
Securities Law Developments

SEC ADOPTS FINAL PRIVACY RULE

On June 22, 2000, the Securities and Exchange Commission (“SEC”) issued its final rule regarding the obligation of securities firms to protect the financial privacy of their consumers.¹ The new rule, Regulation S-P, implements the privacy requirements of last year’s financial modernization legislation, the Gramm-Leach-Bliley Act (“GLBA”). The SEC’s Regulation S-P is substantially similar to regulations recently adopted by the federal banking regulators and the Federal Trade Commission (“FTC”). The final rule reflects several changes made by the SEC in response to industry comments on the proposed rule, which was published on March 2, 2000.

Although the regulation becomes effective on November 13, 2000, compliance is not mandatory until *July 1, 2001*. Nevertheless, in light of the complexity of complying with the regulation, securities firms should start to develop the systems, policies and procedures needed for compliance with the new rule. As an initial matter, securities firms will want to take stock of what types of customer information they collect; what types of information they share with affiliates and nonaffiliated third parties; and whether that information is subject to the SEC’s new regulation.

Who is subject to the rule?

1. **Broker-Dealers**, including municipal securities broker-dealers and government securities broker-dealers, whether or not registered with the SEC. Foreign broker-dealers not registered with the SEC are *not* covered by the rule.
2. **Investment Companies**, whether or not registered with the SEC, including business development companies and registered foreign investment companies.

¹ Privacy of Consumer Financial Information (Regulation S-P), Release Nos. 34-42974, IC-24543, IA1883 (June 22, 2000) (to be codified at 17 C.F.R. pt. 248, and available at <<http://www.sec.gov/rules/final/34-42974.htm>>).

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.

3. **Registered Investment Advisers.** Unlike broker-dealers and investment companies, investment advisers that are not registered with the SEC (such as private investment advisers or investment advisers registered with the states) are *not* covered by the SEC’s Regulation S-P. State-registered advisers, however, are subject to the FTC’s privacy rules.

Note: The SEC’s Regulation S-P does not apply to insurance products offered by securities firms, unless these insurance products are also securities.

What does Regulation S-P require securities firms to do?

Investment advisers, investment companies, and broker-dealers must provide for the following:

1. **Notice.** Provide consumers with a “clear and conspicuous” notice regarding the firm’s privacy policies and practices and describe the conditions under which the firm may disclose “nonpublic personal information” about its consumers to affiliates and 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 of 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 consumer.

Which clients are covered?

The new rule requires a securities 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.

1. **Consumers** are individuals (or their legal representatives) who obtain a financial product or service primarily for personal, family, or household purposes. The final rule clarifies that a consumer includes an individual who provides nonpublic personal information when seeking to obtain brokerage or advisory services, even if the person does not open a brokerage account or enter into an advisory contract with the securities firm. It also clarifies that if a securities firm uses another entity as an agent in connection with the firm’s provision of a financial product or service to an individual, the individual will not be considered a consumer of the agent solely because of that relationship.
2. **Customers** are those consumers who have a *continuing relationship* with the securities firm. In general, the SEC requires that there be more than an isolated transaction to establish such a continuing relationship, but a single transaction may suffice if it establishes an expectation of continued service or further transactions. For example, entering into an advisory contract or buying securities

through a broker with whom a customer opens an account establishes a customer relationship because of the continuing nature of the service. The final rule clarifies, however, that an individual who engages in a transaction and is unlikely to expect future communication about that transaction from the securities firm would not be a customer of that firm. The final rule provides an example: A broker-dealer that provides a securities brokerage service to liquidate a position for an individual without the expectation of engaging in further transactions does not have a customer relationship with the individual.

Note: The regulation does not apply to a securities firm's business or institutional customers.

What information is protected?

Regulation S-P only protects “**nonpublic personal information**,” which is a key definition, that includes two types of information: (1) “personally identifiable financial information” and (2) any list, description, or grouping of consumers that is derived from such nonpublic personally identifiable financial information.

1. ***Personally identifiable financial information***, in turn, is defined broadly to include three types of information:
 - ***Supplied by Consumer***. Any information provided by a consumer to a securities firm in order to obtain a financial product or service, including, e.g., material that a consumer supplies on an application or to an investment adviser when entering into an investment advisory contract.
 - ***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, securities positions, financial products purchased or sold, or simply whether an individual is or was a firm's customer.
 - ***Obtained in Providing Products or Services***. Any information otherwise obtained by an institution 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. Such information need not relate to the consumer's financial condition or otherwise be “financial” in nature. The final rule clarifies that this also includes information collected through Internet “cookies.”

Note: The final rule responded to many industry comments by including an example that clarifies that *aggregated or blind data* lacking personal identifiers (such as account numbers, names, or addresses) is *not* “personally identifiable financial information.”

2. **Publicly available information**, however, is excluded from the definition of nonpublic personal information. Publicly available information means

information that the securities 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 (the final rule clarifies that an Internet site is not considered restricted merely because it requires a fee or password); and
- **Required Disclosures**, such as information in securities files, that are required to be made to the general public by federal, state, or local law.

The rule treats information as public if it *could* be obtained from one of those three public sources, whether or not the securities firm actually obtained it that way. Thus, if a securities firm reasonably believes that the information is lawfully made available to the public from the above-noted sources, then that information is excluded from the scope of *nonpublic personal information*. The final rule clarifies, however, that in evaluating whether it is reasonable to believe that information is publicly available, a securities firm must determine whether the customer has kept the information or his or her identity from being a matter of public record. For example, the SEC states that a firm will have a reasonable belief that a telephone number is publicly available if the firm takes steps to ensure that the number is not unlisted.

When must a securities firm disclose its privacy policy?

The rule requires a securities firm to provide *clear and conspicuous* notices that accurately reflect its privacy policies and practices. The SEC provides that notices are *clear and conspicuous* if they are “designed to call attention to the nature and significance of the information.” The SEC included several examples in the final rule to illustrate how to make the required notices clear and conspicuous and stated that the privacy disclosures may be combined with other required disclosures in a single document.

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 securities 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 rule’s definition of consumer, a securities firm can avoid all of the rule’s 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. The notice may be combined with other information that the

securities firm provides. For example, an investment adviser may provide the privacy notice when it provides the initial Form ADV to its customer. The final rule provides firms with additional flexibility to 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 (for example, when a brokerage account is transferred to a broker by SIPC), (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 nonaffiliated broker-dealer or registered adviser purchases fund shares or establishes an account on behalf of a customer.

- b. **Annual Notice.** For a customer, a securities 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 product 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 securities firm provide its initial and annual notices?

Under the rule, 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.

Regulation S-P permits a single notice to be provided to multiple customers who jointly obtain a financial product or service, *e.g.*, joint accountholders; however, each customer must be given the right to opt out. (A securities firm also has the discretion to provide separate notices to each accountholder.) In certain circumstances, securities firms also are permitted to engage in “householding;” that is, they may deliver a single privacy notice to consumers who share the same address.

The regulation also allows two or more institutions to provide joint notices, as long as they are delivered in accordance with the rule and are accurate for all recipients. Institutions that may give joint notices include (i) an introducing broker and its clearing broker (that clears on a fully disclosed basis), and (ii) an investment company and a broker-dealer that distributes its shares. 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?

The rule requires a securities firm to provide the following information in both the initial and annual privacy notices:

- **Collected Information.** The categories of *nonpublic personal information* about consumers that the firm collects. The final rule defines “collect” to

mean to obtain any such information, if one organizes or can retrieve it by name, symbol, identifying number or other identifying particular assigned to the individual.

- ***Disclosed Information.*** The categories of *nonpublic personal information* about consumers that the firm may disclose.
- ***With Whom is Information Shared.*** The categories of affiliates² and nonaffiliated third parties to whom the firm discloses *nonpublic personal information*.
- ***Information About Former Customers.*** The categories of *nonpublic personal information* about former customers that the securities firm discloses and the categories of affiliates and nonaffiliated third parties to whom the securities firm discloses this information.
- ***Information Disclosed to Non-Affiliated Service Providers.*** The categories of *nonpublic personal information* that are disclosed and the categories of third parties providing the services.
- ***Right to Opt Out.*** An explanation of the consumer’s right to opt out of the disclosure of *nonpublic personal information* to nonaffiliated third parties, and the methods by which a consumer may exercise that right.
- ***Fair Credit Disclosures.*** Disclosures, if any, regarding sharing of “consumer reports” with affiliates that are required by the Fair Credit Reporting Act.
- ***Security Policies.*** The securities firm’s policies and practices with respect to protecting the confidentiality, security, and integrity of *nonpublic personal information*.

In response to comments, the SEC clarified that 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 securities firm shares information. Rather, the rule is intended to require notices that provide consumers with the *types* of third parties with which a securities firm shares information; the *types* of information that the firm shares; and the

² An “affiliate” of a broker-dealer, investment company, or registered investment adviser is defined as any company that controls, is controlled by, or is under common control with that securities firm. The regulation also provides that a broker-dealer, investment company, or registered investment adviser is an affiliate of another company for purposes of the privacy rules if (i) the other company is subject to privacy regulations issued by one of the other financial regulators, and (ii) those privacy rules treat the broker-dealer, investment company, or registered investment adviser as an affiliate of that other company. The SEC explained that this part of the definition was designed to prevent the disparate treatment of affiliates within a holding company structure. The SEC noted that, without this provision, a broker-dealer in a bank holding company structure might not be considered affiliated with another entity in that organization under the SEC’s rules, even though the two entities would be considered affiliated under the federal banking agencies’ privacy rules.

other information listed above. The SEC stated that, in most cases, it believed that the disclosure requirements could be satisfied in a “tri-fold brochure.”

The final rule also reconsiders the SEC’s initial position and authorizes securities 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 securities firm’s full privacy notice. Also, in response to industry comments, the final rule contains sample clauses to show the level of detail the SEC expects.

Note: Despite commenters’ objections, the final rule requires that the initial and annual privacy notices include information on the categories of *affiliates* with which a securities firm shares information.

What is the “opt-out” notice?

Regulation S-P requires a securities firm to provide a *consumer (or customer)* 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 should
 - a. state that the securities firm 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 securities firm in order to opt out is insufficient.
2. **Time to Opt Out.** The SEC 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. In the case of isolated transactions, however, the SEC stated that the consumer should be able to decide whether to opt out “before completing the transaction.” If the consumer does not opt out during this opt-out notice time frame, the firm may disclose the consumer’s nonpublic personal information in accordance with the firm’s privacy notice.
3. **Ability to Opt Out Later.** The rule notes that a consumer who does not exercise his right to opt out *does not lose* that right but may exercise the right later at any time. If he does so, the securities firm must stop information sharing as soon as possible thereafter.

4. ***Partial Opt Out.*** A securities 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 securities firm changes its disclosure policies, it must provide a revised notice and a new opportunity to opt out before disclosing nonpublic personal information to a nonaffiliated third party in a manner that was not anticipated by the prior privacy notice. This is a key point for firms as they start considering compliance with the new rule. 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 firm may provide a single opt out notice that explains how it will treat an opt out direction by a joint accountholder. Each joint accountholder may exercise the right to opt out. The securities firm may either treat an opt out direction by a joint accountholder as applicable to all of the holders of the joint account or permit each joint accountholder to opt out separately. If only one joint accountholder opts out, the firm is prohibited from disclosing any information relating to that individual as well as any information that relates to that individual and other accountholders.
7. ***Specific Means.*** In response to industry comments, the final rule also permits a securities 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?

Regulation S-P implements certain statutory exceptions that enable a securities 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 securities 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 securities 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 securities firm discloses *nonpublic personal information* “as necessary to effect, administer, or process a transaction” that is requested or authorized by the consumer, or for 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 integrity of a securities firm's records, to prevent fraud, to resolve consumer disputes, to respond to judicial process, and for other limited reasons.

What requirements apply to nonaffiliated third parties that receive information?

The regulation prohibits a nonaffiliated third party that receives *nonpublic personal information* from a securities firm from disclosing that information, directly or through an affiliate, to any person not affiliated with the securities firm (or with the third party, if the third party is a securities firm) *unless* the disclosure would be lawful if made directly by the securities firm. For example, a nonaffiliated fund service provider that receives *nonpublic personal information* from a mutual fund may not directly or indirectly disclose information to another nonaffiliated third party of the fund and the service provider unless the fund could lawfully share the information with that party. As a very general rule of thumb, the third party "stands in the shoes" of the securities firm from which the third party received the information.

Securities firms are not required by Regulation S-P to monitor third parties' compliance with the privacy rule. However, the SEC commented that the limits on reuse could provide the basis for an enforcement action against an entity that violated the rule's requirements.

Can an account number be disclosed to third parties?

In general, no. The regulation incorporates 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 marketing purposes. In response to industry comments, the SEC clarified that there are exceptions for providing numbers to agents and service providers (so long as they are not authorized to initiate charges to the account) and encrypted numbers without the key.

Are any policies and procedures to safeguard customer information required?

Yes. A securities firm must establish appropriate standards to safeguard customer records and information. The SEC's rule does not prescribe specific procedures; rather, each firm should tailor its policies and procedures to its own systems and the needs of its customers.

When is Regulation S-P effective?

Although the regulations become effective on November 13, 2000, full compliance is not mandatory until July 1, 2001. Firms must therefore provide customers with the initial privacy and opt-out notices and a reasonable time to opt out by July 1, 2001. The SEC encourages firms to provide the notices as soon as practicable.

Commenters had asked the SEC to "grandfather" pre-existing joint marketing and servicing agreements. The SEC refused to take this approach. Instead, the rule requires that all contracts with nonaffiliated third party service providers entered into before July 1, 2000, be

brought into compliance with the regulations by July 1, 2002. All such contracts entered into after July 1, 2000, must be in compliance with Regulation S-P by July 1, 2001.

How can I get further information on Regulation S-P?

If you would like more information on Regulation S-P or a copy of the regulation, please contact Yoon-Young Lee at (202) 663-6720; Matthew Chambers at (202) 663-6591; Satish Kini at (202) 663-6482; Franca Harris at (202) 663-6557; or David Luigs at (202) 663-6451.

WILMER, CUTLER & PICKERING		
2445 M Street, N.W. Washington, D.C. 20037-1420 Telephone: (202) 663-6000 Facsimile: (202) 663-6363		
Securities Practice Group		
<i>James E. Anderson Brandon Becker Stephen F. Black Joseph K. Brenner Mark D. Cahn Richard W. Cass Bruce E. Coolidge Meredith Cross Charles E. Davidow Paul Engelmayer Robert F. Hoyt Andrew Kaizer Michael R. Klein</i>	<i>Yoon-Young Lee Lewis Liman Eric R. Markus Robert B. McCaw William McLucas Eric J. Mogilnicki Thomas Mueller Jeremy N. Rubenstein Marianne K. Smythe Andrew N. Vollmer Harry J. Weiss Andrew B. Weissman Soo J. Yim</i>	<i>Robert G. Bagnall Matthew A. Chambers Stuart F. Delery Colleen Doherty-Minicozzi Sara E. Emley Steven Finizio</i>
<i>Leon B. Greenfield Satish Kini David Lurie Jeffrey E. McFadden Karen Mincavage Jeffrey Roth</i>	<i>Mark S. Shelton Beth A. Stekler William White Jolie Zimmerman</i>	