MAYER·BROWN

FINANCIAL SERVICES REGULATORY & ENFORCEMENT UPDATE

SEC Proposes Amendments to its Privacy Rules (Regulation S-P)

April 8, 2008

The Securities and Exchange Commission (SEC) is proposing to amend Regulation S-P[1] to require broker-dealers, investment companies, registered investment advisers and registered transfer agents to adopt comprehensive information security programs.[2] In particular, proposed amendments to Sections 15 and 30 of Regulation S-P would create new reporting requirements for institutions that have experienced a breach of information security, introduce mandatory recordkeeping requirements, and limit the client information a registered broker-dealer representative or registered investment adviser representative may take with him or her when that representative moves from one brokerage or advisory institution to another. A summary of the Proposing Release is set forth below.

Background

Section 503 of the Gramm-Leach-Bliley Act (GLBA) requires every financial institution to inform its customers about that institution's privacy policies and practices, and limits the circumstances in which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party without first giving the consumer an opportunity to opt out of the disclosure.[3] Section 504(a) of the GLBA requires various federal regulators, including the SEC, to implement standards for financial institutions overseen by such regulators to safeguard customer information and records.[4] In enacting the GLBA, Congress directed the SEC and other federal financial regulators to establish and implement information safeguarding standards requiring financial institutions subject to their jurisdiction to adopt administrative, technical and physical information safeguards.[5] In response to the statutory mandate in the GLBA, the SEC promulgated Regulation S-P.[6] The other federal regulators adopted substantially similar rules applicable to financial institutions covered by such regulators, and the Federal Trade Commission (FTC) adopted catch-all rules that apply to "financial institutions" not otherwise subject to the jurisdiction of the other federal regulators.[7]

The SEC is proposing amendments to Regulation S-P to address several concerns. First, there have been an increasing number of information security breaches involving the institutions that it regulates and there is a potential for identity theft and other

misuse of personal financial information.[8] Second, the SEC is concerned that some institutions in the securities industry are not regularly reevaluating and updating their information safeguarding programs to deal with the increasingly sophisticated methods of attack, such as "phishing" sites that target the financial sector.[9] Finally, the SEC believes that departing representatives of institutions may have a strong incentive to transfer as much customer information as possible to their new institutions and that information may be transferred without adequate supervision, in contradiction of privacy notices provided to customers, or potentially in violation of Regulation S-P.[10] The Proposing Release is intended to address these specific information security concerns and provide a framework under which institutions with departing representatives could share limited customer contact information and could supervise the information transfer to the representatives' new institutions.

Information Security Program

Under the proposed amendments to Section 30(a)(3) of Regulation S-P, every broker-dealer (other than a notice-registered broker-dealer), investment company, investment adviser registered with the SEC[11] and transfer agent registered with the SEC (Covered Institutions) would be required to develop, implement and maintain a comprehensive "information security program" for protecting personal information and responding to unauthorized access to or use of personal information. Initially this would require Covered Institutions to: designate, in writing, one or more employees to coordinate the information security program; identify, in writing, reasonably foreseeable security risks that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of personal information or personal information systems; create a written record of the design and implementation of their safeguards to control identified risks; train staff to implement the information security program; and oversee service providers and document that oversight in writing.[12] Proposed amended Section 30(a)(3)(vi) of Regulation S-P also would require institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for personal information, document this finding, and enter into contracts with the service providers to implement and maintain appropriate safeguards. Reasonable steps could include the use of a third-party review of those safeguards such as a Statement of Auditing Standards No. 70 (SAS 70) report, a SysTrust report, or a WebTrust report.[13]

Security Breach Response Requirements

Covered Institutions also would have to adopt new written procedures relating to security breach incidents. Under proposed Section 30(a)(4), Covered Institutions would be required to have written procedures to: assess any incident involving unauthorized access or use and identify, in writing, what personal information systems and what types of personal information may have been compromised; take steps to contain and control the incident to prevent further unauthorized access or use and document all such steps taken in writing; promptly conduct a reasonable investigation and

determine, in writing, the likelihood that the information has been or will be misused after the institution becomes aware of any unauthorized access to sensitive personal information; and notify individuals with whom the information is identified as soon as possible (and document the provision of such notification in writing) if the institution determines that misuse of the information has occurred or is reasonably possible.[14]

Moreover, Section 30(a)(4) of Regulation S-P would require an institution to provide notice to the SEC (or for certain broker-dealers, their designated examining authority) using Proposed Form SP-30 as soon as possible after the institution becomes aware of any incident of unauthorized access to or use of personal information in which there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, or in which an unauthorized person has intentionally obtained access to or used sensitive personal information.[15] A prompt response, in accordance with existing SEC guidance on the timely production of records, would be necessary in circumstances involving ongoing misuse of sensitive personal information.[16] Information submitted to the SEC on Form SP-30 would be accorded confidential treatment to the extent permitted by law.[17]

Proposed Section 30(d)(10) of Regulation S-P would define "sensitive personal information" to mean "any personal information, or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information," including the individual's Social Security number, or any one of the individual's name, telephone number, street address, e-mail address or online user name, *in combination with* any one of the individual's account number, credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric authentication record, or other authenticating information.

Proposed Section 30(a)(5) of Regulation S-P would require notice to affected individuals as soon as possible, *although* Covered Institutions may delay notification if law enforcement requests in writing such a delay while it completes its criminal investigation.[18] The notice would be required to: describe the incident and the type of information that was compromised, and what was done to protect the individual's information from further unauthorized access or use; include a toll-free telephone number or other contact information for further information and assistance from the institution; recommend that the individual review account statements and immediately report any suspicious activity to the institution; and include information about FTC guidance regarding the steps an individual can take to protect him or her against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's web site address and toll-free telephone number for obtaining identity theft guidance and reporting suspected incidents of identity theft.

Proposed Section 30(a)(5) of Regulation S-P also would require notice of unauthorized access or use of sensitive personal information to be delivered by "a means designed to ensure that the individual can reasonably be

expected to receive it." It is unclear whether notices could be provided via electronic mail under this proposed provision. Banking agencies have reached the conclusion that an institution may choose to provide notices to all affected customers by telephone or by mail, or for those customers who conduct transactions electronically, using electronic mail notice.[19]

Extending the Scope of Safeguards and the Disposal Rule

Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act") requires banks, broker-dealers and other regulated entities to develop and maintain controls to ensure that they properly dispose of "consumer report information."[20] Section 30(b)(ii), which effectively implemented this statutory mandate when it was adopted in 2004, defines "consumer report information" as any record about an individual, whether in paper, electronic, or other form that is a consumer report or that is derived from a consumer report.

The Proposing Release would amend Section 30(a) (the "safeguards rule") and Section 30(b) (the "disposal rule") under Regulation S-P so that both protect "personal information," and would define the term "personal information" to encompass any record containing either "nonpublic personal information" or "consumer report information." This will expand the scope of information covered by the disposal rule beyond the requirements of Section 216 of the FACT Act and those requirements imposed upon financial institutions by the federal banking agencies. "Personal information" also would include information identified with any consumer, or with any employee, investor, or securityholder who is a natural person, in paper, electronic or other form, that is handled by the institution or maintained on the institution's behalf. The Proposing Release also would make a conforming change to the definition of "personally identifiable financial information" by including, within the definition, information that is handled or maintained by a Covered Institution or on its behalf, and that is identified with any consumer, or with any employee, investor, or securityholder who is a natural person.

The safeguards rule currently applies to broker-dealers, registered investment advisers, and investment companies, but proposed Section 30(d)(14) of Regulation S-P would extend the safeguards rule to registered transfer agents by including information about individual investors maintained by registered transfer agents in the definition of "personal information." The disposal rule currently applies to broker-dealers, registered investment advisers, and investment companies, as well as to registered transfer agents, and proposed Section 30(b)(1) of Regulation S-P would extend the disposal rule to natural persons who are associated persons of a broker-dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.[21]

Records of Compliance Requirement

The proposed amendments to Section 30 of Regulation S-P discussed above will, if adopted, require Covered Institutions to document that they have complied with the elements required to develop, maintain

and implement the policies and procedures for protecting and disposing of personal information, including procedures relating to incidents of unauthorized access to, or misuse of, personal information. The periods of time for which the records would have to be preserved would vary by institution and would need to be consistent with existing recordkeeping rules. Broker-dealers would have to preserve the records for a period of not less than three years, the first two years in an easily accessible place as is generally required under Rule 17a-4 of the Securities Exchange Act of 1934. Registered transfer agents would have to preserve the records for a period of not less than two years, the first year in an easily accessible place. Investment companies would have to preserve the records for a period of not less than six years, the first two years in an easily accessible place. Registered investment advisers would have to preserve the records for five years, the first two years in an appropriate office of the investment adviser.

Information Disclosure When Representatives Leave Their Institutions

Proposed amendments to Section 15 of Regulation S-P will provide a framework under which institutions with departing representatives could share limited customer contact information and could supervise the information transfer to the representatives' new institutions. In particular, proposed Section 15(a)(8) provides an exception to the initial notice requirement in Section 4(a)(2), the opt-out requirements in Sections 7 and 10, and the initial notice requirement in connection with service providers and joint marketing in Section 13 of Regulation S-P. Section 15(a)(8) would limit an institution's disclose to the customer's name, a general description of the type of account and products held by the customer, and contact information, including address, telephone number and electronic mail information. The SEC considered an alternative approach that would require all institutions to include specific notice and opportunity to opt out of this information sharing in their initial and annual privacy notices.[22] The SEC has not chosen the alternative approach and has instead chosen an approach that does not require specific disclosure.

Registered broker-dealers and registered investment advisers seeking to rely on the proposed exception would have to require their departing representatives to provide to them, no later than each representative's separation from employment, a written record of the information that would be disclosed pursuant to the exception, and broker-dealers and registered investment advisers would be required to preserve such records consistent with the proposed recordkeeping provisions of Section 30 of Regulation S-P.[23] Under this limitation, an institution may not require or expect a representative from another institution to bring more information than necessary for the representative to solicit former clients.[24]

Endnotes

1 Regulation S-P is codified at 17 C.F.R. pt. 248.1 *et seq*.

2 *See* Exchange Act Release No. 57,427 (March 4, 2008), 73 Fed. Reg. 13,692 (March 13, 2008) (the "Proposing Release"), *available at* http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf.

3 15 U.S.C. § 6803. As an aside, Regulation S-P's disclosure and opt-out requirements apply only to

"nonpublic personal information" about "consumers" or "customers" (each a defined term). Under Section 3(g)(1) of Regulation S-P, a consumer is any individual who obtains a financial product or service that is to be used primarily for personal, family or household purposes. Under Section 3(j) of Regulation S-P, a customer is a consumer who has a continuing relationship with a financial institution. The distinction between "customer" and "consumer" is significant because the notice requirements are different for each type of relationship. Pursuant to Sections 14 and 15 of Regulation S-P, a financial institution must provide notice of its privacy policy to a "customer" when the customer relationship is formed and at least annually throughout the customer relationship. In contrast, a financial institution is required to provide notice of its privacy policy to a "consumer" only if it intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for purposes other than those permitted by Sections 14 and 15 of Regulation S-P.

4 15 U.S.C. § 6805(b)(1)-(2).

5 *See* 15 U.S.C. § 6801(b).

6 *See* Exchange Act Release No. 42,974 (June 22, 2000), 65 Fed. Reg. 40,334 (June 29, 2000); *see also* Exchange Act Release No. 44,730 (Aug. 21, 2001), 66 Fed. Reg. 45,138 (Aug. 27, 2001) (amending Regulation S-P to permit "notice registered broker-dealers"—i.e., futures commission merchants and introducing brokers that are registered by notice as broker-dealers in order to conduct business in security futures products under Section 15(b)(11)(A) of the Exchange Act—to comply with Regulation S-P by complying with financial privacy rules that the Commodity Futures Trading Commission adopted); *see also* Exchange Act Release No. 2332 (Dec. 2, 2004), 67 Fed. Reg. 71,322 (Dec. 8, 2004) (adopting the disposal rule under Section 30(b) of Regulation S-P and amending Regulation S-P to require that policies and procedures that institutions must adopt under Section 30(a) of Regulation S-P be in writing).

7 *See* 65 Fed. Reg. 33,646 (May 24, 2000) (adopting the FTC's privacy rules).

8 *See* Proposing Release at 13,693. In particular, the SEC notes a recent administrative proceeding, *In re NEXT Financial Group Inc.*, Exchange Act Release No. 56,316 (Aug. 24, 2007).

9 *See* Proposing Release at 13,694.

10 *See id.* at 13,702. It appears that proposed amendments to Section 15 of Regulation S-P have been influenced by the existence of a so-called "recruiting protocol" developed in 2004. In the Proposing Release, the SEC notes that certain large broker-dealers entered into a protocol under which signatories agreed not to sue one another for recruiting one another's registered representatives, if the representatives take only limited client information to another participating firm. The SEC also notes that, under the protocol, the information that a departing representative may take to another firm is limited to each client's name, address, a general description of the type of account and products held by the client, and the client's phone number and e-mail address. Under the protocol, this information may be used at the representative's new firm only by the representative, and only for the purpose of soliciting the representative's former clients. Curiously, the Proposing Release does not address the key issue of whether users of the protocol may be considered compliant with Regulation S-P by the SEC.

11 Unregistered advisers, including state-registered advisers, are treated as "financial institutions" and are subject to FTC rules. *See* 15 U.S.C. § 6809(3)(A) (defining "financial institution" as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12").

12 These requirements are similar to those adopted by the federal banking agencies and imposed on depository institutions. *See*, *e.g.*, 12 C.F.R. Part 30, Appendix B (applicable to national banks).

13 *See* Codification of Accounting Standards and Procedures, Statement on Auditing Standards No. 70, Reports on Processing of Transactions by Service Organizations (American Inst. of Certified Public Accountants); *see also* Proposing Release at 13,696 n.41.

14 The requirements set forth in the Proposing Release are very similar to those imposed by the federal banking agencies. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Notice, 70 Fed. Reg. 15,736 (March 29, 2005).

15 The federal banking agency guidance on the required regulatory notification in the event of a security breach is broader than the SEC's significant risk standard in proposed Section 30(a)(4)(v)(A) of Regulation S-P. The federal banking agency guidance requires notice to the appropriate regulatory agency even in circumstances where there is no significant risk to customers. The federal banking agency made a conscious decision to adopt different standards for the required notice to regulators and the required notice to customers. *See* 70 Fed. Reg. 15,741 (March 29, 2005) ("The Agencies have concluded that the standard for notification to regulators should provide an early warning to allow an institution's regulator to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers if the institution has not already done so.").

16 *See* Proposing Release at 13,698.

[17] *See* 17 C.F.R. § 200.83 (providing a procedure by which persons submitting information to the SEC can request that the information not be disclosed pursuant to a request under the Freedom of Information Act (5 U.S.C. § 552)).

[18] In the case of a hacking or any suspicious transaction relevant to a possible violation of law or regulation, a broker-dealer may need to file a suspicious activity report. *See* 31 C.F.R. § 103.19 (requiring every registered broker-dealer to file with the Financial Crimes Enforcement Network, a bureau of the U.S. Department of Treasury, a report of any suspicious transaction relevant to a possible violation of law or regulation).

[19] *See* 70 Fed. Reg. 15,736, 15,753 (2005).

[20] *See* 15 U.S.C. § 1681w.

[21] The term "associated person of a broker or dealer" would be defined by proposed paragraph (d)(1) of Section 30 to have the same meaning as in Section 3(a)(18) of the Exchange Act (15 U.S.C. § 78c(a)(18)). The term "supervised person of an investment adviser" would be defined by proposed paragraph (d)(13) of Section 30 to have the same meaning as in Section 202(a)(25) of the Investment Advisers Act (15 U.S.C. § 80b-2(a)(25)). The SEC proposed to include "supervised" persons of an investment adviser, rather than "associated" persons, in order to include all employees, including clerical employees, of an investment adviser who may be responsible for disposing of personal information. *See* Proposing Release at 13,701 n.87.

[22] *See id.* at 13,703.

[23] *See id.* at 13,701.

[24] *See id.* at 13,703.

Comments and Questions

Comments on the Proposing Release should be submitted to the SEC on or before May 12, 2008. If you have any questions or would like to receive a copy of the Proposing Release, please contact any of the following attorneys:

Michele L. Gibbons
713.238.2623
mgibbons@mayerbrown.com

Jeffrey P. Taft
202.263.3293
jtaft@mayerbrown.com

Jerome J. Roche
202.263.3773
jroche@mayerbrown.com

Shahriar Hafizi
202.263.3748
shafizi@mayerbrown.com