

SUMMARY OF PROPOSED AMENDMENTS TO REGULATION S-P AFFECTING TRANSFER AGENTS

By **Laura S. Pruitt**

Background



*Laura S. Pruitt
Schiff Hardin LLP*

Pursuant to the Gramm-Leach-Bliley Act (“GLBA”), which was enacted in 1999, federal financial regulators, including the U.S. Securities and Exchange Commission (“SEC”), the U.S. federal banking agencies, and the Federal Trade Commission (“FTC”), were directed to issue regulations that protect the privacy interests of consumers of financial products and services. Among other things, those regulators were required

to establish standards to protect the security, confidentiality, and integrity of customer records and information.

In response to this mandate, the various regulators each adopted regulations for the handling and safeguarding of customer information. The SEC’s Safeguards Rule, 17 CFR § 248.30(a), was adopted as part of Regulation S-P in 2000. This Rule requires entities subject to the rule – which does not include transfer agents – to adopt policies and

procedures that address administrative, technical, and physical safeguards for the protection of customer records and information, and requires that the procedures be reasonably designed to (a) insure the security and confidentiality of customer records and information; (b) protect against any anticipated threats or hazards to the security and integrity of customer records and information; and (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Unlike the more comprehensive rules of the other financial regulators, the SEC’s current Safeguards Rule contains no specific program requirements. In 2004, the SEC added a “Disposal Rule,” which requires financial institutions subject to the Rule – including transfer agents – that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.³

Generally, each of the federal financial regulators’ rules have required the entities subject to the rules to protect and safeguard the confidential financial information of their “customers.”

(Continued on Page 5)

SUMMARY OF PROPOSED AMENDMENTS TO REGULATION S-P AFFECTING TRANSFER AGENTS

(Continued from Page 4)

A transfer agent's "customers" have traditionally been the issuers for whom they serve as agent, and, in connection with plan administration activities, the plans (and not the plan beneficiaries or participants). Depending on the services it provides, however, a transfer agent may have individual "customers" within the meaning of the various regulations. Whether or not an agent has been subject to the FTC's or banking regulators' rules, if the SEC adopts the amendments to Regulation S-P as proposed, all registered transfer agents will become subject to the SEC's Safeguards Rule, and they will have to protect the personal information of a much broader class of persons than just "customers."

The Current SEC Proposal

In an effort to help prevent identity theft of securities industry customers, particularly in light of well-publicized instances of securities firms losing data tapes and laptop computers containing sensitive information, failing to dispose of such information properly, and instances of hacking into customer accounts, on March 4, 2008, the SEC announced proposed changes to its Regulation S-P that would subject registered transfer agents to its Safeguards Rule requirements for the first time. According to the SEC, because registered transfer agents may maintain sensitive personal information about investors, the unauthorized access to or use of which could cause investors substantial inconvenience or harm, they must protect that information by maintaining appropriate safeguards and taking measures to properly dispose of such information.

Under the proposal, the Regulation S-P Safeguards Rule would be revised essentially to mirror (with some variations) the other financial regulators' current safeguarding requirements. Instead of the current general requirement that a financial institution adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information, the proposed rules would require each institution 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 the unauthorized access to or use of personal information. Specifically, the information security program must be reasonably designed to ensure the security and confidentiality of personal information, protect against any anticipated threats or hazards to the security and integrity of personal information, and 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.

Among other things, the rule will require firms to:

- designate an employee or employees to coordinate the information security program;
- perform a written risk assessment and design the program to control the identified risks;
- regularly test and monitor the effectiveness of the

(Continued on Page 6)

From the Editor

Here is a question for our members. Are you taking full benefit of your STA membership? From some of the questions I have received recently, I thought it might be helpful to point out some underutilized features of our website.

Have you looked at the Members Only Section of the site? In this section, you can find past copies of the STA Newsletter and older archived documents. There is also a Personnel Resources section where the STA will post resumes of people seeking work in our industry who have been vouched for by a member.

Most people are aware that the STA Guidelines are available on the public portion of our site. But did you know that this invaluable reference contains a complete and updated table of the various states' requirements for tax waivers (Appendix VD)? Did you know that it also contains an entire section on Paperless Legals (Section 1.4) and a chart showing the levels of surety associated with the differing Medallion alpha prefixes (Appendix I-6)?

The STA continually strives to improve the value of services it provides to its members. To that end, we are presently reviewing and updating the Useful Industry Links section of the website. If readers have any suggestions for additions to this section, please let us know. You can contact me at cjones@stai.org or Carol Gaffney at cgaffney@stai.org. ■



Cynthia

SUMMARY OF PROPOSED AMENDMENTS TO REGULATION S-P AFFECTING TRANSFER AGENTS

(Continued from Page 5)

safeguards' key controls, systems and procedures, including the effectiveness of access controls on personal information systems and controls to detect, prevent and respond to attacks or intrusions by unauthorized persons;

- adjust those controls and procedures as appropriate in light of that testing and monitoring, as well as relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the institution knows or reasonably believes may have a material impact on the program;
- provide training to employees on the information security program; and
- ensure that service providers engaged by the firm have implemented and maintained appropriate safeguards for personal information the firm shares with those service providers.

Because of its concerns about the potential harm to individuals when a data security breach occurs, the SEC also proposed to require information security programs to include procedures for responding to incidents of unauthorized access to or use of personal information as follows:

- If a data security breach occurs, the proposal requires institutions to "take appropriate steps to contain and control the incident ... and maintain a written record of the steps [taken]" and to "conduct a reasonable investigation, determine the likelihood that the information has been or will be misused, and maintain a written record of [that] determination."
- A firm's procedures would have to include providing prompt notice to affected individuals if misuse of "**sensitive personal information**" has occurred or is reasonably possible, as well as providing prompt notice to the SEC if an individual has suffered "**substantial harm or inconvenience**" or an unauthorized person has intentionally obtained access to or used "sensitive personal information."
- The notice to the SEC would require the filing of a new proposed form, Form SP-30. Among other things, proposed Form SP-30 requires customer account losses, to the extent known, to be quantified.
- "Sensitive personal information" would be defined as "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 person'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." (Emphasis added.)

- "Substantial harm or inconvenience" would be defined as "**personal injury, or more than trivial financial loss, expenditure of effort or loss of time.**" It is intended to include harms other than just identity theft, such as extortion by a person who has gained unauthorized access to another's personal financial information, but is not intended to 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 the use of the information results in an institution deciding to change the individual's account number or password, or if the use was the result of an occasional delivery of the information to an incorrect address if the firm determines, promptly and in writing, that the information is highly unlikely to be misused.

In addition, the SEC's Disposal Rule would be expanded to cover, among others, associated persons of transfer agents. The basis for this proposed expansion is the SEC's concern that persons in branches distant from the agent's main office may not dispose of sensitive personal financial information properly. The amendment would make associated persons directly liable for properly disposing of personal information consistent with the policies of the transfer agent. In addition, covered institutions would be required to document in writing their proper disposal of personal information in compliance with their policies.

Comments on the Proposal

The SEC's proposal differs in some minor and some more significant ways from the current regulations of the FTC and the banking regulators. For example, under the proposal, information security programs would cover not only customers, but also "any consumer, employee, investor, or securityholder who is a natural person." This greatly expands the scope of the current Safeguards Rule, and some have argued that it goes beyond GLBA's statutory mandate. Similarly, the proposal would expand the scope of the information subject to the protections of the regulations from "customer information" to "personal information," which means "any record containing consumer report information, or nonpublic personal information." That broad definition is expanded further

(Continued on Page 7)

SUMMARY OF PROPOSED AMENDMENTS TO REGULATION S-P AFFECTING TRANSFER AGENTS

(Continued from Page 6)

through the data breach provisions' use of the term "sensitive personal information." Some commenters have argued that these definitions would mean that nearly all information a firm possesses relating to an individual would be considered "sensitive personal information." This in turn means that the notice provisions would be triggered when a firm believes misuse of any information about a customer or securityholder is possible, resulting in many more notices to those individuals.

In addition, the proposal defines "substantial harm and inconvenience" to include any "personal injury" and any "more than trivial" financial loss, expenditure of effort or loss of time. Commenters have argued that this definition is too broad – they argue that not all personal injuries are "substantial" and the term "more than trivial" is too vague, which will result in notice to the SEC of all breaches, no matter how small.

In its comment letter on the proposal, the STA essentially agreed with the SEC's expansion of the Safeguards Rule as proposed, but urged the SEC, in adopting a final rule, to retain the flexibility the proposed rule provides to transfer agents to use a risk-based approach to formulate and implement programs that fit their unique circumstances. For this reason, the STA also urged that the SEC avoid adopting more specific safeguards, such as multifactor authentication, or layered security for high risk transactions involving access to customer information or movement to third parties, or require specific procedures for so-called "red flags."

With respect to the proposed requirements relating to data security breaches, the STA objected to the requirement that a firm maintain a written record of steps taken to contain and control a breach incident and maintain a written record of any investigation of the incident on the grounds that they may require a waiver of the attorney-client and work-product privileges. It also objected to the requirement to quantify customer losses in Form SP-30, because the information is not likely to be available at the time the form is filed (i.e., "as soon as possible"), it would be burdensome for agents to collect and track the data, and this information is not required under the comparable regulations of the other federal financial regulators. Because this question would almost always be left blank by transfer agents submitting Form SP-30, the STA suggested removing this item from the Form.

In connection with the proposed requirements for notifying individuals of incidents of unauthorized use or access, the STA also noted that, under State laws, transfer agents are not owners of the personal data of shareholders, and shareholders are not "customers" of the agent. State laws generally require entities that do not

own personal data to notify the owner of the data (i.e., the issuer) of a breach concerning such data, and the owner is then required to notify affected individuals. As they would apply to transfer agents, therefore, the individual notification requirements are contrary to some State law requirements, and their application to transfer agents could result in duplicative notices to individuals, generating confusion and anxiety on the part of shareholders. Consequently, the STA proposed that the SEC provide an exception to the individual notification requirement if the issuer provides such notification or the issuer and the transfer agent provide a joint notification to an affected individual.

The comment period for this rule proposal ended on May 12, 2008. The SEC has received several hundred comment letters on its proposal, and the SEC staff is considering all of the comments received. The timing of any final action on the SEC proposals is unknown. ■

¹ Laura Pruitt is a partner in Schiff Hardin LLP's Securities and Futures Regulation Practice Group in the Firm's Washington, D.C. office. Ms. Pruitt can be reached by phone at (202) 778-6470 or by email at lp Pruitt@schiffhardin.com. This summary is not intended to be, and should not be construed as, legal advice.

² See SEC Release No. 34-42974 (June 22, 2000), 65 FR 40334 (June 29, 2000).

³ See 17 CFR §248.30(b), as adopted in SEC Release No. 34-50781 (Dec. 2, 2004), 69 FR 71322 (Dec. 8, 2004).

⁴ A "customer" is defined as a "consumer" (i.e., an individual who obtains or has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative) who has a "customer relationship" with a financial institution (i.e., a continuing relationship between a consumer and an institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes). An example of such a continuing relationship is where a consumer holds an investment product through the institution, such as when the institution acts as a custodian for securities.

⁵ See SEC Release No. 34-57427 (March 4, 2008), 73 FR 13692, 13709 (March 13, 2008).

⁶ A copy of the STA's comment letter can be accessed through the SEC's website at <http://www.sec.gov/comments/s7-06-08/s70608-34.pdf>.