuses on whether the information is lawfully available to the general public, rather than on the type of medium from which information is obtained.

³⁰ See section 160.3(t)(2).

the protections afforded to nonpublic personal information.

The rules incorporate the concept of information being lawfully obtained. Thus, information unlawfully obtained will not be deemed to be publicly available notwithstanding that it may be available to the general public through widely distributed media.

(w) *You*. The rules define you as any FCM, CTA, CPO or IB subject to the jurisdiction of the Commission. The term “you” is used in order to make the rules easier to understand and use.

Subpart A—Privacy and Opt Out Notices

Section 160.4 Initial Privacy Notice to Consumers Required

Initial notice required. The GLB Act requires that a financial institution provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided no later than at the time of establishing a customer relationship. For consumers who do not, or have not yet, become customers, the notice must be provided before disclosing nonpublic personal information about the consumer to a nonaffiliated third party.

Paragraph (a) of section 160.4 states the general rule regarding these notices. A financial institution must provide a clear and conspicuous notice, as defined in section 160.3(b), that accurately reflects the institution’s privacy policies and practices. Accordingly, a financial institution must maintain the protections that its notice represents it will provide. The Commission expects that FCMs, CTAs, CPOs and IBs will take appropriate measures to adhere to their stated privacy policies and practices.

The rules do not prohibit two or more institutions from providing a joint initial, annual or opt out notice, as long as the notice is delivered in accordance with the rules and is accurate with respect to all institutions.³³ For example, institutions that could provide joint notices include: (i) an IB and its FCM; (ii) a CTA and the FCM carrying the customer’s account; and (iii) a clearing FCM and an executing FCM. Similarly, the rules do not preclude an institution from establishing different privacy policies and practices for different categories of consumers, customers or products so long as each particular consumer or customer receives a notice that is accurate with respect to that individual.

Notice to customers. The rules require that a financial institution provide an

individual a privacy notice not later than the time that it establishes a customer relationship subject to the limited circumstances set forth in paragraph (e), as discussed below. Thus, the initial notice may be provided at the same time an FCM, CTA, CPO or IB is required to give other notices, such as the rule 1.55 risk disclosure statement that an FCM or IB is required to provide before opening an account for a customer and the part 4 disclosure document that a CPO or CTA is required to provide before soliciting or accepting funds from pool participants (in the case of a CPO) or soliciting or entering into an agreement to direct a client’s account (in the case of a CTA).³⁴ This approach is intended to strike a balance between (i) ensuring that consumers will receive privacy notices at a meaningful point during the process of “establishing a customer relationship” and (ii) minimizing unnecessary burdens on FCMs, CTAs, CPOs and IBs that may otherwise result if the rule were to require financial institutions to provide consumers with a series of notices at various times in a transaction.

Paragraph (c) of section 160.4 identifies the time a customer relationship is established as the point at which a financial institution and a consumer enter into a continuing relationship. The examples in paragraph (c) clarify that, for customer relationships that are contractual in nature including, for example, a commodity interest advisory relationship, a customer relationship is established when the customer enters into the contract (whether written or oral) that is necessary to engage in the activity in question. Thus, for example, a customer relationship is established with an FCM when the customer executes a commodity interest trade through the FCM or opens an account with the FCM under its procedures.

Notice to consumers. For consumers who do not establish a customer relationship, the initial privacy notice may be provided at any point before the financial institution discloses nonpublic personal information to nonaffiliated third parties. As provided in paragraph (b) of section 160.4, if the institution does not intend to disclose the information in question or intends to

make only those disclosures that are authorized by one of the exceptions or as required by law,³⁵ the institution is not required to provide the initial notice.

How to provide notice. When you are required by this section to deliver an initial privacy notice, the notice must be delivered according to the provisions of section 160.9. The general rule requires that the initial notice be provided so that each recipient can reasonably be expected to receive actual notice.

New notices not required for each new financial product or service. The Commission believes that it would be burdensome, with little corresponding benefit to the consumer, to require a financial institution to provide the same consumer with additional copies of its initial notice every time the consumer obtains a financial product or service. Accordingly, the final rule states, in section 160.4(d), that a financial institution will satisfy the notice requirements when an existing customer obtains a new financial product or service if the institution’s initial, revised or annual notice is accurate with respect to the new financial product or service.

Exceptions to allow subsequent delivery of notice. As proposed, section 160.4(e) would permit a financial institution to provide subsequent delivery of the initial notice required by paragraph (a)(1) within a reasonable time after the customer relationship is established in limited instances. For example, the institution may provide notice after the fact if the customer has not elected to establish a customer relationship. This might occur, for instance, when a commodity interest account is transferred from a financially-distressed FCM to another FCM in an emergency situation. Subsequent delivery of the initial notice would also be permitted after the establishment of a customer relationship when to do otherwise would substantially delay the consumer’s transaction and the customer agrees to receive the notice at a later time. An example of this is when an investor requests over the telephone that an FCM execute a trade.

In response to the proposed rules, FIA commented that it was unclear how the subsequent delivery exceptions would apply in the context of a bulk transfer under Commission Rule 1.65. Rule 1.65 establishes a “negative consent” procedure for the transfer of customers’ accounts from one FCM to another. Because the customer has the right to move his or her account to another FCM prior to the transfer, FIA requested

³⁴ The Commission recognizes that the disclosure requirements of part 4 apply as early as the solicitation stage, which often occurs before a customer relationship has been established. See 17 CFR 4.21 (CPO disclosure document) and 17 CFR 4.31 (CTA disclosure document). In these circumstances, a CPO or CTA would not be required to provide the initial privacy notice until such time as the customer relationship has been established, although it could elect to provide the notice earlier at the time of the solicitation.

³⁵ See sections 160.14, 160.15.

³³ See also *infra* discussion of section 160.9(f).

clarification regarding the ability of a transferee FCM to take advantage of the section 160.4(e) exceptions. FIA expressed the belief that subsequent delivery of the initial notice should also be permitted in the bulk transfer context, and asked the Commission to amend the rule accordingly. The Commission agrees with this interpretation and notes that historically, the Commission has considered a bulk transfer to be a transfer that is not at the customer's election. Nevertheless, to provide further guidance, the Commission has determined to add a new exception in paragraph (e)(1)(iv) that specifically addresses a bulk transfer carried out in accordance with Rule 1.65.

We note that, in most situations, a financial institution should give the initial notice at a point when the consumer still has a meaningful choice about whether to enter into the customer relationship. The exceptions listed in the examples, while not exhaustive, are intended to illustrate the less frequent situations when delivery either would pose a significant impediment to the conduct of a routine business practice or the customer agrees to receive the notice later in order to obtain a financial product or service immediately.

In circumstances when it is appropriate to deliver an initial notice after the customer relationship has been established, a financial institution should deliver an initial notice within a reasonable time thereafter. The Commission believes that a rule prescribing the maximum number of days in which a financial institution must deliver a notice in these circumstances would be inappropriate because (a) the circumstances when an after-the-fact notice is appropriate are likely to vary significantly, and (b) a rule that attempts to accommodate every circumstance is likely to provide more time than is appropriate in many circumstances.³⁶

Section 160.5 Annual Privacy Notice to Customers Required

Section 503 of the GLB Act requires a financial institution to provide notices of its privacy policies and practices to its customers at least annually. Section 160.5 implements this requirement by

requiring that a clear and conspicuous notice that accurately reflects the institution's current privacy policies and practices be provided at least once during any period of twelve consecutive months during which the customer relationship exists. An institution may select a calendar year as the 12-month period within which notices will be provided and provide the first annual notice at any point in the calendar year following the year in which the customer relationship was established. Section 160.5(a)(1) also requires that an institution apply the 12-month rule to its customers on a consistent basis. The rules governing how to provide an initial notice also apply to annual notices.

Section 503(a) of the GLB Act requires that the annual notice be provided "during the continuation" of a customer relationship. Accordingly, the rules state that a financial institution is not required to provide an annual notice to a customer with whom it no longer has a continuing relationship. For example, a customer becomes a former customer when the individual's account is closed.

Section 160.6 Information To Be Included in Privacy Notices

Section 503 of the GLB Act identifies the categories of information that must be included in a financial institution's initial and annual privacy notices and establishes the general requirement that a financial institution must provide customers with a notice describing the institution's policies and practices with respect to, among other things, disclosing nonpublic personal information to both affiliates and nonaffiliated third parties. Section 503(b) of the GLB Act identifies certain elements that the notice must address.

The required content is the same for initial and annual notices of privacy policies and practices. While the information contained in the notices must be accurate as of the time the notices are provided, a financial institution may prepare its notices based on current and anticipated policies and practices.

Subsection (a) of section 160.6 prescribes the information to be included; subsection (c) provides examples of how to comply with this requirement.

1. *Categories of nonpublic personal information that a financial institution may collect.* Section 503(b)(2) of the GLB Act requires a financial institution to inform its customers about the categories of nonpublic personal information that the institution collects. Section 160.6(a)(1) implements this requirement and paragraph (c)(1)

provides an example of compliance that focuses on the source of the information collected. As described in the example, a financial institution will satisfy this requirement if it categorizes the information according to the sources, such as application information, transaction information, and consumer report information. While financial institutions may provide more detail about the categories and information collected, they are not required to do so.

2. *Categories of nonpublic personal information that a financial institution may disclose.* Section 503(a)(1) of the GLB Act requires the financial institution's initial and annual notice to provide information about the categories of nonpublic personal information that may be disclosed either to affiliates or nonaffiliated third parties. Rule 160.6(a)(2) implements this requirement. The examples of how to comply with this rule in paragraph (c)(2) focus on the content of the information to be disclosed. A financial institution may satisfy this requirement by categorizing information according to source and providing examples of the content of this information. These categories might include application information (such as assets, income, and investment goals), identifying information (such as name, address and social security number), transaction information (such as information about account activity and balances), and information from consumer reports (such as credit history).

Financial institutions may choose to provide more detailed information in the initial and annual notices. If a financial institution does not disclose, and does not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, its initial and annual notices may simply state this fact without further elaboration about categories of information disclosed.

3. *Categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information.* Section 503(a) of the GLB Act includes a general requirement that a financial institution provide notice to its customers of the institution's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) provides that the notice required by section 503(a) must include certain specified items, including the requirement that a financial institution inform its customers about its policies and practices with respect to disclosing nonpublic personal information to nonaffiliated third parties. We believe

³⁶ The Commission believes, however, that allowing the transferee FCM 60 days to deliver the initial privacy notice to the customer following a Rule 1.65 bulk transfer as requested by FIA would be unreasonable and inconsistent with the intent of the privacy rules. Instead, the transferee FCM would be expected to deliver the initial privacy notice no later than the time that it delivers the monthly account statements required by Rule 1.33.

that sections 503(a) and 503(b) of the GLB Act, when read together, require a financial institution's notice to address disclosures of nonpublic personal information to both affiliates and nonaffiliated third parties.

Rule 160.6(a)(3) implements the notice requirement of section 503. The example in paragraph (c)(3) explains that a financial institution will adequately categorize the affiliates and nonaffiliated third parties to whom it discloses nonpublic information about consumers if it identifies the types of businesses in which they engage. Types of businesses may be described in general terms, such as financial products or services, if the financial institution provides examples of the significant types of businesses engaged in by the recipient, such as retail banking, mortgage lending, life insurance or securities brokerage.

Section 502(e) of the GLB Act creates exceptions to the requirements that apply to the disclosure of nonpublic personal information to nonaffiliated third parties. In addition, section 503(b) of the GLB Act does not require a financial institution to list the categories of persons to whom information may be disclosed under any of those enumerated exceptions. Accordingly, rule 160.6(b) requires only that a financial institution inform consumers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice.

If a financial institution does not disclose, and does not intend to disclose, nonpublic personal information to affiliates or nonaffiliated third parties, its initial and annual notices may state this fact without further elaboration about categories of third parties.

4. *Information about former customers.* Section 503(a)(2) of the GLB Act requires that the financial institution's initial and annual privacy notices include the institution's policies and practices with respect to disclosing nonpublic personal information about persons who have ceased to be customers of the financial institution. Section 503(b)(1)(B) requires that this information be provided with respect to information disclosed to nonaffiliated third parties. We believe that, read together, sections 503(a)(2) and (b)(1)(B) require a financial institution to include in its initial and annual notices the institution's policies and practices with respect to sharing information about former customers with all affiliates and nonaffiliated third parties. Rule 160.6(a)(4) sets forth this requirement. This rule does not require a financial

institution to provide notice and opportunity to opt out to a former customer before sharing nonpublic personal information about the former customer with an affiliate.

5. *Information disclosed to service providers.* Section 502(b)(2) of the GLB Act permits a financial institution to disclose nonpublic personal information about a consumer to a nonaffiliated third party that performs services for the institution, including marketing financial products or services under a joint agreement between the financial institution and at least one other financial institution. In such cases, a consumer has no right to opt out, but the financial institution must inform the consumer that it will be disclosing the information in question unless the service falls within one of the exceptions enumerated in section 502(e) of the GLB Act.

Rule 160.6(a)(5) implements these provisions by requiring that, if a financial institution discloses nonpublic personal information to a nonaffiliated third party under the exception for service providers and joint marketing, it must include in its initial and annual privacy notices a separate description of the categories of information that are disclosed and the categories of third parties providing the services. A financial institution may comply with these requirements by providing the same level of detail in the notice as is required to satisfy sections 160.6(a)(2) and (3).

6. *Right to opt out.* Sections 503(a)(1) and (b)(2) of the GLB Act require a financial institution to provide customers with a notice of its privacy policies and practices concerning, among other things, disclosure of nonpublic personal information consistent with section 502 of the GLB Act. Rule 160.6(a)(6) implements this section of the GLB Act by requiring the initial and annual privacy notices to explain the right to opt out of disclosures of nonpublic personal information to nonaffiliated third parties, and the methods available to exercise that right.

7. *Disclosures made under the Fair Credit Reporting Act.* Pursuant to section 503(b)(4) of the GLB Act, a financial institution's initial and annual notice must include the disclosures, if any, required under section 603(d)(2)(A)(iii) of the FCRA.³⁷ That section excludes from the definition of "consumer report" (and, accordingly, the protections provided under the FCRA for information contained in consumer reports) the communication

of certain consumer information among affiliated entities if the consumer is notified about the disclosure of the information and given an opportunity to opt out of the information sharing. Information that can be shared among affiliates under this provision generally is personal information provided directly by the consumer to the financial institution, such as income and social security number, in addition to information contained in credit bureau reports.

Rule 160.6(a)(7) implements section 503(b)(4) of the GLB Act by requiring that a financial institution's initial and annual privacy notices include any disclosures the institution makes under section 603(d)(2)(A)(iii) of the FCRA.

8. *Confidentiality and security.* Pursuant to section 503(a)(3) of the GLB Act, a financial institution's initial and annual privacy notices must provide information about the institution's policies and practices with respect to protecting the nonpublic personal information of consumers. Section 503(b)(3) requires that the notices include the policies that the financial institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 501, which requires the federal functional regulators to establish standards governing the administrative, technical and physical safeguards of customer information.³⁸

Rule 160.6(a)(8) implements these provisions by requiring a financial institution to include in its initial and annual privacy notices the institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information. The example in the rules states that a financial institution may comply with the requirement for confidentiality and security if the institution explains such matters as who has access to the information and the circumstances under which the information may be accessed. An institution's security policy should include safeguards to protect the integrity of nonpublic personal information and thus, should also focus on the measures the financial institution takes to protect against reasonably anticipated threats or hazards. The rule does not require a financial institution to disclose technical or proprietary information about how it safeguards consumer information.

Short-form initial notice. Although the general rule requires a financial institution to provide both the initial

³⁷ 15 U.S.C. 1681a(d)(2)(A)(iii).

³⁸ See *infra* discussion of section 160.30.

and opt out notices to a consumer before disclosing nonpublic financial information about that person to nonaffiliated third parties, the Commission believes that the need to provide a copy of a financial institution's complete initial notice to consumers is less compelling when there is no customer relationship. Accordingly, section 160.6(d) states that a financial institution may provide a "short-form" initial privacy notice along with the opt out notice to a consumer with whom the institution does not have a customer relationship. The short-form notice must clearly and conspicuously state that the disclosure containing information about the institution's privacy policies and practices is available upon request and provide one or more means by which the consumer may obtain a copy of the notice. The rule also requires a financial institution to provide a consumer who is interested in the more complete privacy disclosures with a reasonable means to obtain them.

Section 160.7 Form of Opt Out Notice to Consumers; Opt Out Methods

Section 160.7 provides that any financial institution required to supply an opt out notice under section 160.10 must provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out. The notice must inform the consumer that the institution may disclose nonpublic personal information to nonaffiliated third parties, state that the consumer has the right to opt out, and provide the consumer with a reasonable means by which to opt out.

The examples provided in paragraph (a)(2) of section 160.7 state that a financial institution will provide adequate notice of the right to opt out if it identifies the categories of information that may be disclosed and the categories of nonaffiliated third parties to whom the information may be disclosed and explains that the consumer may opt out of those disclosures. A financial institution that plans to disclose only limited types of information or to make disclosures only to a specific type of nonaffiliated third party may provide a correspondingly narrow notice to consumers. To minimize the number of opt out notices a financial institution must provide, however, the institution may wish to base its notices on current and anticipated information sharing plans. A new opt out notice is not required for disclosures to different types of nonaffiliated third parties or of different types of information so long as the most recent opt out notice is sufficiently

broad to cover the entities or information in question. A financial institution also need not provide subsequent opt out notices when a consumer establishes a new type of customer relationship with that financial institution, unless the institution's opt out policies vary based on the type of customer relationship.

The examples suggest several methods of providing reasonable means to opt out, including check-off boxes, reply forms, electronic mail addresses, and toll-free telephone numbers. A financial institution does not provide a reasonable means of opting out if the only means provided is for the consumer to write his or her own letter requesting to opt out, although an institution may honor such a letter if received.

Paragraph (b) of section 160.7 applies to delivery of the opt out notice the same rules that apply to delivery of the initial and annual privacy notices,³⁹ and clarifies that the opt out notice may be provided together with, or on the same form as, the initial and annual notices. Paragraph (c) provides that if the opt out notice is provided after the initial notice, a financial institution must provide a copy of the initial notice along with the opt out notice.

Paragraph (d) of section 160.7 states that if two or more consumers jointly obtain a financial product or service from a financial institution, the institution may provide a single opt out notice. The opt out notice must, however, explain how the financial institution will treat an opt out direction by a joint customer. The Commission invited comment on how the right to opt out should apply in the case of joint accounts; no comments were received. The Commission has observed, however, that disclosure obligations arising from joint accounts are well settled under other rules, such as the regulations implementing the Equal Credit Opportunity Act (Regulation B, 12 CFR part 202) and the Truth in Lending Act (Regulation Z, 12 CFR part 226). Under both Regulation B and Regulation Z, a financial institution is permitted to give only one notice. The authorities cited include requirements that the financial institution give disclosures, as appropriate, to the "primary applicant" if this is readily apparent (see 12 CFR 202.9(f) (Reg. B) and 226.5(b) (Reg. Z)). The Commission accordingly believes that a financial institution should have the option of providing one privacy notice per account, regardless of the number of persons on the account. Each of the

account holders must, however, have the right to opt out. The Commission also recognizes that there may be circumstances where one or more of the joint account holders may want separate notices. Accordingly, the final rule states in § 160.7(d) that the financial institution may send one notice, but must honor requests from one or more joint account holders for separate notices. The final rule also requires a financial institution to state in its opt out notice provided to a joint account holder whether the institution will consider an opt out by a joint account holder as an opt out by all of the account holders or whether each account holder is permitted to opt out separately.

Paragraph (e) provides that a financial institution must comply with the customer's opt out as soon as reasonably practicable after receiving it. Paragraph (f) clarifies that a consumer has the right to opt out at any time.

Paragraph (g) states that an opt out will continue until it is revoked by the consumer in writing, in hard copy or, if the consumer agrees, electronically. When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information collected by the financial institution during or related to the relationship. That opt out will continue until the customer revokes it. If that individual subsequently establishes a new customer relationship with the financial institution, however, the opt out direction that applied to the former relationship does not apply to the new relationship and the institution must provide a new opt out notice to the customer in connection with the new relationship.

Section 160.8 Revised Privacy Notices

This section sets forth the rules governing a financial institution's obligations in the event the institution changes its disclosure policies. As stated in this section, a financial institution may not directly or through an affiliate disclose nonpublic personal information to a nonaffiliated third party under the new policy unless the institution first provides a revised notice and a new opportunity to opt out. The institution must wait a reasonable period of time before disclosing information according to the terms of the revised notice in order to afford the consumer a reasonable opportunity to opt out. A financial institution must provide a consumer the revised notice of its policies and practices and an opt out notice in a manner such that each consumer can reasonably be expected to

³⁹ See section 160.9.

receive actual notice, as provided in Section 160.9.

Section 160.9 Delivering Privacy and Opt Out Notices

Paragraph (a) of section 160.9 requires that any privacy and opt out notices provided by a financial institution be provided in a manner such that each consumer can reasonably be expected to receive actual notice in writing, either in hard copy or, if the customer agrees, electronically. Paragraph (b) sets forth examples of reasonable expectation of actual notice, including, for example, hand-delivery to the consumer of a printed copy of the notice, mailing a printed copy of the notice to the last known address of the consumer, and, for a consumer who conducts transactions electronically, posting the notice on the electronic site and requiring the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service. It would not be sufficient to provide only a posted copy of the notice in a lobby. Similarly, it would not be sufficient to provide an initial notice only on a Web page, unless the consumer is required to access that page to obtain the product or service in question. Electronic delivery generally should be in the form of electronic mail to ensure that a consumer actually receives the notice. If a financial institution and a consumer orally agree to enter into a contract for a financial product or service over the telephone, the institution may provide the consumer with the option of receiving an initial notice after providing the product or service so as not to delay the transaction.⁴⁰

Paragraph (c) describes additional examples of reasonable expectation of actual notice that apply only in the context of the annual privacy notice. A financial institution may reasonably expect that a customer who uses the institution's web site to obtain financial products and services will receive actual notice of the annual privacy notice if the customer has agreed to accept notices at the institution's web site and if the institution continuously posts a current notice of its privacy policies and practices in a clear and conspicuous manner on the web site. This paragraph also makes clear that a financial institution need not send the annual privacy notice to a customer who affirmatively requests no communication from the institution, provided that the notice is available upon request. Paragraph (d) prohibits financial institutions from providing

privacy notices orally. Paragraph (e) clarifies that the requirement that a privacy policy be provided in a manner that permits a customer to retain or reaccess the policy may be satisfied if the financial institution makes available on its web site the privacy policy currently in effect.

Section 160.9(f) expressly permits the provision of joint notice from two or more financial institutions as long as the notice is accurate with respect to all financial institutions and identifies each institution by name. The Commission believes that FCMs, CTAs, CPOs and IBs should be able to combine initial, annual, or revised disclosures in one document and to give, on a collective basis, a consumer only one copy of the notice. For example, a clearing FCM could provide a joint notice with an executing FCM for which it clears transactions on a fully disclosed basis, or an IB could provide a joint notice with the FCM to which it introduces trades. The Commission emphasizes that this notice must be accurate for each institution that uses the notice and must identify each institution by name.⁴¹

Where two or more consumers jointly obtain a financial product or service from a financial institution, paragraph (g) of section 160.9 permits the financial institution to satisfy the initial, annual and revised notice requirements of this section by providing one notice to those customers jointly. The final rule adds the provisions that while only one notice is required to be sent in connection with a joint account, the financial institution must honor requests from one or more joint account holders for separate notices and may in its discretion provide notices to each party to an account.

Subpart B—Limits on Disclosures

Section 160.10 Limits on Disclosure of Nonpublic Personal Information to Nonaffiliated Third Parties

Section 502(a) of the GLB Act generally prohibits a financial institution from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution provides the consumer with notice of the institution's privacy

policies and practices. Section 502(b) further requires that the financial institution provide the consumer with a clear and conspicuous notice that the consumer's nonpublic personal information may be disclosed to nonaffiliated third parties, that the consumer be given an opportunity to opt out of that disclosure, and that the consumer be informed as to how to opt out.

Section 160.10 implements these provisions by setting forth the criteria that a financial institution must satisfy before disclosing nonpublic personal information to nonaffiliated third parties and by defining "opt out" in a way that incorporates the exceptions to the right to opt out enunciated in sections 160.13, 160.14 and 160.15.

The rule requires that the consumer's opportunity to opt out be "reasonable," which recognizes that the appropriate waiting time before disclosure will vary depending on many factors including, for example, the method of delivery of the opt out notice. The examples that follow the general rule are intended to provide guidance in situations involving notices by mail or by electronic means and notices that are to be provided in the case of isolated transactions with a consumer. In the case of mail and electronic notices, the consumer will be considered to have had a reasonable opportunity to opt out if the financial institution provides 30 days in which to opt out. In the case of an isolated transaction, the opportunity will be reasonable if the consumer must decide as part of the transaction whether to opt out before completing the transaction.

The requirement that a consumer have a reasonable opportunity to opt out does not mean that the consumer forfeits that right once the opportunity passes. As provided in section 160.7(f), a consumer always has the right to opt out. If, however, a consumer does not exercise the opt out right when first presented with the opportunity, the financial institution will be permitted to disclose nonpublic personal information to nonaffiliated third parties during the period of time before it implements the consumer's subsequent opt out direction.

All customers are consumers under the rules. Accordingly, paragraph (b) of section 160.10 clarifies that the right to opt out applies regardless of whether a consumer has established a customer relationship with the financial institution. The fact that a consumer establishes a customer relationship with a financial institution does not change the institution's obligations to comply with the requirements of section 160.10 before sharing nonpublic personal

⁴¹ In this regard, the Commission believes that each subsidiary or affiliate of a holding company or like structure need not necessarily be identified by legal name as long as the joint notice clearly identifies the institutions covered by the privacy policy. For instance, a privacy policy for ABC & Co. could state that it applies to all institutions with the ABC name. However, if the privacy policy applies to affiliated companies that do not share the ABC name, the policy should specifically identify those affiliates.

⁴⁰ See also section 160.4(e).

information about the consumer with nonaffiliated third parties. Importantly, the rule applies as well in the context of a consumer who had a customer relationship with a financial institution and subsequently terminated the relationship. Paragraph (b) also establishes that the consumer protections afforded by paragraph (a) apply to all nonpublic personal information collected by a financial institution, regardless of when collected. Thus, if a consumer elects to opt out of information sharing with nonaffiliated third parties, the election applies to all nonpublic information about the consumer in the financial institution's possession, regardless of when the information is obtained.

Paragraph (c) of section 160.10 provides that a financial institution may—but is not required to—provide consumers with the option of a partial opt out in addition to the opt out required by this section. This option could enable a consumer to limit, for instance, the types of information disclosed to nonaffiliated third parties or the types of recipients of the nonpublic personal information about that consumer. If the financial institution elects to provide the partial opt out, it must state this option in a way that clearly informs the consumer about the choices available and the resulting consequences.

Section 160.11 Limits on Rediscovery and Reuse of Information

Section 502(c) of the GLB Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or through an affiliate, disclose the information to any person that is not affiliated with either the financial institution or the third party, unless the disclosure would be lawful if it were made directly by the financial institution. Section 160.11 implements the GLB Act's restrictions on rediscovery and reuse of nonpublic personal information about consumers.

The GLB Act places the institution that receives the nonpublic personal information in the shoes of the institution that discloses the information for the purpose of determining whether rediscoveries by the receiving institution are lawful. Thus, the GLB Act permits the receiving institution to rediscover the information to an entity to whom the original transferring institution could disclose the information pursuant to one of the exceptions in sections 160.14 or 160.15, or to an entity to whom the original transferring institution could have disclosed the information as described

under its notice of privacy policies and practices, unless the consumer has exercised the right to opt out of that disclosure. Because a consumer can exercise the right to opt out of a disclosure at any time, the GLB Act may effectively preclude third parties that receive information to which the opt out right applies from rediscovering the information other than under one of the exceptions in sections 160.14 or 160.15.

Sections 502(b)(2) and 502(e) of the GLB Act describe the circumstances under which a financial institution may disclose nonpublic personal information without providing the consumer with the initial privacy notice and an opportunity to opt out. Those exceptions apply only when the information is used for the specific purposes set forth in those sections which include, for example, disclosure as necessary to effect, administer, or enforce a transaction authorized by the consumer. Paragraph (a)(2) of section 160.11 clarifies this limitation on reuse as it applies to financial institutions by providing that a financial institution may use nonpublic personal information about a consumer that it receives from a nonaffiliated financial institution in accordance with an exception under section 160.14 or 160.15 only for the purpose of that exception. Paragraph (b)(2) applies the same restrictions on reuse to any nonaffiliated third party that received nonpublic personal information from a financial institution. The Commission has determined not to impose a specific duty on financial institutions to monitor third parties' use of nonpublic personal information provided by the institutions.

The definition of nonpublic personal information dictates that all of the information a financial institution provides to a consumer reporting agency is nonpublic personal information. The financial institution is permitted under section 160.15(a)(5) to disclose nonpublic personal information to a consumer reporting agency without giving the consumer notice and the opportunity to opt out. Thus, the traditional consumer reporting business, whereby financial institutions report information about their consumers to the consumer reporting agencies which, in turn, disclose that information in the form of consumer reports to those who have a permissible purpose to obtain them, continues unaffected. This exception, however, does not permit consumer reporting agencies to rediscover the nonpublic personal information it receives from financial institutions other than in the form of a consumer report. Accordingly, the

exception does not operate to permit the disclosure of "credit header information" to individual reference services, direct marketers, or any other party that does not have a permissible purpose to obtain that information as part of a consumer report.⁴²

Section 160.12 Limits on Sharing Account Number Information for Marketing Purposes

Section 502(d) of the GLB Act prohibits a financial institution from disclosing, other than to a consumer reporting agency, account numbers or similar forms of access numbers or access codes for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or marketing through electronic mail to the consumer. Section 160.12 applies this prohibition to disclosures made directly or indirectly as it has been applied by the Agencies, and incorporates the exceptions that have been established by the Agencies.⁴³ Thus, the rule provides for two exceptions. First, it permits an FCM, CTA, CPO or IB to disclose account numbers to an agent for the purposes of marketing the institution's financial products or services so long as the agent has no authority to initiate charges to the account. Second, it permits disclosure in a private-label credit card or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program. As a matter of clarification, the rule also contains an example that provides that an account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.⁴⁴

Subpart C—Exceptions

Section 160.13 Exception to Opt Out Requirements for Service Providers and Joint Marketing

Section 502(b) of the GLB Act creates an exception to the opt out rules for the disclosure of information to a nonaffiliated third party for its use to perform services for, or functions on behalf of, the financial institution,

⁴² Credit header information traditionally has been defined to include identifying information such as name, address, telephone number, social security number, mother's maiden name, and age.

⁴³ See, e.g., 17 CFR 248.12 (SEC privacy rules).

⁴⁴ This approach thus recognizes that the prohibition in section 502(d) of the GLB Act focuses on numbers that provide access to an account. Without a decryption number or code, the consumer's account number cannot be accessed.

including the marketing of the financial institution's own products or services or financial products or services offered under a joint agreement between two or more financial institutions. A consumer will not have the right to opt out of disclosing nonpublic personal information about the consumer to nonaffiliated third parties under these circumstances, if the financial institution satisfies certain requirements.

Before the information may be shared, section 502(b)(2) of the GLB Act requires the institution to (i) "fully disclose" to the consumer that it will provide this information to the nonaffiliated third party and (ii) enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of the information. Paragraph (a) of section 160.13 would implement these provisions of the GLB Act by requiring the FCM, CTA, CPO or IB to (i) provide the initial notice required by section 160.4; and (ii) enter into a contract that prohibits the third party from disclosing or reusing the information other than to carry out the purposes for which the information was disclosed, including use under an exception in sections 160.14 and 160.15 in the ordinary course of business to carry out those purposes. The contract should be designed to ensure that the third party will (a) maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it, and (b) use the information solely for the purposes for which the information is disclosed or as otherwise permitted under the rules.⁴⁵

Section 160.14 Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions

Section 502(e) of the GLB Act creates exceptions to the requirements that apply to the disclosure of nonpublic personal information to nonaffiliated third parties. Paragraph (1) of that section provides certain exceptions for disclosures made in connection with the administration, processing, servicing and sale of a consumer's account. Section 160.14 sets forth those exceptions and also the definition of "necessary to effect, administer, or enforce" contained in section 509(7) of the GLB Act.

⁴⁵ Consistent with the approach taken by the Agencies, the Commission will grandfather existing service agreements. Thus, paragraph (c) of rule 160.18 provides that contracts entered into before the March 31, 2002 compliance date must be brought into compliance with section 160.13 by March 31, 2003.

These exceptions and the exceptions discussed in section 160.15, below, do not affect a financial institution's obligation to provide initial notices of its privacy policies and practices at or prior to the time it establishes a customer relationship and annual notices thereafter. These notices must be provided to all customers, even if the financial institution intends to disclose the nonpublic personal information only under the exceptions in section 160.14.

Section 160.15 Other Exceptions to Notice and Opt Out Requirements

As discussed above, section 502(e) of the GLB Act contains several exceptions to the requirements that otherwise would apply to the disclosures of nonpublic personal information to nonaffiliated third parties. Section 160.15 sets forth the exceptions that are not made in connection with the administration, processing, servicing or sale of a consumer's account. For example, one of the exceptions stated in the rule is for disclosures made with the consent, or at the direction of the consumer, provided the consumer has not revoked the consent.

Subpart D—Relation to Other Laws; Effective Date

Section 160.16 Protection of Fair Credit Reporting Act

Section 506(c) of the GLB Act states that, except for the amendments regarding rulemaking authority, nothing in Title V is to be construed to modify, limit or supersede the operation of the FCRA, and no inference is to be drawn on the basis of the provisions of Title V whether information is transaction or experience information under section 603 of the FCRA. Section 160.16 implements section 506(c) of the GLB Act by restating the GLB Act with clarifying changes.

Section 160.17 Relation to State Laws

Section 507 of the GLB Act provides that Title V does not preempt any state law that provides greater protections than are provided by Title V. Determinations whether a state law or Title V provide greater protections are to be made by the FTC after consultation with the agency that regulates either the party filing a complaint or the financial institution about which the complaint was filed. Determinations of whether state or federal law affords greater protection may be initiated by any interested party or on the FTC's own motion.

Section 160.17 is substantively identical to section 507, noting that the rules (like the GLB Act) do not preempt

state laws that provide greater protection for consumers than do the rules.

Section 160.18 Effective Date; Transition Rule

Section 160.18 establishes an effective date for part 160 of June 21, 2001, which is the date by which the Commission is required to prescribe final rules implementing Title V.⁴⁶ In order to provide financial institutions sufficient time to bring their policies and procedures into compliance with the requirements of the rules, the Commission proposed a compliance date of December 31, 2001. The commenter recommended that the Commission delay compliance for small entities which may not have the staff or resources to quickly develop systems and software, and for whom compliance may be particularly burdensome. The Commission agrees that six months may be insufficient in certain instances for a financial institution, regardless of size, to ensure that its forms, systems and procedures comply with the rule. In order to accommodate situations requiring additional time, and consistent with the approach taken by the other Agencies, the Commission will give financial institutions until March 31, 2002 to be in full compliance with the rule. Financial institutions are expected, however, to begin compliance efforts promptly, to use the period prior to March 30, 2002, to implement and test their systems, and to be in full compliance by March 31, 2002. The Commission is also adopting a provision that phases in compliance with respect to existing service agreements.

Under the final rule, full compliance with the rules' restrictions on disclosures will be required by March 31, 2002. To be in full compliance, FCMs, CTAs, CPOs and IBs will be required to provide their existing customers with a privacy notice, an opt out notice, and a reasonable amount of time to opt out before that date. If these have not been provided, the disclosure restrictions will apply. This means that an FCM, CTA, CPO or IB must cease sharing customers' nonpublic personal information with nonaffiliated third parties on that date, unless it may share the information under an exception under sections 160.14 or 160.15. FCMs, CTAs, CPOs and IBs that both provide the required notices and allow a reasonable period of time to opt out before March 31, 2002, would be able to share nonpublic personal information

⁴⁶ See Section 5g of the CEA, as amended by section 124 of the CFMA.

after that date for customers who do not opt out.

Under the final rule, FCMs, CTAs, CPOs and IBs are not required to give initial notices to customers whose relationships had terminated before the date by which institutions must be in compliance with the rules. Thus, if under a financial institution's policies an account is inactive before March 31, 2002, then no initial notice will be required in connection with that account. However, because these former customers will remain consumers, an FCM, CTA, CPO or IB must provide a privacy and opt out notice to them if the institution intends to disclose their nonpublic personal information to nonaffiliated third parties beyond the exceptions in sections 160.14 and 160.15.

Section 160.30 Procedures to Safeguard Customer Information and Records

Section 501 of the GLB Act directs the Agencies to establish appropriate safeguards for financial institutions relating to administrative, technical and physical safeguards to protect customer records and information. Section 160.30 implements this directive by requiring every FCM, CTA, CPO or IB that is subject to the jurisdiction of the Commission to adopt policies and procedures to address the safeguards described above. Consistent with the GLB Act, the rule further requires that the policies and procedures be reasonably designed to: (i) Insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The Commission believes it is appropriate for each financial institution to tailor its policies and procedures to its own systems of information gathering and transfer and to the needs of its customers and has not prescribed specific policies or procedures that financial institutions must adopt.

IV. Cost-Benefit Analysis

Section 15 of the Act, as amended by section 119 of the CFMA, requires the Commission, before issuing a new regulation under the Act, to consider the costs and benefits of its action. The Commission understands that, by its terms, section 15 does not require the Commission to quantify the costs and

benefits of a new regulation or to determine whether the benefits of the proposed regulation outweigh its costs.

Section 15 further specifies that costs and benefits shall be evaluated in light of five broad areas of market and public concern: (1) Protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. Accordingly, the Commission could in its discretion give greater weight to any one of the five enumerated areas of concern and could in its discretion determine that, notwithstanding its costs, a particular rule was necessary or appropriate to protect the public interest or to effectuate any of the provisions or to accomplish any of the purposes of the Act.

The Commission has solicited comment on its consideration of these costs and benefits.⁴⁷ No comments were received. The Commission has considered the costs and benefits of this rule package in light of the specific areas of concern identified in section 15,⁴⁸ and has endeavored to impose minimal costs on the FCMs, CTAs, CPOs and IBs that would be subject to this rule while ensuring that the benefits of the rule can be fully realized. The Commission notes that the disclosure and reporting requirements of this rule would be minimal for those financial institutions that do not share nonpublic personal information about consumers with nonaffiliated third parties. The Commission further notes that the CFMA specifically mandates that the Commission adopt rules to protect the privacy of consumer financial information in accordance with Title V of the GLB Act. Accordingly, the Commission has determined to adopt part 160 as discussed above.

V. Related Matters

A. Paperwork Reduction Act of 1995

This rule contains information collection requirements. As required by the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.*, the Commission submitted a copy of the proposed rule to the Office of Management and Budget (OMB) for its review. In response to the Commission's invitation in the notice of proposed rulemaking to comment on any potential paperwork burden associated with this regulation, no comments were received from the public.

⁴⁷ *Id.* at 15563.

⁴⁸ *See* 66 FR at 15562–15563.

The final rule contains several disclosure requirements. The financial institutions covered by this regulation must prepare and provide the initial notice to all current customers and all new customers at the time of establishing a customer relationship (section 160.4(a)). Subsequently, an annual notice must be provided to all customers at least once during a twelve-month period during the continuation of the customer relationship (section 160.5(a)). The initial notice and opt out notice must be provided to a consumer prior to disclosing nonpublic personal information to certain nonaffiliated third parties. If a financial institution wishes to disclose information in a way that is inconsistent with the notices previously given to a consumer, the institution must provide consumers with revised notices (section 160.8(c)).

The final rule also contains consumer reporting requirements. In order for consumers to prevent financial institutions from sharing their information with nonaffiliated third parties, they must opt out (sections 160.7(a)(2)(ii), 160.10(a)(2), and 160.10(c)). At any time during their continued relationship with the institution, consumers have the right to change or update their opt out status with the institution (sections 160.7(f) and (g)).

The rule requires the collection of certain information from FCMs, CTAs, CPOs and IBs subject to the Commission's jurisdiction. The Commission may not conduct or sponsor, and a person is not required to respond to an information collection unless it displays a currently valid OMB control number. The Commission is currently requesting a control number for this information collection from OMB.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), 5 U.S.C. 601 *et seq.*, requires that federal agencies, in proposing rules, consider the impact of those rules on small businesses. The rules adopted herein would affect all FCMs, CTAs, CPOs and IBs, including CPOs and CTAs that are exempt from registration requirements. The Commission has previously established certain definitions of "small entities" to be used by the Commission in evaluating the impact of its rules on small entities in accordance with the RFA.⁴⁹ The Commission has previously determined that registered FCMs and registered CPOs are not small entities for the purpose of the RFA.⁵⁰ With

⁴⁹ 47 fr 18618–21 (aPR. 30, 1982).

⁵⁰ *Id.* at 18619–20.

respect to IBs and CTAs, the Commission has stated that it is appropriate to evaluate within the context of a particular rule whether some or all of the affected entities should be considered small entities and, if so, to analyze the economic impact on them of any rule.

The Commission proposed part 160 and requested comments on the rule and related issues in a **Federal Register** release on March 19, 2001.⁵¹ At the time of issuance of the proposed rule, the Commission could not make a determination that part 160 would not have a significant economic impact on a substantial number of small entities, and therefore the Commission provided an Initial Regulatory Flexibility Analysis (IRFA) in accordance with 5 U.S.C. 603 of the RFA. The Commission did not receive any comments specifically addressing the IRFA. Given that the burden imposed on small institutions stems in large part from Title V of the GLB Act, and in light of the substantial flexibility provided in the final rule to allow any financial institution, regardless of size, to tailor its privacy practices to its individual needs, the Commission does not believe that the rule will have a significant economic impact on a substantial number of small entities. Nevertheless, because Title V creates a set of requirements that are new both to the Commission and to FCMs, CTAs, CPOs and IBs in general, the Commission has prepared the following Final Regulatory Flexibility Analysis (FRFA).

1. Need for and Objectives of the Final Rule; Legal Basis for the Rule

Section 5g of the Act makes the Commission a Federal functional regulator for purposes of applying the provisions of Title V, Subtitle A of the GLB Act addressing consumer privacy to any FCM, CTA, CPO or IB that is subject to the Commission's jurisdiction with respect to any financial activity, and directs the Commission to prescribe regulations necessary to implement Title V's provisions within 6 months from the date the CFMA was signed into law (December 21, 2000). In general, Title V requires financial institutions to provide notice to consumers about the institution's privacy policies and practices, restricts the ability of a financial institution to share nonpublic personal information about consumers to nonaffiliated third parties, and permits consumers to prevent the institution from disclosing nonpublic personal information about them to certain nonaffiliated third parties by

"opting out" of that disclosure. Title V also requires the Commission to establish appropriate standards for financial institutions subject to its jurisdiction to safeguard customer information and records.

The Commission believes that by adopting a rule implementing Title V that is consistent with and comparable to those of the Agencies, the Commission will provide the private sector greater certainty on how to comply with the statute and clearer guidance on how the rule will be enforced with respect to financial institutions that are subject to the Commission's jurisdiction.

2. Small Entities to Which the Rule Will Apply

The final rule would apply to all FCMs, CTAs, CPOs and IBs subject to the Commission's jurisdiction, regardless of size, including those with assets of under \$100 million. As noted in the IRFA, neither Title V nor section 5g of the Act provide a general exception for small entities, nor does it appear that such an exception would be consistent with the purposes of the GLB Act. Because the rule would also apply to CTAs and CPOs that are exempt from the Commission's registration requirements, the Commission cannot make a precise estimate of the number of small entities that would be subject to the final rule.

3. Compliance Requirements and Effects of the Final Rule on Small Entities

A detailed description of the final rule's requirements is set forth above in the section-by-section analysis (part III). Among other things, the final rule requires financial institutions, *i.e.*, FCMs, CTAs, CPOs and IBs, to prepare a notice of their privacy practices and policies and provide that notice to consumers under conditions as specified in the rule (*e.g.*, a privacy notice must be provided no later than at the time that a customer relationship is established and then once annually for the duration of that customer relationship). A financial institution that discloses nonpublic personal information about consumers to nonaffiliated third parties will be subject to additional mandates, including a requirement to provide an opt out notice to consumers along with a reasonable opportunity to opt out of certain disclosures. If the institution does not intend to share that information with nonaffiliated third parties, then it need not provide a privacy or opt out notice to the consumer. In addition to the notice and opt out requirements, Title V directs the

Commission to establish appropriate standards for administrative, technical and physical safeguards to protect customer records and information. The rule implements this section by requiring every FCM, CTA, CPO and IB to adopt policies and procedures to address these safeguards.

There are many exceptions to the general requirements stated above. For example, an institution may share a consumer's nonpublic personal information with nonaffiliated third parties without having to give an opt out notice if such sharing is necessary to effect, administer or enforce a transaction requested or authorized by the consumer. These exceptions have the effect of minimizing the burden on institutions of all sizes. In addition, the rules do not specify the means by which institutions may ensure the safety of customer information and records in order to allow each institution to tailor its policies and procedures to its own systems of information gathering and transfer, and the needs of its customers.

To comply with the final rule, financial institutions will need, among other things, to prepare disclosure forms, make various operational changes, and train staff. Professional skills needed to comply with the final rule may include clerical, computer systems, personnel training, as well as legal drafting and advice. Compliance requirements will vary considerably among institutions depending, for example, on an institution's information sharing practices, whether the institution already has or discloses a privacy policy, and whether the institution already has established an opt out mechanism pursuant to the Fair Credit Reporting Act. The Commission did not receive any comments addressing the compliance requirements described in the IRFA.

4. Summary of Significant Issues Raised by the Public Comments; Descriptions of Steps the Commission Has Taken to Minimize Burden

In response to comments received on the proposed rule, the Commission has considered the following alternatives to minimize the economic burden of the rule: (a) An exemption from coverage of the rule, or any part thereof, for unregistered entities; (b) delay of the compliance date; and (c) substituted compliance for dual registrants and affiliated financial institutions.

As discussed above, neither the GLB Act nor section 5g of the CEA provide a general exception for small or unregistered entities. As stated in section 501(a) of the GLB Act, "It is the policy of Congress that *each* financial

⁵¹ 66 FR 15550.

institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." (Emphasis added.) Section 5g of the CEA provides that *any* futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker that is subject to the jurisdiction of the Commission under this Act with respect to any financial activity *shall* be treated as a financial institution for purposes of title V of [the GLB Act] with respect to such financial activity." (Emphasis added.) Accordingly, the rule applies to all FCMs, CTAs, CPOs and IBs, including those that are small entities or are unregistered pursuant to an exemption. The final rule, however, reflects certain changes that should increase flexibility and lower costs for those entities.

First, the Commission has extended the compliance date of the rule from December 31, 2001 to March 31, 2002. Similarly, the Commission has extended the compliance date with respect to existing service agreements to March 31, 2003. The Commission expects that delaying compliance for an additional 90 days will lessen the burden of the rule on small entities because they will have additional time to budget for any necessary expenses and to implement all necessary operational changes required to comply with this rule.

Second, the Commission has expanded its substituted compliance proposal to permit commodity trading advisors that are registered or required to be registered as an investment advisor with a state securities regulator to comply with this rule by complying with the privacy rule issued by the Federal Trade Commission. This minimizes any potential regulatory overlap that these entities otherwise might have faced.

Finally, the final rule, like the proposed rule, provides for performance rather than design standards. The rule does not specify the form of privacy notices or the method of delivery of the notices to customers and consumers. Similarly, the rule does not specify the policies and procedures that FCMs, CTAs, CPOs and IBs must adopt to ensure the privacy of the financial information and records of their customers and consumers. The Commission has also included non-exclusive examples of conduct throughout the final rule that illustrate ways to comply with particular provisions. Accordingly, the rule provides substantial flexibility so that FCMs, CTAs, CPOs and IBs may meet

the requirements of part 160 in a way that best suits the institution's individual needs.

List of Subjects in 17 CFR Part 160

Brokers, Consumer protection, Privacy, Reporting and recordkeeping requirements.

Text of Final Rules

For the reasons articulated in the preamble, the Commission amends Title 17 of the Code of Federal Regulations by adding a new Part 160 to read as follows:

PART 160—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

- 160.1 Purpose and scope.
- 160.2 Rule of construction.
- 160.3 Definitions.

Subpart A—Privacy and Opt Out Notices

- 160.4 Initial privacy notice to consumers required.
- 160.5 Annual privacy notice to customers required.
- 160.6 Information to be included in privacy notices.
- 160.7 Form of opt out notice to consumers; opt out methods.
- 160.8 Revised privacy notices.
- 160.9 Delivering privacy and opt out notices.

Subpart B—Limits on Disclosures

- 160.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.
- 160.11 Limits on redisclosure and re-use of information.
- 160.12 Limits on sharing account number information for marketing purposes.

Subpart C—Exceptions

- 160.13 Exception to opt out requirements for service providers and joint marketing.
- 160.14 Exceptions to notice and opt out requirements for processing and servicing transactions.
- 160.15 Other exceptions to notice and opt out requirements.

Subpart D—Relation to Other Laws; Effective Date

- 160.16 Protection of Fair Credit Reporting Act.
- 160.17 Relation to state laws.
- 160.18 Effective date; transition rule.
- 160.19–160.29 [Reserved]
- 160.30 Procedures to safeguard customer records and information.

Appendix to Part 160—Sample Clauses

Authority: 7 U.S.C. 7b–2 and 12a(5); 15 U.S.C. 6801 *et seq.*

§ 160.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing nonpublic personal information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§ 160.13, 160.14, and 160.15.

(b) *Scope.* This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services primarily for business, commercial, or agricultural purposes. This part applies to all futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers that are subject to the jurisdiction of the Commission, regardless whether they are required to register with the Commission. These entities are hereinafter referred to in this part as "you." This part does not apply to foreign (non-resident) futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers that are not registered with the Commission. Nothing in this part modifies, limits or supercedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d–1320d–8.

§ 160.2 Rule of construction.

(a) *Safe harbor.* The examples in this part and the sample clauses in the Appendix to this part are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part.

(b) *Substituted compliance.* (1) Any person or entity otherwise subject to this part that is subject to and in compliance with Securities and Exchange Commission Regulation S–P, 17 CFR part 248, will be deemed to be in compliance with this part.

(2) Any commodity trading advisor otherwise subject to this part that is registered or required to be registered as an investment adviser in the state in

which it maintains its principal office and place of business as defined in § 275.203A-3 of this title, and that is subject to and in compliance with 16 CFR part 313, will be deemed to be in compliance with this part.

§ 160.3 Definitions.

For purposes of this part, unless the context requires otherwise:

(a) *Affiliate* of a futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker means any company that controls, is controlled by, or is under common control with a futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker that is subject to the jurisdiction of the Commission. In addition, a futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker subject to the jurisdiction of the Commission will be deemed an affiliate of a company for purposes of this part if:

(1) That company is regulated under Title V of the GLB Act by the Federal Trade Commission or by a federal functional regulator other than the Commission; and

(2) Rules adopted by the Federal Trade Commission or another federal functional regulator under Title V of the GLB Act treat the futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker as an affiliate of that company.

(b)(1) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) *Examples*—(i) *Reasonably understandable*. Your notice will be reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) *Designed to call attention*. Your notice is designed to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) Use distinctive type size, style and graphic devices, such as shading or sidebars when you combine your notice with other information.

(iii) *Notices on web sites*. If you provide notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page, if necessary to view the entire notice, and ensure that other elements on the web site, such as text, graphics, hyperlinks or sound, do not distract from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) *Collect* means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d) *Commission* means the Commodity Futures Trading Commission.

(e) *Commodity pool operator* has the same meaning as in section 1a(5) of the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(f) *Commodity trading advisor* has the same meaning as in section 1a(6) of the Commodity Exchange Act, as amended, and includes anyone registered as such under the Act.

(g) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association or similar organization.

(h)(1) *Consumer* means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family or household purposes, or that individual's legal representative.

(2) *Examples*. (i) An individual is your consumer if he or she provides nonpublic personal information to you in connection with obtaining or seeking to obtain brokerage or advisory services, whether or not you provide services to the individual or establish a continuing relationship with the individual.

(ii) An individual is not your consumer if he or she provides you only with his or her name, address and general areas of investment interest in connection with a request for a brochure or other information about financial products or services.

(iii) An individual is not your consumer if he or she has an account with another futures commission merchant (originating futures commission merchant) for which you provide clearing services for an account in the name of the originating futures commission merchant.

(iv) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(v) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vi) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(vii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(i) *Consumer reporting agency* has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(j) Control of a company means the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. Any person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of any company is presumed to control the company. Any person who does not own more than 25 percent of the voting securities of a company will be presumed not to control the company.

(k) *Customer* means a consumer who has a customer relationship with you.

(l)(1) *Customer relationship* means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family or household purposes.

(2) *Examples*—(i) *Continuing relationship*. A consumer has a continuing relationship with you if:

(A) You are a futures commission merchant through whom a consumer has opened an account, or that carries the consumer's account on a fully-disclosed basis, or that effects or engages in commodity interest

transactions with or for a consumer, even if you do not hold any assets of the consumer.

(B) You are an introducing broker that solicits or accepts specific orders for trades;

(C) You are a commodity trading advisor with whom a consumer has a contract or subscription, either written or oral, regardless of whether the advice is standardized, or is based on, or tailored to, the commodity interest or cash market positions or other circumstances or characteristics of the particular consumer;

(D) You are a commodity pool operator, and you accept or receive from the consumer, funds, securities, or property for the purpose of purchasing an interest in a commodity pool;

(E) You hold securities or other assets as collateral for a loan made to the consumer, even if you did not make the loan or do not effect any transactions on behalf of the consumer; or

(F) You regularly effect or engage in commodity interest transactions with or for a consumer even if you do not hold any assets of the consumer.

(ii) *No continuing relationship.* A consumer does not have a continuing relationship with you if:

(A) You have acted solely as a "finder" for a futures commission merchant, and you do not solicit or accept specific orders for trades; or

(B) You have solicited the consumer to participate in a pool or to direct his or her account and he or she has not provided you with funds to participate in a pool or entered into any agreement for you to direct his or her account.

(m) *Federal functional regulator means:*

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board;

(6) The Securities and Exchange Commission; and

(7) The Commodity Futures Trading Commission.

(n)(1) *Financial institution means:*

(i) Any futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker that is registered with the Commission as such or is otherwise subject to the Commission's jurisdiction; and

(ii) Any other institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k).

(2) *Financial institution* does not include:

(i) Any person or entity, other than a futures commission merchant, commodity trading advisor, commodity pool operator or introducing broker that, with respect to any financial activity, is subject to the jurisdiction of the Commission under the Act.

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

(o)(1) *Financial product or service means:*

(i) Any product or service that a futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker could offer that is subject to the Commission's jurisdiction; and

(ii) Any product or service that any other financial institution could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k).

(2) *Financial service* includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(p) *Futures commission merchant* has the same meaning as in section 1a(20) of the Commodity Exchange Act, as amended, and includes any person registered as such under the Act.

(q) *GLB Act* means the Gramm-Leach-Bliley Act (Pub. L. No. 106-102, 113 Stat. 1338 (1999)).

(r) *Introducing broker* has the same meaning as in section 1a(23) of the Commodity Exchange Act, as amended, and includes any person registered as such under the Act.

(s)(1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your affiliate, but *nonaffiliated third party* includes the other company that jointly employs the person.

(2) *Nonaffiliated third party* includes any company that is an affiliate solely by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant

banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k)(4)(H) and (I).

(t)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description or other grouping of consumers, and publicly available information pertaining to them, that is derived using any personally identifiable financial information that is not publicly available information.

(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as included on a list described in paragraph (t)(1)(ii) of this section or when the publicly available information is disclosed in a manner that indicates the individual is or has been your consumer; or

(ii) Any list, description or other grouping of consumers, and publicly available information pertaining to them, that is derived without using any personally identifiable financial information that is not publicly available information.

(3) *Examples of lists.* (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available information, such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available information, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(u)(1) *Personally identifiable financial information* means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples.*—(i) *Information included.* Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to open a commodity trading account, invest in a commodity pool, or to obtain another financial product or service;

(B) Account balance information, payment history, overdraft history, margin call history, trading history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information you collect through an Internet "cookie" (an information-collecting device from a web server); and

(F) Information from a consumer report.

(ii) *Information not included.* Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; or

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

(v)(1) *Publicly available information* means any information that you reasonably believe is lawfully made available to the general public from:

(i) Federal, state or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by federal, state or local law.

(2) *Examples.*—(i) *Reasonable belief.*

(A) You have a reasonable belief that information about your consumer is made available to the general public if you have confirmed, or your consumer has represented to you, that the information is publicly available from a source described in paragraphs (v)(1)(i)–(iii) of this section.

(B) You have a reasonable belief that information about your consumer is made available to the general public if you have taken steps to submit the information, in accordance with your internal procedures and policies and with applicable law, to a keeper of federal, state or local government records that is required by law to make the information publicly available.

(C) You have a reasonable belief that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or on an

internet listing service, or the consumer has informed you that the telephone number is not unlisted.

(D) You do not have a reasonable belief that information about a consumer is publicly available solely because that information would normally be recorded with a keeper of federal, state or local government records that is required by law to make the information publicly available, if the consumer has the ability in accordance with applicable law to keep that information nonpublic, such as where a consumer may record a deed in the name of a blind trust.

(ii) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings.

(iii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or password, so long as access is available to the general public.

(w) *You* means:

(1) Any futures commission merchant;

(2) Any commodity trading advisor;

(3) Any commodity pool operator; and

(4) Any introducing broker subject to the jurisdiction of the Commission.

Subpart A—Privacy and Opt Out Notices

§ 160.4 Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 160.14 and 160.15.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a) of this section if:

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party other than as authorized by §§ 160.14 and 160.15; and

(2) You do not have a customer relationship with the consumer.

(c) *When you establish a customer relationship.*

(1) *General rule.* You establish a customer relationship when you and the consumer enter into a continuing relationship.

(2) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(i) Instructs you to execute a commodity interest transaction for the consumer;

(ii) Opens a commodity interest account through an introducing broker or with a futures commission merchant that clears transactions for its customers through you on a fully-disclosed basis;

(iii) Transmits specific orders for commodity interest transactions to you that you pass on to a futures commission merchant for execution, if you are an introducing broker;

(iv) Enters into an advisory contract or subscription with you, whether in writing or orally, and whether you provide standardized, or individually tailored commodity trading advice based on the customer's commodity interest or cash market positions or other circumstances or characteristics, if you are a commodity trading adviser; or

(v) Provides to you funds, securities, or property for an interest in a commodity pool, if you are a commodity pool operator.

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice under § 160.8 that covers the customer's new financial product or service; or

(2) If the initial, revised or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(e) *Exceptions to allow subsequent delivery of notice.* (1) You may provide the initial notice required by paragraph (a)(1) of this section within a reasonable time after you establish a customer relationship if:

(i) Establishing the customer relationship is not at the customer's election;

(ii) Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction and the

customer agrees to receive the notice at a later time;

(iii) A nonaffiliated financial institution establishes a customer relationship between you and a consumer without your prior knowledge; or

(iv) You have established a customer relationship with a customer in a bulk transfer in accordance with § 1.65, if you are a transferee futures commission merchant or introducing broker.

(2) *Examples of exceptions.*—(i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if you acquire the customer's commodity interest account from another financial institution and the customer does not have a choice about your acquisition.

(ii) *Substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction when you and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service.

(iii) *No substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at your office or through other means by which the customer may view the notice, such as on a web site.

(f) *Delivery of notice.* When you are required by this section to deliver an initial privacy notice, you must deliver it according to the provisions of § 160.9. If you use a short-form initial notice for non-customers according to § 160.6(d), you may deliver your privacy notice as provided in section § 160.6(d)(3).

§ 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, you are required to state only that you make disclosures to other nonaffiliated parties 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 nonaffiliated 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) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in the Appendix of this part.

§ 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 nonaffiliated 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 through a specific means, as long as that means is reasonable for the consumer.

(b) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form, as the initial notice you provide in accordance with § 160.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice after the initial notice in accordance with § 160.4, you 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 you, you may provide a single opt out notice; however, you must honor a request from one or more joint account holders for a separate opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer.

(2) Any of the joint consumers may exercise the right to opt out. You 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 you permit each joint consumer to opt out separately, you must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) You may not require all joint consumers to opt out before you implement any opt out direction.

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

(i) Send a single opt out notice to John's address, but you 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 you do so, and John opts out, you may not require Mary to opt out as well before implementing John's opt out direction; or

(iii) Permit John and Mary to make different opt out directions. If you do so:

(A) You must permit John and Mary to opt out for each other.

(B) If both opt out, you must permit both to notify you in a single response (such as on a form or through a telephone call).

(C) If John opts out and Mary does not, you may only disclose nonpublic personal information about Mary, but not about John, and not about John and Mary jointly.

(e) *Time to comply with opt out.* You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive 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, either by hard copy or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that you collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with you, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When you are required by this section to deliver an opt out notice, you must deliver it according to § 160.9.

§ 160.8 Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated

third party other than as described in the initial notice that you provided to that consumer under § 160.4, unless:

(1) You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;

(2) You have provided to the consumer a new opt out notice;

(3) You have given the consumer a reasonable opportunity, before you disclose 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 §§ 160.13, 160.14, and 160.15, you must provide a revised notice before you:

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

(ii) Disclose 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 you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice.

(c) *Delivery.* When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 160.9.

§ 160.9 Delivering privacy and opt out notices.

(a) *How to provide notices.* You 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 either in hard copy or, if the consumer agrees, electronically.

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

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

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

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

(2) *Examples of unreasonable expectation of actual notice.* You may

not, however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(i) Only post a sign in your branch or office or generally publish advertisements of your privacy policies and practices; or

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

(c) *Annual notices only.* You may reasonably expect that a consumer will receive actual notice of your annual privacy notice if:

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

(2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

(d) *Oral description of notice insufficient.* You may not provide any notice required by this part solely by orally explaining the notice, either in person or over the telephone.

(e) *Retention or accessibility of notices for customers.*

(1) For customers only, you must provide the initial notice required by § 160.4(a)(1), the annual notice required by § 160.5(a), and the revised notice required by § 160.8, so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) *Examples of retention or accessibility.* You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:

(i) Hand-deliver a printed copy of the notice to the customer;

(ii) Mail a printed copy of the notice to the last known address of the customer; or

(iii) Make your current privacy notice available on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the web site.

(f) *Joint notice with other financial institutions.* You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.

(g) *Joint relationships.* If two or more customers jointly obtain a financial

product or service from you, you may satisfy the initial, annual, and revised notice requirements of paragraph (a) of this section by providing one notice to those customers jointly; however, you must honor a request by one or more joint account holders for a separate notice.

Subpart B—Limits on Disclosures

§ 160.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.

(a)(1) *Conditions for disclosure.*

Except as otherwise authorized in this part, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

- (i) You have provided to the consumer an initial notice as required under § 160.4;
- (ii) You have provided to the consumer an opt out notice as required in § 160.7;
- (iii) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt of the disclosure; and
- (iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 160.13, 160.14 and 160.15.

(3) *Examples of reasonable opportunity to opt out.* You provide a consumer with a reasonable opportunity to opt out if:

(i) *By mail.* You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days after the date you mailed the notices.

(ii) *By electronic means.* A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(iii) *Isolated transaction with consumer.* For an isolated transaction with a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction,

whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information.*

(1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship.

(2) Unless you comply with this section, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you have collected it before or after receiving the direction to opt out from the consumer.

(c) *Partial opt out.* You may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

§ 160.11 Limits on redisclosure and reuse of information.

(a) (1) *Information you receive under an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in §§ 160.14 or 160.15, your disclosure and use of that information is limited as follows:

(i) You may disclose the information to the affiliate of the financial institution from which you received the information;

(ii) You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and

(iii) You may disclose and use the information pursuant to an exception in § 160.14 or 160.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account-processing services under the exception in § 160.14(a), you may disclose that information under any exception in §§ 160.14 or 160.15 in the ordinary course of business in order to provide those services. For example, you could disclose that information in response to a properly authorized subpoena or in the ordinary course of business to your attorneys, accountants, and auditors. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

(b)(1) *Information you receive outside of an exception.* If you receive nonpublic personal information from a

nonaffiliated financial institution other than under an exception in §§ 160.14 or 160.15, you may disclose the information only:

(i) To the affiliates of the financial institution from which you received the information;

(ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

(2) *Example.* If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in §§ 160.14 and 160.15:

(i) You may use that list for your own purposes;

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed that list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in §§ 160.14 and 160.15, such as in the ordinary course of business to your attorneys, accountants, or auditors.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in §§ 160.14 or 160.15, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to your affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in §§ 160.14 or 160.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information you disclose outside of an exception.* If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in §§ 160.14 or 160.15, the third party may disclose the information only:

(1) To your affiliates;

(2) To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if you made it directly to that person.

§ 160.12 Limits on sharing account number information for marketing purposes.

(a) *General prohibition on disclosure of account numbers.* You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's credit card account, deposit account or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

(b) *Exceptions.* Paragraph (a) of this section does not apply if you disclose an account number or similar form of access number or access code:

(1) To your agent or service provider solely in order to perform marketing for your own services or products, as long as the agent or service provider is not authorized to directly initiate charges to the account; or

(2) To a participant in a private-label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(c) *Example.* An account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.

Subpart C—Exceptions

§ 160.13 Exception to opt out requirements for service providers and joint marketing.

(a) *General rule.* (1) The opt out requirements in §§ 160.7 and 160.10 do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf if you:

(i) Provide the initial notice in accordance with § 160.4; and

(ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in §§ 160.14 or 160.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If you disclose nonpublic personal information under

this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in §§ 160.14 or 160.15 in the ordinary course of business to carry out that joint marketing.

(b) *Service may include joint marketing.* The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

(c) *Definition of joint agreement.* For purposes of this section, *joint agreement* means a written contract pursuant to which you and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

§ 160.14 Exceptions to notice and opt out requirements for processing and servicing transactions.

(a) *Exceptions for processing and servicing transactions at consumer's request.* The requirements for initial notice in § 160.4(a)(2), for the opt out in §§ 160.7 and 160.10, and for initial notice in § 160.13 in connection with service providers and joint marketing, do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Processing or servicing a financial product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with you, or with another entity as part of an extension of credit on behalf of such entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(3) A proposed or actual securitization, secondary market sale or similar transaction related to a transaction of the consumer.

(b) *Necessary to effect, administer or enforce a transaction* means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the financial service or financial product;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;

(v) In connection with:

(A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(B) The transfer of receivables, accounts or interests therein; or

(C) The audit of debit, credit or other payment information.

§ 160.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to notice and opt out requirements.* The requirements for initial notice in § 160.4(a)(2), for the opt out in §§ 160.7 and 160.10, and for initial notice in § 160.13 in connection with service providers and joint marketing do not apply when you disclose nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2)(i) To protect the confidentiality or security or your records pertaining to the consumer, service, product or transaction;

(ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with

industry standards, and your attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 *et seq.*, to law enforcement agencies (including a federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a State insurance authority, with respect to any person domiciled in that insurance authority's state that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)(i) To a consumer reporting agency in accordance with the Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*; or

(ii) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(7)(i) To comply with federal, state or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance or other purposes as authorized by law.

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated mortgage lender of the value of the assets in the customer's account so that the lender can evaluate the consumer's application for a mortgage loan.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 160.7(f).

Subpart D—Relation To Other Laws; Effective Date

§ 160.16 Protection of Fair Credit Reporting Act.

Nothing in this part shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*,

and no inference shall be drawn on the basis of the provisions of this part regarding whether information is transaction or experience information under section 603 of that Act.

§ 160.17 Relation to state laws.

(a) *In general.* This part shall not be construed as superseding, altering or affecting any statute, regulation, order or interpretation in effect in any state, except to the extent that such state statute, regulation, order or interpretation is inconsistent with the provisions of this part, and then only to the extent of the inconsistency.

(b) *Greater protection under state law.* For purposes of this section, a state statute, regulation, order or interpretation is not inconsistent with the provisions of this part if the protection such statute, regulation, order or interpretation affords any consumer is greater than the protection provided under this part, as determined by the Federal Trade Commission, after consultation with the Commission, on the Federal Trade Commission's own motion, or upon the petition of any interested party.

§ 160.18 Effective date; compliance date; transition rule.

(a) *Effective date.* This part is effective on June 21, 2001. In order to provide sufficient time for you to establish policies and systems to comply with the requirements for this part, the compliance date for this part is June 21, 2002.

(b)(1) *Notice requirement for consumers who are your customers on the effective date.* By March 31, 2002, you must have provided an initial notice, as required by § 160.4, to consumers who are your customers on June 21, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on March 31, 2002 if, by that date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *One-year grandfathering of service agreements.* Until March 31, 2003, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 160.13(a)(1)(ii) even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the agreement on or before March 31, 2002.

§§ 160.19–160.29 [Reserved]

§ 160.30 Procedures to safeguard customer records and information.

Every futures commission merchant, commodity trading advisor, commodity pool operator and introducing broker subject to the jurisdiction of the Commission must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:

(a) Insure the security and confidentiality of customer records and information;

(b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Appendix to Part 160—Sample Clauses

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

A-1—Categories of Information You Collect (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 160.6(a)(1) to describe the categories of nonpublic personal information you collect.

Sample Clause A-1

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates or others; and
- Information we receive from a consumer reporting agency.

A-2—Categories of Information You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use one of these clauses, as applicable, to meet the requirement of § 160.6(a)(2) to describe the categories of nonpublic personal information you disclose. You may use these clauses if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 160.13, 160.14 and 160.15.

Sample Clause A-2, Alternative 1

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as "your name, address, social security number, assets and income"*];
- Information about your transactions with us, our affiliates or others, such as [*provide illustrative examples, such as "your account balance, payment history, parties to transactions and credit card usage"*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as "your creditworthiness and credit history"*].

Sample Clause A-2, Alternative 2

We may disclose all of the information that we collect, as described [*describe location in the notice, such as "above" or "below"*].

A-3—Categories of Information You Disclose and Parties to Whom You Disclose (Institutions That Do Not Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirements of §§ 160.6(a)(2), (3) and (4) to describe the categories of nonpublic personal information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose. You may use this clause if you do not disclose nonpublic personal information to any party, other than as is permitted by the exceptions in §§ 160.14 and 160.15.

Sample Clause A-3

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4—Categories of Parties to Whom You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 160.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 160.13, 160.14 and 160.15, as well as when permitted by the exceptions in §§ 160.14 and 160.15.

Sample Clause A-4

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [*provide illustrative examples, such as "mortgage bankers"*];
- Non-financial companies, such as [*provide illustrative examples, such as "retailers, direct marketers, airlines and publishers"*]; and
- Others, such as [*provide illustrative examples, such as "non-profit organizations"*].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5—Service Provider/Joint Marketing Exception

You may use one of these clauses, as applicable, to meet the requirements of § 160.6(a)(5) related to the exception for service providers and joint marketers in § 160.13. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A-5, Alternative 1

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as "your name, address, social security number, assets and income"*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as "your account balance, payment history, parties to transactions and credit card usage"*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as "your creditworthiness and credit history"*].

Sample Clause A-5, Alternative 2

We may disclose all of the information we collect, as described [*describe location in the notice, such as "above" or "below"*] to companies that perform marketing services on our behalf or to other financial

institutions with which we have joint marketing agreements.

A-6—Explanation of Opt Out Right (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 160.6(a)(6) to provide an explanation of the consumer's right 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. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 160.13, 160.14 and 160.15.

Sample Clause A-6

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties you may opt out of those disclosures; that is, you may direct us not to make those disclosures (other than disclosures permitted or required by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [*describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)"*].

A-7—Confidentiality and Security (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 160.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7

We restrict access to nonpublic personal information about you to [*provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"*]. We maintain physical, electronic and procedural safeguards that comply with federal standards to safeguard your nonpublic personal information.

Dated: April 20, 2001.

By the Commission.

Catherine D. Dixon,
Assistant Secretary.

[FR Doc. 01-10398 Filed 4-26-01; 8:45 am]

BILLING CODE 6351-01-U