The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 11699

March 6, 2000

SEC PROPOSES REGULATION S-P GOVERNING PRIVACY OF CONSUMERS' NONPUBLIC PERSONAL INFORMATION

1 Release Nos. 34-32484, IC-24326, and IA-1856 (the Proposing Release). The Proposing Release has not been published in the Federal Register yet, but it is available on the SEC's web site at http://www.sec.gov/rules/proposed/34-42484.htm. 2 The distinction between customers and consumers is an important one. See the discussion of "consumer," "customer" and "customer relationship" in the section on definitional issues below. [11699] March 6, 2000 TO: BOARD OF GOVERNORS No. 11-00 INVESTMENT ADVISER ASSOCIATE MEMBERS No. 5-00 INVESTMENT ADVISER MEMBERS No. 5-00 SEC RULES MEMBERS No. 17-00 UNIT INVESTMENT TRUST MEMBERS No. 3-00 RE: SEC PROPOSES REGULATION S-P GOVERNING PRIVACY OF CONSUMERS' NONPUBLIC PERSONAL INFORMATION _____ On March 2, 2000, the Securities and Exchange Commission proposed a new regulation, Regulation S-P, containing the privacy rules mandated by the Gramm-Leach-Bliley Act (the Act).1 A copy of the Proposing Release is attached and it is summarized below. Comments on the proposal are due on March 31, 2000. Background As required by the Act, proposed Regulation S-P generally requires every broker-dealer, investment company and investment adviser to: (i) Provide each of its customers2 with a notice of its privacy policies and practices at the time of establishing the customer relationship (the initial notice) and annually thereafter (the annual notice); (ii) Provide each of its consumers (who have not yet become customers) with an initial notice before disclosing nonpublic personal information about that consumer to a nonaffiliated third party; (iii) Refrain from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution has provided the consumer with an initial notice and an additional notice describing that practice and the consumer's right to prevent it (the opt out notice); and (iv) Adopt policies and procedures 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 3 The other federal financial regulators proposed their privacy rules in late February under the heading "Privacy of Consumer Financial Information." See 65 FR 8770 (Feb. 22, 2000) (joint proposal by the Federal Reserve Board, OCC, FDIC and OTS); www.ftc.gov (FTC proposal, issued Feb. 24, 2000); and www.ncua.gov (National Credit Union Administration proposal, issued Feb. 24, 2000). 4 See Proposing Release at n. 5 ("The examples are intended to describe ordinary situations that would comply with the applicable rule, but the particular facts and circumstances relating to each specific situation will determine whether compliance with an example constitutes compliance with the rule.") 5 The proposed rules define the term "clear and conspicuous" to mean that the notice is reasonably understandable and designed to call attention to the

nature and significance of the information contained in the notice. The proposed rules do not mandate the use of any particular technique for making the notices clear and conspicuous, but instead allow each financial institution the flexibility to decide for itself how best to comply with this requirement. 6 Proposing Release at 22. In a letter to the SEC staff in anticipation of the privacy rule proposal, the Institute recommended that the rules provide flexibility for any entity in a particular investment company complex to provide the required privacy notices. See Letter from Craig S. Tyle to Robert E. Plaze dated December 21, 1999 (the Initial Recommendation Letter). (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. The Act requires the federal financial regulators, including the SEC, to adopt regulations implementing its provisions no later than May 12, 2000.3 The Use of Examples in Proposed Regulation S-P Proposed Regulation S-P contains rules of general applicability followed by examples that illustrate the application of the general rules. These examples differ in substance from those used by the other federal financial regulators in their rule proposals, in an attempt to provide more meaningful guidance to the financial institutions subject to the Commission's jurisdiction. The examples also differ from the other regulators' proposals in terms of legal effect, in that compliance with the examples in proposed Regulation S-P would not necessarily constitute compliance with the applicable rule.4 In the other proposals, compliance with the examples would be considered a safe harbor. The Commission has requested comment on whether including examples in the rule is useful, and suggestions on additional or different examples that may be helpful in providing guidance as to the applicability of the rule. Initial and Annual Privacy Notices Initial notices. The Act requires a financial institution to provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided 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. Proposed Regulation S-P requires every financial institution to provide these notices in a manner that is "clear and conspicuous," that accurately reflects the institution's privacy policies and practices, and that is provided so that each recipient can reasonably be expected to receive actual notice.5 The proposed 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 rule and is accurate for all recipients. For example, an investment company and a broker-dealer that distributes its shares would be permitted, but not required, to provide a joint notice.6 The initial notice must be provided to the customer prior to the time that the financial institution and the customer establish a customer relationship. The proposed rules define a customer relationship to be established at the point at which the financial institution and the consumer enter into a continuing relationship. For example, when a consumer purchases investment company shares (in his or 7 Proposing Release at 23-24. 8 Section 502 of the Act. The examples that follow the general rule suggest several ways in which a financial institution may provide reasonable means to opt out, including check-off boxes, reply forms, and electronic mail addresses. 3 her own name) through a principal underwriter, the consumer establishes a customer relationship with the underwriter and the investment company.7 For a consumer who has not established a customer relationship with the financial institution, the initial notice may be provided at any point before the financial institution discloses nonpublic personal information about that consumer to nonaffiliated third parties. Annual notices. The Act requires a financial institution to provide notices of its privacy policies and practices at least annually to its customers. The proposed rules implement this requirement by requiring a clear and conspicuous notice that accurately reflects the current privacy policies and practices to be provided at least once during any period of twelve consecutive months. The rules governing how to provide an

initial notice also apply to annual notices. Opt Out Rights and Opt Out Notices The Act generally prohibits a financial institution from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution has provided the consumer with (i) an initial privacy notice (as described above) and (ii) a clear and conspicuous opt out notice. The opt out notice must inform the consumer that the institution may disclose nonpublic personal information to nonaffiliated third parties, state that the consumer has a right to opt out, and provide the consumer with a reasonable means by which to opt out.8 As with the initial and annual privacy notices, the opt out notice must be provided so that each recipient can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic form. The consumer's right to opt out is limited by several exceptions enumerated in the Act. One of these provides an exception for the disclosure of a consumer's nonpublic personal information to a nonaffiliated third party for its use to perform services for, or functions on behalf of, the financial institution, 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. In order to avail itself of this exception, the financial institution must (i) fully disclose to the consumer that it will provide this information to the nonaffiliated third party before the information is shared and (ii) enter into a contract with the third party that requires the third party to maintain the confidentiality of the information. Several other exceptions in the Act are for disclosures made, generally speaking, in connection with the administration, processing, servicing and sale of a consumer's account. Proposed Regulation S- P substantively reiterates these exceptions, making only stylistic changes to the statutory text that are intended to make the exceptions easier to read. Procedures to Safeguard Customer Information and Records The Act directs the Commission (and the other federal financial regulators) to establish appropriate standards for financial institutions relating to administrative, technical and physical safeguards to protect customer records and information. Proposed Regulation S-P implements this provision by requiring every broker, dealer, investment company, and registered investment adviser to adopt policies and procedures 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 9 See Initial Recommendation Letter. 10 Conversely, investment company shareholders who are not the record owners of their shares would not be consumers of the investment company. 11 The Institute had recommended that the Commission define the customer relationship, for fund shares sold through an intermediary, to mean the relationship between the shareholder and the intermediary. See Initial Recommendation Letter. 4 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. This approach follows a suggestion made by the Institute prior to the rulemaking.9 Definitional Issues "Consumer," "customer" and "customer relationship." Consistent with the Act, proposed Regulation S-P draws a distinction between "consumers" and "customers." The proposed rules define "consumer" to mean an individual who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. A "customer" is a consumer who has a customer relationship with a particular financial institution. The examples in the proposed rule make clear that an investor that purchases shares of an investment company in his or her own name would be a customer of that investment company.10 This is true even if the consumer purchased those shares through a broker or investment adviser. In that case, the individual will be a customer of both the broker or investment adviser who sold the shares and the investment company.11 Conversely, if the shares are not held in the name of the investor (e.g., if they are held in street name or in an omnibus account) the investor would be neither a consumer nor a

customer of the investment company. The distinction between consumer and customer 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 248.10 and 248.11 of the proposed regulation). By contrast, if a consumer becomes a customer, the institution must provide a copy of its privacy policy before it establishes the customer relationship and at least annually during the continuation of the customer relationship. “Nonpublic personal information” and “nonpublic personal financial information.” The Act defines “nonpublic personal information” to mean “personally identifiable financial information”(which the Act does not define) 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. “Nonpublic personal information” 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. The proposed rules implement this provision of the Act by restating the general categories of information described above and providing that “nonpublic personal information” does not include publicly available information when the information is part of a list, description, or other grouping of consumers that is derived without using personally identifiable financial information. The definition in the proposed rules also excludes any other publicly available information, unless the information is part of a list, description, or other grouping of consumers that is derived using personally identifiable financial information. As a general matter, the proposed rules treat any personally identifiable information as financial if the financial institution obtains the information in connection with providing a financial product or 12 This differs from the OCC, OTS and FDIC rule proposals, which included alternative definitions of publicly available information and requested comment on which would be preferable. One of the alternatives is similar to the definition in proposed Regulation S-P; the other definition would treat information as publicly available only if it was actually collected from a public source. 5 service to a consumer. This interpretation would cover a broad range of personal information provided to a financial institution, including, for example, information about the consumer’s health. “Publicly available information.” The proposed rules define “publicly available information” as information that the financial institution reasonably believes is lawfully made available to members of the general public from official public records, widely distributed media, or disclosures required to be made to the general public by federal, State, or local law. The proposed rules treat information as publicly available if it could be obtained from one of these three public sources, whether or not the institution actually obtains the information from such a source.12 Effective Date As proposed, new Regulation S-P would take effect on November 13, 2000, six months after final rules are required by the Act to be adopted. The Commission has requested comment on whether six months after adoption of final rules is sufficient to enable financial institutions to comply with the rules. Robert C. Grohowski Assistant Counsel Attachment Note: Not all recipients receive the attachment. To obtain a copy of the attachment referred to in this Memo, please call the ICI Library at (202) 326-8304, and ask for attachment number 11699. ICI Members may retrieve this Memo and its attachment from ICINet (http://members.ici.org).