

Client Alert

An informational newsletter from Goodwin Procter LLP

SEC Proposes Expansion of Privacy Regulation

On March 4, 2008, the Securities and Exchange Commission announced proposed changes to Regulation S-P (“Reg S-P”) to address identity theft of securities industry customers. Reg S-P was adopted seven years ago under the Gramm-Leach-Bliley Act (“GLBA”) and the Fair Credit Reporting Act, and requires financial institutions under the authority of the SEC (including investment advisers, mutual funds, broker-dealers and SEC-registered transfer agents) to adopt policies and procedures to protect client information. The two requirements of Reg S-P relating to safeguarding and disposal of confidential information have not kept pace with bank and other regulators’ detailed programs for information privacy and data security.

The four proposed amendments to Reg S-P will require more comprehensive information security programs similar to the framework adopted by other financial institution regulators. Comments on the proposed amendments are due 60 days after publication in the Federal Register.

Safeguards Rule Strengthened. The first proposal creates more specific standards under the safeguards rule of Reg S-P, including physical, technical and administrative safeguards, written policies and required responses to data security breach incidents.

- While the current rule requires a financial institution in the securities industry to adopt its own policies and procedures to comply with the GLBA, the proposed amendment would require the financial institution to develop and execute a more detailed “information security program” similar to programs required by other federal regulators. The information security program must be in writing and must designate an employee in charge of information security, identify anticipated threats and implement controls to address those threats. The amendment, if adopted, would also require staff training, regular testing and coordination with service providers to maintain the program’s effectiveness.
- Subject to certain basic requirements, an individual financial institution’s information security program must be reasonably calculated to prevent the breach and misuse of client information that results in “substantial harm or inconvenience,” a term defined as “personal injury, or more than trivial financial loss, expenditure of effort or loss of time.” For example, according to the SEC, identify theft and extortion would likely cause “substantial harm or inconvenience,” while inadvertent misdelivery of an account statement would not.

- In an entirely new section of Reg S-P, a financial institution would need to notify the affected individual and, potentially, the SEC in the event of a data security breach. The financial institution must notify the affected individual when the institution becomes aware of unauthorized access to personal information and determines that misuse of personal information has occurred or is reasonably possible. This “risk of harm” standard is similar to that used in the guidance relating to customer notification of security breaches issued by the bank regulatory agencies. In contrast to the existing framework in the banking industry, however, which requires notice to banking regulators at a very low threshold, the SEC would require notification to the SEC only when the breach poses a significant risk of substantial harm or inconvenience to a consumer or when someone has intentionally obtained “sensitive personal information,” such as a social security number. Financial institutions must report the incident to the SEC on proposed Form SP-30. The proposed amendment also requires written procedures for responding to a data security breach.

Expanded Coverage of Reg S-P’s Scope. Secondly, the SEC proposes to broaden the type of information and persons covered by the SEC safeguards and disposal rules.

- Under the current rule, the types of information protected by the safeguards and disposal requirements of the rule differ slightly. The SEC proposes to have both rules protect “personal information,” which encompasses “nonpublic personal information” under the GLBA and “consumer report information” under the Fair and Accurate Credit Transactions Act of 2003. While “personal information” means personally identifiable financial information, “consumer report information” focuses on information generally contained in consumer reports.
- According to the SEC, in addition to nonpublic personal information and consumer report information of “consumers,” “personal information” also would include information identified with any employee, investor or security holder who is a natural person that is handled by the institution or maintained on the institution’s behalf. This broad proposal therefore covers employees rather than only clients of financial institutions, including employee user names and passwords, which, if compromised, could undermine the integrity of a financial institution’s information security system.
- The SEC safeguards rule would also apply to registered transfer agents in addition to the brokers, dealers, registered investment advisers, and investment companies. Notice-registered broker-dealers, already exempt from the SEC disposal rule, would be excluded from the safeguards rule as well.
- The SEC disposal rule would also apply to “natural persons who are associated persons of a broker or dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.”

The rule would continue to cover broker-dealers, investment companies, registered investment advisers and registered transfer agents.

Record-keeping. The third proposed amendment creates record-keeping requirements for policies and procedures to comply with the proposed regulation, as well as documentation of compliance.

Broker Mobility. Finally, the SEC proposes a fourth amendment to create a new exception allowing a broker who is changing firms to take limited personal information to the new firm in order to maintain relationships with clients.

State Law Compliance. Financial institutions subject to the bank regulatory agency guidance providing notice of a security breach under that standard are exempt from the requirements of several of the numerous state data security breach notice laws. Those financial institutions providing notice under the new SEC standard will now also be permitted under many state laws to provide notice to consumers under the federal standard rather than the different state standards.

If you have questions regarding the proposed amendments to Reg S-P, security breach notification requirements under federal and state law or any other privacy and data security topic, please contact:

Deborah S. Birnbach	dbirnbach@goodwinprocter.com	617.570.1339
Lynne B. Barr	lbarr@goodwinprocter.com	617.570.1610
Elizabeth Shea Fries	efries@goodwinprocter.com	617.570.1559
Agnes Bundy Scanlan	abundyscanlan@goodwinprocter.com	617.570.1161

Full access to all articles on privacy and data security prepared by Goodwin Procter is available [here](#).

Full access to all articles prepared by Goodwin Procter is available [here](#).

This publication, which may be considered advertising under the ethical rules of certain jurisdictions, is provided with the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin Procter LLP or its attorneys. Additionally, the foregoing discussion does not constitute tax advice. Any discussion of tax matters contained in this publication is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter. © 2008 Goodwin Procter LLP. All rights reserved.