WILMERHALE

SEC Proposal for Better Safeguarding Personal Information: Easier Said Than Done?

2008-04-11

In response to the growing number of data breaches in recent years, the Securities and Exchange Commission (Commission or SEC) has recently proposed to improve the safeguarding of information by amending Regulation S-P.[i] Initially adopted in 2000, Regulation S-P currently applies privacy, information safeguarding, and disposal obligations to financial institutions, including broker-dealers.[ii]

The Release contains four primary amendments to Regulation S-P: (i) an obligation to create specific and tailored standards for compliance with safeguarding rules; (ii) a change in the type of information covered under safeguards and disposal rules and a broader scope of institutions and persons covered by the rule; (iii) an obligation for subject institutions to document their safeguards and disposal policies and procedures and their compliance with such policies and procedures; and (iv) an exception from Regulation S-P's notice and opt-out requirements to allow existing clients to more easily follow registered representatives when they move to a new firm. If adopted in their current form, the proposed amendments would significantly impact procedures and controls that broker-dealers have in place today, including those governing privacy of customer information, record retention, remote supervision, and recruiting.

This newsletter identifies key open issues that broker-dealers and their privacy and information technology officers must consider. In particular, we discuss the interplay between the SEC's proposal and various state consumer protection laws and regulations. The Release represents an important opportunity for broker-dealers and other financial institutions to help shape the ongoing policy debate in this area. **Comments must be submitted to the SEC by May 12, 2008.**

Safeguarding Policies and Procedures

As originally adopted, Regulation S-P required firms to adopt policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information. The Commission now proposes to require broker-dealers to develop, implement, and maintain a comprehensive "information security program" that includes the existing safeguard requirements under the Gramm-Leach-Bliley Act (GLBA) and would include an obligation to establish policies and procedures that address how the firm will respond to unauthorized access to or use of personal

information.

The proposed amendments specify particular elements that must be part of this program, including an obligation to establish the following in writing: identification of an employee(s) to coordinate the security program; identification and documentation of reasonably foreseeable security risks and implementation of safeguards to control the identified risks; regular testing or other monitoring of the program's effectiveness; training of staff to implement the program; oversight of third-party service providers (which may include affiliates); and evaluation and adjustments of the program in response to testing results and technological changes.[iii]

Potential comment topics:

- The SEC has solicited comments on whether covered institutions should be required to include in their information security programs "red flag" elements that would be relevant to detecting, preventing, and mitigating identity theft. However, since the SEC was not given authority to promulgate "red flag" rules under the Fair Credit Reporting Act, covered institutions may already be subject to the Federal Trade Commission's "red flag" rules. If so, this proposal may pose the risk that the FTC and SEC could impose inconsistent requirements.
- Supervising Service Providers:

    Do the proposed amendments impose unduly burdensome challenges when retaining offshore service providers?

    In the past, under certain circumstances, a function outsourced to a third-party service provider rendered the person performing that function an associated person by virtue of performing that function, thereby effectively negating any outsourcing because members are responsible for the supervision of all associated persons. How do these requirements relate to the proposed servicer supervision duties?

    If one affiliate acts as a service provider to multiple other affiliates, must each affiliate separately evaluate the service provider affiliate? Why not permit one affiliate subject to GLB the ability to evaluate the service provider affiliate on behalf of all affiliates

    Should clearer guidance be provided as to when to audit or obtain audit reports on service providers?

- The obligation to identify and report instances of unauthorized access or use of information to the Commission may duplicate Bank Secrecy Act reporting requirements. Should a simplified reporting mechanism be developed to address both Bank Secrecy Act and GLBA requirements?
- Should the SEC propose authentication standards on the Internet, such as multifactor authentication? Is there a risk that such static requirements in a regulation will not keep up with potential threats and changes in technology? Would it be preferable to establish performance standards instead?

Data Security Breach Response

Under the proposed amendments, firms would establish procedures for responding to incidents of potential unauthorized access to or use of personal information. This would include: (i) assessing information and systems that may have been compromised; (ii) containing and controlling the incident; (iii) conducting a reasonable investigation; and, (iv) notifying affected individuals if misuse has occurred or is reasonably possible.[iv] Additionally, firms would be required to provide notice to the Commission if an individual identified with information has suffered substantial harm or inconvenience or an unauthorized person has intentionally obtained access or used sensitive personal information.

Potential comment topics:

- Will the trigger for notifying the SEC lead to over-notification? There only needs to be a significant risk of "more than trivial financial loss" or even just an "expenditure of effort" or "loss of time" by the affected client.
- Is there also a potential for over-notification of clients? If misuse is "reasonably possible," notification must be provided. In practice, will firms conclude that almost anything is possible and err on the side of notification? Would "has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired" constitute a preferable standard?
- Should compromise of encrypted data or data otherwise not practicably readable be excluded from the breach notification trigger?
- Should notice only be required for compromise of electronic and not paper records?
- Over three dozen states have notification requirements, only some of which exclude entities subject to Reg. S-P. Is there a risk that double notification may be required where the required contents of the state and federal notices differ? Will the SEC try to coordinate reporting requirements with the states?

Broadened Applicability of Safeguards and Disposal Rules

Previously, the Commission adopted the safeguards and disposal rules at different times and under different statutes that varied in scope. The Commission proposes to amend Regulation S-P so that both safeguards and disposal rules would protect all information previously covered by either rule, referring to that information now as "personal information," which includes any record containing either non-public personal information or consumer report information. The proposed definition of personal information would include any information identified with any consumer or with any employee, investor, or security holder who is a natural person in paper, electronic, or other form that is handled by the institution or maintained on the institution's behalf, including user names and passwords.[v]

Additionally, the Commission proposes to expand the application of the disposal rules to transfer agents and to individuals associated with covered financial institutions.[vi] The Commission is concerned that natural persons associated with financial institutions are disposing of sensitive personal information in a manner inconsistent with the registered entity's disposal policies.

Proposed Definition of "Personal Information"

- What is the statutory authority to extend protections to employees who are neither customers nor necessarily the subjects of consumer reports?
- Will it be practical for firms to categorize the type of information that they possess and apply different protections?
- In a largely unprecedented step in the data security context, the Commission has proposed creating individual liability for violations by expanding the scope of the safeguard rules to associated persons of broker-dealers, supervised persons of investment advisers, and associated persons of transfer agents. Is this appropriate? Does the Commission have authority to impose such requirements on individuals?
- The Commission has sought input on extending disposal requirements to corporate as well as individual data. What are the burdens that would be associated with this?

Maintaining Records of Compliance

As proposed by the Release, broker-dealers would be required to document compliance with safeguards and disposal rules and maintain written records of related policies and procedures.[vii] Record retention requirements would be consistent with existing recordkeeping rules. For example, broker-dealers would have to preserve records for a period not less than three years, with the first two years in a readily accessible place.

Proposed Recordkeeping Requirements

- How will firms evidence compliance with policies and procedures?

Exception from Notice and Opt-Out Requirements to Allow Investors to Follow Representatives to New Firms

The Commission proposes an exception from the notice and opt-out requirements to facilitate the transfer of customer accounts when a representative moves to a new firm and provide structure to a process that representatives may use to try to retain existing clients when moving to a new firm.[viii] The exception permits limited information sharing that could be used by the new firm to contact existing clients of the transferring representative and offer a choice about whether to transfer their accounts to their representative's new firm. Shared information may not include any account numbers, Social Security numbers, or securities positions.

Broker-Dealers that allow representatives to rely on this exception would have to acquire, no later then when the representative terminates his employment, a written record of information that would be disclosed. Additionally, broker-dealers would be required to preserve such records.

Proposed Exception to Notice and Opt-Out Provision for Transferring Representatives

- Will broker-dealers that, during the recruiting process receive permissible information regarding a representative's book of business, be under an obligation to establish heightened policies and procedures to monitor for exchanges and switches? Should broker-dealers involve their compliance department in cases when portability of the

representative's book of business is likely to result in recommended switches and/or exchanges?

- Should all broker-dealers be required to offer their departing representatives the opportunity to take advantage of this exception to prevent firms from impeding the ability of representatives to move to new firms?
- Should safeguards requirements be imposed on the departing representative and the representative's new firm to protect information taken from the old firm and properly dispose of it?

CONCLUSION

If adopted, the proposed amendments to Regulation S-P would require a significant allocation of resources by broker-dealers and other financial institutions to review and revise their existing privacy and data security policies and procedures. Given the importance of these issues to the investing public, affected institutions should consider participating in the ongoing rulemaking process by voicing their views during the comment period.

---

[i] SEC Release Nos. 34-57427; IC-28178; IA-2712; File No. S7-06-08, 73 Fed. Reg. 13,692 (March 13, 2008) (Release).

[ii] Regulation S-P is codified at 17 C.F.R. Part 248.

[iii] Release, 73 Fed. Reg. at 13696.

[iv] Release, 73 Fed. Reg. at 13697.

[v] Release, 73 Fed. Reg. at 13700.

[vi] Release, 73 Fed. Reg. at 13701.

[vii] Release, 73 Fed. Reg. at 13702.

[viii] Release, 73 Fed. Reg. at 13702.