MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Privacy and Security Advisory: Proposed Amendments May Expand Protection of Consumer Financial Information in the Securities Industry

4/28/2008

On March 4, 2008, the Securities and Exchange Commission (SEC or the "Commission") proposed amendments to Regulation S-P, which governs the privacy of consumer financial information in the securities industry, in an effort to prevent and address information security breaches in the industry and better protect investor information.

Regulation S-P was adopted by the SEC on June 29, 2000 to implement certain privacy rules of the Gramm-Leach Bliley Act (GLBA) and consumer protection rules of the Fair Credit Reporting Act (FCRA), which apply to entities regulated by the Commission such as brokers, dealers, investment advisers registered with the SEC, and investment companies. The proposed revisions will change Regulation S-P in four principal ways:

- by requiring more specific standards for safeguarding personal information and responding to data security breaches under Rule 30(a) of Regulation S-P (the "safeguards rule");
- by expanding the scope of the information covered by the safeguards rule and Rule 30(b) of Regulation S-P (the "disposal rule") and broadening the types of entities and persons covered by the safeguards and disposal rules;
- by requiring entities subject to the safeguards and disposal rules to maintain written records of their policies and procedures and their compliance with such policies and procedures; and
- by creating a new exception from Regulation S-P's notice and opt-out requirements to permit limited disclosure of investor information when certain kinds of personnel move from one brokerage or advisory firm to another.

## Specific Standards for Safeguarding Personal Information and Responding to Data Security Breaches

The current safeguards rule simply requires institutions to adopt written policies and procedures to address the safeguarding objectives stated in the GLBA. Under the proposed amendments—modeled after safeguarding guidelines adopted by the Federal Banking Agencies and the Federal Trade Commission—institutions subject to the safeguards rule would be required to develop, implement, and maintain a comprehensive "information security program," including written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information and for responding to incidents of unauthorized access to, or use of, personal information.

While an information security program can be tailored by institutions according to their size, nature, and scope of business activities and the sensitivity of the personal information at issue, the program must be reasonably designed to:

> (i) ensure the security and confidentiality of personal information, (ii) protect against any anticipated threats or hazards to the security or integrity of personal information; and (iii) protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or securityholder who is a natural person.[1]

For this purpose, "substantial harm or inconvenience" would be defined to mean "personal injury, or more than trivial financial loss, expenditure of effort or loss of time, including theft, fraud, harassment, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the unauthorized use of the information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise use the individual's account." "Substantial harm or inconvenience" would *not* include "unintentional access to personal information by an unauthorized person that results only in trivial financial loss, expenditure of effort or loss of time," such as if use of the information results in an institution deciding to change the individual's account number or password.

The information security program must also include detailed written data-breach incident response policies and procedures that include notice to affected individuals, and potentially the SEC, or, for certain broker-dealers, to their designated examining authority. Such notices (under the proposed SEC rule) must be provided in the event that a data breach results in substantial harm or inconvenience to an individual or an unauthorized person has intentionally obtained access to or used sensitive personal information. The proposed data security breach response procedures are also modeled after, and intended to be consistent with, the security breach notification guidelines adopted by the Federal Banking Agencies.

## Expansion of the Scope of Information and Type of Entities and Persons Covered by the Safeguards and Disposal Rules

Because the Commission adopted the safeguards and disposal rules at different times and under different statutes, they differ in the scope of information they cover and thus do not adequately protect against the unauthorized disclosure of personal financial information. The Commission proposes to amend the two rules so that both protect "personal information," and to define the term to encompass any record containing either "nonpublic personal information"[2] under the GLBA or "consumer report information"[3] under the FCRA, that is "identified with any consumer, or with any employee, investor, or securityholder who is a natural person, "whether in paper, electronic, or other form,"[4] that is handled or maintained by an institution or on the institution's behalf.

The proposed amendments to Regulation S-P also broaden the type of institutions covered by the safeguards rule. Currently, the safeguards rule applies to brokers, dealers, registered investment advisers, and investment companies, while the disposal rule applies to those entities and also to registered transfer agents.[5] The Commission intends to extend the application of the safeguards rule to registered transfer agents as well, to require that these institutions maintain adequate safeguards to protect investor personal information, in addition to taking measures to properly dispose of such information. On the other hand, the proposed amendments would exclude notice-registered broker-dealers, who are registered as broker-dealers in order to conduct business in security futures products under Section 15(b)(11)(A) of the Exchange Act, from the scope of the safeguards rule.

The Commission also proposes to extend the disposal rule to apply to natural persons who are associated persons of a broker or dealer, supervised persons of registered investment advisers, and associated persons of a registered transfer agent.[6] The purpose of this amendment is to "make persons associated with a covered institution directly responsible for properly disposing of personal information consistent with the institution's policies."[7]

## Records of Compliance with the Safeguards and Disposal Rules

The Commission further proposes to amend Regulation S-P to require institutions subject to the safeguards and disposal rules to maintain written records of their safeguards and disposal policies and procedures and to document their compliance with "the elements required to develop, maintain and implement these policies and procedures for protecting and disposing of personal information, including procedures relating to incidents of unauthorized access to or misuse of personal information."[8] The periods of time for which records would have to be preserved would vary from institution to institution and are specifically provided in the proposed amendments.[9]

## New Exception to the Notice and Opt-out Requirements

Lastly, the proposed amendments create a new exception from Regulation S-P's notice and opt-out requirements, to allow limited disclosure of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or advisory firm to another. This exception would permit the

disclosure of the following information between firms:

> [i] the customer's name, [ii] a general description of the type of account and products held by the customer, and [iii] contact information, including address, telephone number and e-mail information.[10]

The proposed exception is intended to promote investor choice by allowing investors to more easily follow a representative who moves from one firm to another, "to provide legal certainty, and reduce potential incentives for improper disclosures."[11]

Comments on the proposed amendments are due on or before May 12, 2008. The proposed regulation is available on the SEC's web site here.

---

**Endnotes**

[1] *See* proposed paragraph (a)(2) of Section 30 of Regulation S-P.

[2] *See* 15 U.S.C. 6802(a), (b). "Nonpublic personal information" is defined in the GLBA and the current Regulation S-P as personally identifiable financial information, as well as any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available, subject to certain exceptions.

[3] *See* 15 U.S.C. 1681w(a)(1). "Consumer report information" is defined as any record about an individual in any form "that is a consumer report or is derived from a consumer report," as well as a compilation or such records. "Consumer report information" does not include information that does not identify individuals, such as aggregate information or blind data. The term "consumer report" has the same meaning as in section 603(d) of the FCRA (15 U.S.C. 1681(d)).

[4] *See* proposed paragraph d(8) of Section 30 of Regulation S-P.

[5] *See* proposed paragraph d(14) of Section 30 of Regulation S-P. The term "transfer agent" has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).

[6] *See* proposed paragraph (b)(1) of Section 30 of Regulation S-P. The term "associated person of a broker dealer" is defined in proposed paragraph (d)(1) of Section 30 of Regulation S-P to have the same meaning as in Section 3(a)(18) of the Exchange Act of 1934 (15 U.S.C. 78c(a)(18)). The term "supervised person of an investment adviser" is defined in proposed paragraph (d)(13) of Section 30 of Regulation S-P to have the same meaning as in Section 202(a)(25) of the Investment Advisers Act of 1940 (15 U.S.C. 80b-2(a)(25)).

[7] *See* Exchange Act Release No. 57427 (March 4, 2008) at 38.

[8] *See* Exchange Act Release No. 57427 (March 4, 2008) at 40.

[9] *See* proposed paragraph (c)(2) of Section 30 of Regulation S-P.

[10] *See* proposed paragraph (a)(8)(i) of Section 15 of Regulation S-P.

[11] *See* Exchange Act Release No. 57427 (March 4, 2008) at 44.

---

*For assistance in this area,*
*please contact:*

**Cynthia Larose**
**(617) 348-1732**
CLarose@mintz.com

*or the Mintz Levin attorney who ordinarily handles your legal affairs.*