

Securities Law Developments

NEWSLETTER

MARCH 20, 2002

THE CFTC'S PRIVACY RULES

Last April, the Commodity Futures Trading Commission ("CFTC") issued its final rules regarding the obligation of futures commission merchants, commodity trading advisors, commodity pool operators, and introducing brokers to protect the financial privacy of their consumers.¹ The new rules ("part 160")² implement the privacy requirements of the Gramm-Leach-Bliley Act ("GLBA")³ as amended by the Commodity Futures Modernization Act ("CFMA").⁴ Part 160 is substantially similar to regulations adopted by the Securities and Exchange Com-

mission ("SEC") and the Federal Trade Commission ("FTC").⁵

The mandatory compliance date for part 160 (*i.e.*, the end of March) is fast approaching. Commodities and futures firms should, by now, be making substantial progress towards developing the systems, policies and procedures to comply with the new rules and should have sent out, or be prepared to send out shortly, the notices to their clients required by the rule. For reference, the key provisions of part 160 are summarized briefly below.

¹ *Privacy of Consumer Financial Information*, 66 Fed. Reg. 21,236 (April 27, 2001).

² *See* 17 C.F.R. §§ 160.1-160.30.

³ Pub. L. No. 106-102, 113 Stat. 1338 (1999). The GLBA has been codified in scattered sections of 12 U.S.C. and 15 U.S.C., with the privacy provisions of Title V of the act located at 15 U.S.C. §§ 6801-6809.

⁴ Pub. L. No. 106-554, 114 Stat. 2763 (2000). Prior to the enactment of the CFMA, the CFTC and entities subject to its jurisdiction were excluded from the privacy provisions of Title V of the GLBA. The federal regulatory agencies that were originally covered by Title V – the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Secretary of the Treasury, the National Credit Union Administration, the FTC, and the SEC – have each previously adopted analogous privacy regulations, which have all become effective.

⁵ Indeed, Section 160.2(b)(1) of the CFTC's rules provides that entities subject to its jurisdiction that are also registered with the SEC and have complied with the provisions of the SEC's privacy rules, Regulation S-P (17 C.F.R. § 248), may substitute such compliance for compliance with part 160. Likewise, the SEC amended Section 248.2 of Regulation S-P to provide that security futures product broker-dealers subject to and in compliance with part 160 will also be in compliance with Regulation S-P. *See* Exchange Act Release No. 44,730 (Aug. 21, 2001). Similarly, Section 160.2(b)(2) provides that a commodity trading advisor that is a state registered investment adviser (but not registered with the SEC) may comply with part 160 by substituting compliance with the FTC's privacy rules (16 C.F.R. § 313). For more information on the SEC's Regulation S-P, *see* SEC Adopts Final Privacy Rule, *available at* http://www.wilmer.com/docs/news_items/SecNews71300.pdf.

WILMER, CUTLER & PICKERING

Who is subject to these rules?

All domestic or resident futures commission merchants (“FCMs”), commodity pool operators (“CPOs”),⁶ commodity trading advisors (“CTAs”), and introducing brokers (“IBs”) whether or not registered with the CFTC are subject to part 160. All foreign or non-resident FCMs, CPOs, CTAs, and IBs that *are* registered or required to be registered with the CFTC are also subject to part 160. For purposes of this newsletter, FCMs, CPOs, CTAs, and IBs subject to part 160 will be referred to collectively as “covered firms.”

What does part 160 require covered firms to do?

Covered firms must do three main things:

1. **Notice.** Provide a “clear and conspicuous” notice regarding the firm’s privacy policies and practices and describing the conditions under which the firm may disclose “nonpublic personal information” about its consumers to affiliates and to nonaffiliated third parties.
2. **Opt Out.** Provide a method for consumers to “opt out” of the disclosure of nonpublic personal information to third parties.
3. **Safeguarding Policies and Procedures.** Adopt policies and procedures reasonably designed to protect customer records and information from any anticipated threats, hazards, or unauthorized access or use that could result in “substantial harm or inconvenience” to any customer.

Which clients of a covered firm are covered?

The CFTC’s rules require a covered firm to protect information about its “consumers” and “customers.” The distinction between consumer and customer determines the type and timing of notices that need to be provided.

⁶ To avoid jurisdictional confusion, the CFTC has issued an interpretation that CPOs that operate hedge funds are subject to the CFTC’s privacy rules (rather than the privacy rules of the FTC). See CFTC Letter No. 01-48 (May 31, 2001), available at <http://www.cftc.gov/tm/letters/01letters/tm01-48.htm>.

⁷ The CFTC has stressed that institutional investors, such as pension funds, are not individuals investing for personal, family, or household purposes, and, therefore, do not fit within the definition of “consumer” in Section 160.3(h)(1). See CFTC Letter No. 01-70 (July 6, 2001), available at <http://www.cftc.gov/tm/letters/01letters/tm0-70.htm>.

1. **Consumers** are individuals (or their legal representatives) who obtain a financial product or service primarily for personal, family, or household purposes. The rules clarify that a consumer includes an individual who provides nonpublic personal information when seeking to obtain commodity interest trading or advisory services, even if the person does not open a trading account or enter into an advisory contract with the covered firm.
2. **Customers** are those consumers who have a *continuing relationship* with the covered firm. In general, the CFTC requires that there be more than an isolated transaction to establish such a continuing relationship, but a single transaction may suffice if it establishes a reasonable expectation of continued service or further transactions. For example, buying a futures or options contract through an FCM with whom a customer opens an account establishes a customer relationship because of the continuing nature of the service. An individual who engages in a transaction and is unlikely to expect future communication about that transaction from the covered firm would not, however, be a customer of that firm. The rules provide an example: An IB that merely refers an individual to an FCM would not have a customer relationship with that individual if the IB does not enter orders for such individual.

Note: Part 160 does not apply to a covered firm’s *business* or *institutional* customers.⁷

What information is protected?

Part 160 only protects “**nonpublic personal information**,” which is a key definition that generally includes two types of information: (1) “personally identifiable financial information” and (2) any list, descrip-

tion, or grouping of consumers that is derived from such nonpublic personally identifiable financial information.

1. **Personally identifiable financial information**, in turn, is defined to include three types of information:

- **Supplied by Consumer.** Any information provided by a consumer to a covered firm in order to obtain a financial product or service, including, *e.g.*, material that a consumer supplies on an application to open a commodity trading account.
- **Resulting from Transactions.** Any information that results from a transaction with the consumer involving a financial product or service. This category includes information about account balances, trading history, overdraft history, margin call history, or simply that an individual is or was a firm's customer.
- **Obtained in Providing Products or Services.** Any information otherwise obtained by a covered firm in connection with providing a product or service to the consumer. This includes information from a consumer report or other outside source used to verify information on a consumer. This also includes information collected through Internet "cookies."

Note: Personally identifiable financial information does not include *aggregated or blind data* that lacks personal identifiers (such as account numbers, names, or addresses).

2. **Publicly available information**, however, is generally excluded from the definition of nonpublic personal information.⁸ Publicly available information means information that the covered firm "reasonably believes" is lawfully available to members of the public from three sources:

- **Official Public Records**, such as real estate recordations or security interest filings;
- **Widely Distributed Media**, including information obtained over the Internet if it is obtainable from a public site available on an unrestricted basis (an Internet site is not considered restricted merely because it requires a fee or password); and
- **Required Disclosures**, such as information that is required to be disclosed to the general public by federal, state, or local law.

When must a covered firm disclose its privacy policy?

The rules require a covered firm to provide *clear and conspicuous* notices that accurately reflect its privacy policies and practices. The CFTC provides that notices are *clear and conspicuous* if they are "reasonably understandable and designed to call attention to the nature and significance of the information in the notice." The CFTC has included several examples in the rules to illustrate how to make the required notices clear and conspicuous and has stated that the privacy disclosures may be combined with other required disclosures in a single document.⁹

⁸ It is important to note that "nonpublic personal information" *does* include any list, description or other grouping of consumers, *and* publicly available information pertaining to them, that is derived in whole or in part from personally identifiable financial information that is not publicly available information. See Section 160.3(t)(1)(ii).

⁹ The CFTC, along with the other federal agencies that promulgated privacy rules under Title V of the GLBA, co-hosted a public workshop to discuss strategies for providing effective financial privacy notices last December. The materials used at the workshop, which may prove useful in drafting notices, are available through the FTC's Web site at <http://www.ftc.gov/bcp/workshops/glb/index.html>.

The timing of a notice depends on whether a consumer becomes a customer.

1. **To a Consumer.** For a consumer who never becomes a customer, a covered firm is *not* required to provide any notice *unless* the firm decides to disclose *nonpublic personal information* about that consumer to a nonaffiliated third party. This is a key point: Despite the breadth of the definition of consumer, a covered firm can avoid all of the rules' disclosure requirements for its non-customer consumers so long as the firm does *not* share information about its consumers with nonaffiliated third parties.

2. **To a Customer.**

a. **Initial Notice.** For a customer, an *initial privacy notice* generally should be provided *no* later than the time of establishing the customer relationship. Covered firms may, however, provide notices within a "reasonable" time *after* establishing an account relationship in certain limited circumstances: (1) if the customer has not elected to establish an account relationship, (2) when to do otherwise would substantially delay the transaction and the consumer agrees to receive the notice at a later time, or (3) when a non-affiliated financial institution establishes an account on behalf of a customer without a covered firm's prior knowledge.

b. **Annual Notice.** For a customer, a covered firm also must provide *annual privacy notices* during the continuation of the customer relationship. The annual notice must, once again, "clearly and conspicuously" disclose the current privacy policies and practices of the firm.

3. **Notice to an Existing Customer.** When an existing customer obtains a new financial prod-

uct or service, no new notice is required so long as the most recently provided notice was accurate with respect to the new product or service.

How must a covered firm provide its initial and annual notices?

The notices must be provided *in writing* or, if the consumer agrees, in electronic form. Notices should be provided in a manner that allows customers to retain or obtain them at a later date. Oral notices are insufficient.

Part 160 permits a single notice to be provided to multiple customers who jointly obtain a financial product or service, *e.g.*, joint accountholders. A covered firm also has the discretion to provide separate notices to each accountholder. Part 160 also allows two or more institutions to provide *joint* notices, as long as they are delivered in accordance with the rules and are accurate for all recipients. This provision also may be helpful for affiliated firms that are part of the same holding company.

What must be included in initial and annual privacy notices?

A covered firm must provide the following information in both the initial and annual privacy notices (if applicable):

- **Collected Information.** The categories of *nonpublic personal information* about consumers that the firm collects.
- **Disclosed Information.** The categories of *nonpublic personal information* about consumers that the firm may disclose.
- **With Whom is Information Shared.** The categories of affiliates¹⁰ and nonaffiliated third parties to whom the firm discloses *nonpublic personal information*.

¹⁰ An "affiliate" of a covered firm is defined as any company that controls, is controlled by, or is under common control with that covered firm. The rules also provide that a covered firm is an affiliate of another company for purposes of the privacy rules if: (i) the other company is subject to privacy rules issued by one of the other financial regulators, and (ii) those privacy rules treat the covered firm as an affiliate of that other company.

- **Information About Former Customers.** The categories of *nonpublic personal information* about former customers that the covered firm discloses and the categories of affiliates and nonaffiliated third parties to whom the covered firm discloses this information.
- **Information Disclosed to Non-Affiliated Service Providers and Joint Marketers.** The categories of *nonpublic personal information* that are disclosed and the categories of third parties providing services, which may include joint marketing.
- **Right to Opt Out.** An explanation of the consumer's right to opt out of the disclosure of *nonpublic personal information* to non-affiliated third parties, and the methods by which a consumer may exercise that right.
- **Fair Credit Disclosures.** Disclosures regarding sharing of certain consumer data with affiliates that the covered firm may make under the Fair Credit Reporting Act ("FCRA"), which is further discussed below.
- **Security Policies.** The covered firm's policies and practices with respect to protecting the confidentiality, security, and integrity of *nonpublic personal information*.
- **Disclosures Under the "Opt-Out" Exceptions.** A description of disclosures of *nonpublic personal information* made under the "opt-out" exceptions, which are further discussed below.

These requirements are not intended to mandate lengthy disclosures that precisely identify every type of information collected or shared or the name of every institution with which the covered firm shares information. Rather, the rules are intended to require notices that provide consumers with the *types* of third parties with which a covered firm shares information; the *types* of information that the firm shares; and the other information listed above.

The rules also authorize covered firms to provide "short form" notices to consumers with whom a firm does not have a customer relationship. The "short form," however, must provide the consumer with "reasonable means" to obtain the covered firm's full privacy notice.

What is the "opt-out" notice?

Part 160 requires a covered firm to provide a consumer with a reasonable opportunity to prevent the firm from disclosing the consumer's *nonpublic personal information* to nonaffiliated third parties - *i.e.*, to "opt out."

1. **Form and Method.** The opt-out notice, like the other required notices, must be *clear and conspicuous* and must:
 - a. state that the covered firm discloses or reserves the right to disclose *nonpublic personal information* to nonaffiliated third parties;
 - b. explain that the consumer has the right to opt out of that disclosure, *i.e.*, to direct that the information not be shared; and
 - c. afford a reasonable means by which the consumer may exercise that right (*e.g.*, check-off boxes in a prominent position on relevant forms with the opt-out notice or a toll-free phone number). Requiring the consumer to write his or her own letter to the covered firm in order to opt out is insufficient.
2. **Time to Opt Out.** Like the other regulators, the CFTC declined to mandate the length of the period that firms must allow consumers to exercise their opt-out right. In many circumstances, it would seem reasonable to give a consumer 30 days within which to opt out of information sharing.
3. **Ability to Opt Out Later.** The rules note that a consumer who does not exercise his right to opt out *does not lose* that right but may exercise

the right later. If he does so, the covered firm must stop information sharing as soon as possible thereafter.

4. **Partial Opt Out.** A covered firm may — but is *not* required to — provide a consumer with the option of a partial opt out in addition to the opt out required by this rule. The partial opt out may, for example, allow the consumer to limit the types of recipients of nonpublic personal information about that consumer.
5. **Change of Policy.** If a covered firm changes its disclosure policies with respect to sharing with nonaffiliated third parties, it must provide a revised notice and a new opportunity to opt out before disclosing nonpublic personal information to a nonaffiliated third party. This is a key point for firms as they start considering compliance with the rules. Firms will want to ensure that their policies anticipate future needs and activities so that the policies will not need to be revised and new notices be sent.
6. **Joint Accounts.** For joint accounts, a covered firm may provide a single opt out notice that explains how it will treat an opt direction by a joint consumer. Each joint consumer may exercise the right to opt out. The covered firm may either treat an opt out direction by a joint customer as applicable to all of the associated joint consumers or permit each joint consumer to opt out separately. If the covered firm permits each joint consumer to opt out separately, it must permit one of the joint consumers to opt out on behalf of all of the joint consumers.
7. **Specific Means.** The rules also permit a covered firm to require that a consumer opt out through a specific means, so long as that means is reasonable for the consumer.

What are the exceptions to the “opt-out” requirements?

Part 160 implements certain statutory exceptions that enable a covered firm to share information with certain nonaffiliated third parties without having to provide a right to opt out.

1. **Service Providers and Joint Marketing.** An important exception allows a covered firm to disclose *nonpublic personal information* to a nonaffiliated third party for use by that third party to perform services for, or functions on behalf of, the covered firm (including marketing), so long as the firm (a) fully discloses to the consumer that it will provide this information to the nonaffiliated third party before it is shared, and (b) enters into a contract with the third party that bars the third party from using the information for other purposes beyond those for which the information was disclosed.
2. **Processing and Servicing Transactions.** The opt out requirements also do not apply if the covered firm discloses *nonpublic personal information* “as necessary to effect, administer, or process a transaction” that is requested or authorized by the consumer, or for certain other purposes, including maintaining and servicing a customer’s account.
3. **At the Direction of the Consumer or for Other Limited Reasons.** Other exceptions include disclosures made at the direction or with the consent of the consumer, to protect the security of a covered firm’s records, to prevent fraud, to resolve consumer disputes, to respond to judicial process, and for other limited reasons.

What requirements apply to information received from a nonaffiliated third party?

Part 160 restricts the use or disclosure of *nonpublic personal information* received from a nonaffiliated third party financial institution. For example, in certain circumstances, the covered firm that received the information “stands in the shoes” of the nonaffiliated third party that disclosed the information.

Can an account number be disclosed to third parties?

In general, not for direct marketing purposes. The rules incorporate the GLBA statutory provision that prohibits a financial institution from disclosing a customer’s account number (or similar form of access

number or code) to a nonaffiliated third party (other than to a consumer reporting agency) for direct marketing purposes. There are exceptions, however, for providing numbers to agents and service providers (so long as they are not authorized to directly initiate charges to the account) and encrypted numbers without the key.

Are any policies and procedures to safeguard customer information required?

Yes. A covered firm must establish appropriate standards to safeguard customer records and information. The CFTC's rules do not prescribe specific procedures; rather, each firm should tailor its policies and procedures to its own systems and the needs of its customers. However, certain other federal agencies have issued guidelines, which, while not binding on covered firms, may provide helpful guidance.¹¹

When is part 160 effective?

Although the CFTC's rules became effective on June 21, 2001, full compliance is not mandatory until March 31, 2002. Firms must therefore provide initial privacy and opt-out notices to customers by March 31, 2002. Following a similar approach to that adopted by the other federal regulators, the CFTC provided an extended compliance timeframe for pre-existing joint marketing and servicing agreements. In other words, the rules require that all contracts with nonaffiliated third party service providers entered into before March 31, 2002, be brought into compliance with the rules by March 31, 2003.

Are there other considerations for covered firms?

Notwithstanding the summary above, the CFTC's rules present many ambiguities. For example, Section 160.11(a)(1) establishes limits on the reuse and redisclosure of *nonpublic personal information* re-

ceived from an nonaffiliated financial institution, but Section 160.11(a)(2) presents examples that appear to materially expand on these limits. Other ambiguities have been created by the frequently asked questions ("FAQs") that were recently issued by staff of the FTC and the federal bank and thrift agencies to interpret their versions of the GLBA privacy regulations.¹² (CFTC staff participated in the drafting of these FAQs, but did not issue FAQs applicable to the CFTC privacy regulations.)

In addition, covered firms must integrate their programs for complying with part 160 with programs to comply with other related statutes. For example, the FCRA governs the sharing of certain types of consumer data among affiliates, as well as creating other requirements — such as requiring that covered firms provide consumers with adverse action notices under certain circumstances. There are also many state laws and regulations generally analogous to the CFTC privacy rules and to the FCRA. Some of these state provisions are consistent with federal laws and rules, or are preempted by them; other provisions go beyond the federal requirements and would appear not to be preempted.

How can I get more information?

If you would like more information on the CFTC's privacy rules, the FCRA, or privacy matters in general, or a copy of any of the materials referenced herein, please contact:

Satish Kini (202) 663-6482
skini@wilmer.com;

James Mann (212) 230-8843
jmann@wilmer.com; or

Jerome Roche (202) 663-6870
jroche@wilmer.com

¹¹ See Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8,616 (Feb. 1, 2001).

¹² These FAQs are available through the FTC's Web site at <http://www.ftc.gov/privacy/glbact/glb-faq.htm>. For more information on these FAQs, see Selected Recent Developments Regarding Consumer Financial Privacy: Vermont Regulations And Federal Agency FAQs, available at http://www.wilmer.com/docs/news_items/ACFE71.pdf. Similarly, the SEC has issued an interpretive letter in question and answer format about its Regulation S-P, available at <http://www.sec.gov/divisions/investment/iard/faqregsp.shtml>.

WILMER, CUTLER & PICKERING

2445 M Street, N.W.
Washington, D.C. 20037-1420
Telephone: (202) 663-6000
Facsimile: (202) 663-6363

Securities Practice Group

James E. Anderson
Robert G. Bagnall
Brandon Becker
Joseph K. Brenner
Mark D. Cahn
Richard W. Cass
Bruce E. Coolidge
Meredith Cross
Charles E. Davidow

Stuart F. Delery
Colleen Doherty-Minicozzi
Paul Engelmayer
Simon Firth
Robert F. Hoyt
Andrew Kaizer
Satish Kini
Michael R. Klein
Yoon-Young Lee
Lewis Liman

Martin E. Lybecker
Robert B. McCaw
William McLucas
Mark S. Shelton
Marianne K. Smythe
Andrew N. Vollmer
Harry J. Weiss
Andrew B. Weissman
Soo J. Yim

Adam Abensohn
Stephanie Avakian
Matthew A. Chambers
Douglas J. Davison
Sara E. Emley
Leon B. Greenfield

Fraser Hunter
David Luigs
David Lurie
Cherie L. Macauley
Kevin McEnery
Jeffrey E. McFadden

Karen Mincavage
John C. Nagel
Bruce Newman
Gordon Pearson
Jeffrey Roth
Sam J. Salario, Jr.

Victoria E. Schonfeld
Erika Singer
Beth A. Stekler
William E. White
Jolie Zimmerman

This letter is for general informational purposes only and does not represent our legal advice as to any particular set of facts, nor does this letter represent any undertaking to keep recipients advised as to all relevant legal developments.

2445 M Street, N.W. Washington, D.C. 20037-1420 Telephone: (202) 663-6000	520 Madison Avenue New York, NY 10022 Telephone: (212) 230-8800	100 Light Street Baltimore, MD 21202 Telephone: (410) 986-2800	1600 Tysons Boulevard McLean, VA 22102-4826 Telephone: (703) 251-9700	4 Carlton Gardens London SW1Y5AA Telephone: 011 (44207) 872-1000	Rue de la Loi 15 Wetstraat B-1040 Brussels, Belgium Telephone: 011 (322) 285-4900	Friedrichstrasse 95 D-10117 Berlin Telephone: 011 (49-30) 2022-6400
---	---	--	---	--	---	---