SEC PROPOSES AMENDMENTS TO REGULATION S-P TO SAFEGUARD CUSTOMER PRIVACY

On March 4, 2008, the Securities and Exchange Commission ("SEC") proposed for comment amendments to Regulation S-P[1] which governs consumer privacy obligations of registered investment companies, registered broker-dealers, registered investment advisers, and registered transfer agents ("Covered Institutions"). The proposed amendments: (i) specify additional standards for information security programs, including standards that would apply to data security breach incidents, (ii) extend Regulation S-P's disposal rule to cover associated persons of broker-dealers and registered transfer agents, as well as supervised persons of registered investment advisers, (iii) require institutions subject to the safeguards and disposal rules to maintain written records of their policies and procedures and their compliance with them, (iv) extend Regulation S-P's safeguards rule to cover registered transfer agents, and (v) provide a new exception to permit the disclosure of limited customer information when representatives move from one broker-dealer or registered investment adviser to another.

Background on Regulation S-P

The Gramm-Leach-Bliley Act (the "GLBA"), adopted in 1999, requires federal financial regulators, including the SEC, the Commodity Futures Trading Commission ("CFTC"), the Federal Trade Commission ("FTC"), the Federal Deposit Insurance Corporation ("FDIC"), and other banking regulators, to adopt rules to govern the use of consumers' personal information by the financial institutions under their jurisdiction. In accordance with the GLBA, the SEC adopted Regulation S-P in 2000.[2] Regulation S-P implements notice requirements and restricts the ability of Covered Institutions to disclose nonpublic personal information about **individual** consumers (*i.e.*, natural persons only).

---

1 SEC Release 34-57427 (March 4, 2008) (the "Release"). The Release is available on the SEC Website at http://www.sec.gov/rules/proposed/2008/34-57427.pdf.

2 Investment advisers not registered with the SEC or the CFTC and investment companies not subject to SEC or CFTC regulation, such as hedge funds and private equity funds, are subject to the FTC's privacy rules. Any fund operated by a commodity pool operator that is registered with the CFTC or an investment adviser registered with the CFTC as a commodity trading adviser will be subject to the CFTC's privacy rules. Both the CFTC's and FTC's privacy rules are similar but not identical to Regulation S-P. If a person or entity is registered with both the CFTC and the SEC, compliance with Regulation S-P will also satisfy the CFTC's privacy rules. 17 C.F.R. Part 160, Section 160.2(b).

In general terms, Regulation S-P requires the following:

- Covered Institutions must notify "consumers" and "customers"[3] of their policy regarding disclosure of "nonpublic personal information."
- To the extent that Covered Institutions choose (or reserve the right) to disclose nonpublic personal information to non-affiliated third parties[4] outside the exceptions contained in Regulation S-P, they must provide consumers and customers with the opportunity to "opt out" from such disclosures.
- Covered Institutions must adopt policies and procedures reasonably designed to ensure the security, confidentiality, and integrity of customer records and protect them against anticipated hazards and unauthorized access or use that could result in substantial harm or inconvenience.

Additionally, since 2005, Regulation S-P has required Covered Institutions to adopt appropriate standards through written procedures which include administrative, technical and physical safeguards to protect customer records and information ("safeguards rule"), and proper disposal of consumer report information ("disposal rule").

Proposed Changes to Regulation S-P

Revised Safeguarding Policies and Procedures

The proposed amendments would require each Covered Institution to develop, implement, and maintain a comprehensive "information security program." A significant change that is part of the SEC's proposal is that the security program must include policies and procedures for responding to "data breaches," *i.e.*, unauthorized access to or use of personal information.[5]

---

[3] For the purposes of Regulation S-P, a "consumer" is an individual who obtains, from a Covered 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" or continuing relationship with a Covered Institution to obtain such products or services.

[4] Generally speaking, an affiliation exists when one company controls, is controlled by, or is under common control with another company.

[5] These procedures would include notice to affected individuals if misuse of sensitive personal information has occurred or is reasonably possible, and notice to the appropriate regulator under circumstances in which the individual has suffered substantial harm or inconvenience or an unauthorized person has intentionally obtained access to or used sensitive personal information. The goal here is to avoid requiring notification in circumstances in which there is no significant risk of substantial harm or inconvenience. This standard is much more lenient with respect to notice to regulators than the GLBA guidelines of the banking agencies, which require notice to a financial institution's primary regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. Many state laws have exemptions/exceptions from breach notification requirements for institutions subject to federal breach notification requirements. For those states, compliance with Regulation S-P's breach notification law would satisfy a Covered Institution's state obligations.

Additionally, a Covered Institution's security program would be required to: (i) designate an employee or employees to coordinate the comprehensive information security program, (ii) document and implement certain information safeguards after identifying certain security risks, (iii) regularly document and monitor the effectiveness of the security program, (iv) train staff that will implement the security program, (v) oversee service providers and contract with them to implement and maintain appropriate safeguards, and (vi) evaluate and adjust the security program if appropriate.

Expansion of the Scope of the Safeguards and Disposal Rules

Another change from the current safeguards and disposal rules is that a wider scope of information would be protected. Rather than the current rules that protect "customer records and information"[6] or "consumer report information"[7], the proposed amendments would extend that protection to "personal information", which would encompass any record containing either "nonpublic personal information"[8] or consumer report information. Moreover, the rules would be significantly expanded by including within the definition of personal information such information identified with any consumer, or with any employee, investor, or securityholder of a Covered Institution who is a natural person. The purpose of this expansion is to protect those who may not be a consumer or customer of a Covered Institution.

The proposed amendments would extend the safeguards rule to registered transfer agents, but would now specifically exclude notice-registered broker-dealers,[9] which are covered by the CFTC's privacy rules.

In addition, the disposal rule would apply to associated persons of brokers or dealers and registered transfer agents and supervised persons of registered investment advisers. The SEC believes that investors would benefit by having persons associated with a Covered Institution directly responsible for properly disposing of personal information consistent with the institution's policies.

---

6 A term used in the current safeguards rule.

7 A term used in the current disposal rule, "consumer report information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data.

8 17 C.F.R. §248.3(t) defines "nonpublic personal information" as "personally identifiable financial information," including "any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available information, such as account numbers."

9 Regulation S-P was amended in 2001 to permit futures commission merchants and introducing brokers that are registered by notice as broker-dealers in order to conduct business in security futures products to comply with Regulation S-P by complying with the financial privacy rules of the CFTC.

Records of Compliance

The proposed amendments would require Covered Institutions to preserve written records of their safeguards and disposal policies and procedures. Covered Institutions would be required to document that they have complied with the elements required to develop, maintain, and implement policies and procedures for protecting and disposing of personal information, including procedures relating to incidents of unauthorized access to or misuse of personal information.[10]

Exception for Limited Information Disclosure When Personnel Leave Their Firms

As noted above, notice and opt-out requirements may apply when certain non-public personal information of customers is shared between non-affiliated Covered Institutions. The proposed amendments would add a new exception that would: (i) permit limited disclosures of customer information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one firm to another, and (ii) permit one firm to disclose to another only the following information: the customer's name; contact information, including address, telephone number, and e-mail information; and a general description of the type of account and products held by the customer. The shared information may not include any customer's account number, Social Security number or securities positions. Moreover, a departing representative may only solicit customers that were the representative's clients.

The proposed exception is designed to facilitate the transfer of customer contact information that would help broker-dealers and registered investment advisers offer clients the choice of following a departing representative to a new firm, while requiring firms to safeguard more sensitive client information. The proposed exception would not, however, affect firm policies that prohibit the transfer of any customer information other than at the customer's specific direction.

Practical Effect of Changes if Adopted

If these proposed significant changes are adopted, it would become important for a Covered Institution to review its policies and procedures to determine if they address all of the issues under the revised rules, including, but not limited to, responding to data breaches, maintaining proper records, designating and training appropriate staff, and allocating sufficient resources in order to carry out a comprehensive information security program. If a Covered Institution's policies and procedures are not sufficient under such revised rules, then changes to the policies and procedures should be drafted and implemented as soon as possible, so that they are in effect by the time any revised rules become effective. The deadline for receipt of comments on the proposal is May 12, 2008.

---

[10] The Covered Institutions would maintain these records for time periods specified in the existing record-keeping rules applying to the particular institution.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Martin R. Miller (212-728-8690, mmiller@willkie.com), Daniel Schloendorn (212-728-8265, dschloendorn@willkie.com), Francis Buono (202-303-1104, fbuono@willkie.com), Benjamin Haskin (202-303-1124, bhaskin@willkie.com), Rita M. Molesworth (212-728-8727, rmolesworth@willkie.com), or the attorney with whom you regularly work.

This memorandum was authored by Martin R. Miller and Marc J. Lederer.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

March 18, 2008