NOVEMBER/DECEMBER 2009 Special Reprint

NSCP CURRENTS

A Publication of the NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Privacy Best Practices and Updates on Regulation S-P

by Michelle L. Jacko

Regulation S-P was adopted by the SEC in accordance with Title V of the Gramm-Leach-Bliley Act (the "GLB Act").[1] The GLB Act requires the SEC and other federal agencies to adopt rules relating to notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about its consumers.[2] The two primary rules under Regulation S-P are Rule 10 (the Disclosure Rule) and Rule 30 (the Safeguard Rule). Rule 10 limits the information about customers that may be disclosed by a financial institution to any non-affiliated third party unless the financial institution complies with the notice and opt out provisions of Regulation S-P and the customer has not opted out of the disclosure.[3] Rule 30 requires every broker, dealer, and investment company, and every SEC-registered investment adviser to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[4] Such safeguarding policies and procedures must be reasonably designed to: ensure that consumer records and information are kept secure and confidential; protect against anticipated threats or hazards to the security of such consumer records and information; and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience.[5]

Changes to Privacy Rules

Recently, the SEC has been considering amendments to Regulation S-P that will impact both of these rules, and consequently will affect the way firms manage nonpublic personal information about their customers. Although the proposed substantive revisions to Regulation S-P proposed in 2008 have not yet been adopted,[6] on November 16, 2009, the SEC, together with several other regulatory agencies, released the final version of a model privacy form that firms may rely on as a safe harbor to the notice, disclosure, and opt-out requirements of Subtitle A of Title V of the GLB Act.[7]

New Model Privacy Form

Section 503 of the GLB Act requires each financial institution to provide a notice of its privacy policies and practices to customers describing the financial institution's policies with respect to disclosing nonpublic personal information about a consumer to both affiliated and nonaffiliated third parties and must provide a reasonable opportunity to opt-out of certain disclosures to nonaffiliated third parties.[8] Under Regulation S-P, institutions regulated by the SEC are required to deliver, at the time a customer relationship is formed and annually thereafter, a clear and conspicuous notice that accurately reflects the firm's privacy policies and practices, and informs consumers of their right to opt-out of certain disclosures.[9] However, the notice provisions did not set forth any specific format or standardized wording for the required notices, resulting in notices that varied among financial institutions depending on their practices, many of which were long and not easily understood.[10]

Michelle Jacko *is Managing Partner at Jacko Law Group, PC ("JLG"). Michelle is also a Board Member of NSCP. JLG works extensively with investment advisers, broker-dealers, investment companies, hedge funds and banks on legal and regulatory compliance matters.*

The model forms are designed to meet the requirements of the GLB Act and are intended to be easier for consumers to understand. The new form can be used by financial institutions regulated by the SEC to satisfy their privacy notice obligations under the Investment Advisers Act of 1940 and Regulation S-P.

Importantly, the new model privacy form is designed to make it easier for consumers to more readily understand how financial institutions collect and share information about its consumers. To accomplish this, two versions of the model privacy notice form are provided for firms to use: one contains opt-out language, while the other does not. In either case, the model form is comprised of two pages, and may be printed on two sides of a single piece of paper. Page one includes background information, a disclosure table, and opt-out information, while page two provides additional explanatory information that is necessary to ensure all disclosure requirements of the GLB Act are met.[11]

Significantly, use of the model form is not required, but rather serves as a safe harbor that reflects the view of the regulators as to how content and form of privacy notices should be presented.[12] Some other important features of the model form noted in the adopting release include: a standardized format that allows consumers to compare information sharing practices of multiple financial institutions; utilization of a checklist approach that alerts consumers to when they can or cannot opt-out; a clear and conspicuous statement at the top of the form that discloses that the privacy notice is required by federal law; and a prohibition against including extraneous marketing-type information.[13]

If a financial institution elects to use the model form, it must determine whether or not its information-sharing practices require the use of the opt-out language. Accordingly, financial institutions should determine whether switching to the model form is the best format to use for its privacy notice and if so, which version of the model form is the best fit for their business model. If there is any uncertainty as to which model form to use, firms should seek the advice of legal counsel.

Other Proposed Amendments

On March 4, 2008, the SEC proposed changes to Regulation S-P, which addressed (in part) enhanced notification requirements for alleged Regulation S-P breaches and included a new exception to the notice and opt-out requirements to allow limited information sharing when representatives move from one firm to another.[14] These changes were not addressed in the most recent release, however, which was limited to a discussion of the final model privacy form. It therefore remains to be seen what effect any amendments to the substance of Regulation S-P will have on the use and applicability of the model form.

Recent SEC Enforcement Actions

In recent years, there has been an increase in SEC enforcement actions related to Regulation S-P. The following list represents some of the most noteworthy cases involving Regulation S-P, both historically and as of late. Because the SEC has not yet adopted its proposed revisions to Regulation S-P, we are left with analyzing trends of recent enforcement actions in order to understand the SEC's interpretation of Regulation S-P. A basic understanding of the facts surrounding the following administrative proceedings may help in the development of safeguards for your firm to consider.

• Next Financial Group, Inc. – Registered representatives were found to have aided and abetted the firm in violating Regulation S-P by taking clients' personal information when leaving the firm and not disclosing to customers that non-public personal information was being shared with nonaffiliated third parties.[15]

• LPL Financial Corporation – LPL was found to have (1) violated Rule 30 of Regulation S-P (the Safeguard Rule) by failing to have adequate safeguards in its online trading platform which resulted in a security breach; and (2) failed to have a customer information policy that adequately protected customer records and information.[16]

• Commonwealth Equity Services – Commonwealth was found to have violated Regulation S-P by its lack of security measures to protect nonpublic personal information about their customers. Specifically, customer information was left vulnerable to unauthorized access because Commonwealth only recommended—but did not require—that its registered representatives have anti-virus software on their computers.[17]

• Merriman Curhan Ford – The firm was held liable for the conduct of its associated persons

in disseminating confidential customer information to nonaffiliated parties.[18]

• SEC v. Sydney Mondschein – The firm was found to be liable for its registered representative's activities in violation of Regulation S-P by failing to disclose to customers that he intended to sell, and did sell, their confidential personal information to insurance agents.[19]

Privacy Best Practices

In order to help ensure your firm is in compliance with Regulation S-P, consider the following best practices. **Remember your Duty of Loyalty and Fiduciary Responsibilities to Consumers**. The SEC can determine that a firm's failure to protect their clients' confidential information is a breach of their fiduciary duties under the Investment Advisers Act of 1940 as well as Regulation S-P.

1. Always Provide a Privacy Notice to New Clients and Annually Thereafter. The Privacy Notice required by Regulation S-P must adequately describe the firm's privacy policies and the circumstances under which the firm shares of nonpublic personal information with nonaffiliated third parties. The notice must be given to clients at the commencement of the client relationship and on an annual basis thereafter.

2. Make Certain the Privacy Policy Includes "No Phishing" Language. Include procedures to confirm the identity of any individual requesting clients' confidential information.

3. Documentation. Always keep a record of your efforts to upholding your privacy policy and include internal testing results as well as other compliance related work.

4. Require Non-Disclosure Agreements for Third-Party Service Providers. If a third party could potentially have access to clients' confidential information, a Non Disclosure Agreement should be required.

5. Adhere to the Technological Requirements of the Privacy Policy. An IT consultant or an in-house IT administrator can design and test major components of your privacy procedures to ensure the security and reliability of the firm's safeguarding and disposal process.

6. Hold Annual Trainings on your Privacy Policy. Have each employee sign a statement indicating their participation in privacy training sessions and acknowledging that they have read and understand the firm's privacy policy, emphasizing the importance of keeping clients' confidential information secure.

If the 2008 proposed amendments, the series of SEC enforcement actions, and the release of the model privacy form are any indication of the regulatory attention given to protecting consumer information, there is no better time than now to review your firm's privacy policies. With the end of the year fast approaching, be sure to give adequate consideration to your firm's privacy practices and keep abreast of SEC developments, as further amendments are likely to come sooner than later.

1. Privacy of Consumer Financial Information (Regulation S–P), Exchange Act Release No. 34-42974, Advisers Act Release No. IA-1883, Investment Company Act Release No. IC-24543, 65 Fed. Reg.40334 (June 29, 2000).
2. 15 U.S.C. 6803(a).
3. 17 C.F.R. § 248.10.
4. *Id.* § 248.30.
5. *Id.*
6. *See* Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information, Exchange Act Release No. 34–57427; Investment Company Act Release No. IC–28178; Advisers Act Release No. IA–2712, 73 Fed. Reg. 13,692 (proposed Mar. 13, 2008) [hereinafter Proposing Release].
7. Final Model Privacy Form under the Gramm-Leach-Bliley Act, Exchange Act Release No. 34-61003, Advisers Act Release No. IA-2950, Investment Company Act Release No. IC 28-997, 74 Fed. Reg. 62,890 (Dec. 1, 2009), *available at* http://www.sec.gov/rules/final/2009/34-61003fr.pdf [hereinafter Final Model Privacy Form].
8. *See* 15 U.S.C. 6803.
9. *See* 17 C.F.R. Part 248A.
10. Final Model Privacy Form, *supra* note 7 at 62,892.
11. *Id.* at 62,891-92.
12. *Id.* at 62,907.
13. *Id.* at 62,891-92.
14. Proposing Release, *supra* note 6 at 13,693-94.
15. Next Financial Group, Inc., SEC File No. 3-12738 (June 18,2008), http://www.sec.gov/litigation/aljdec/2008/id349jtk.pdf.
16. LPL Financial Corp., SEC File No. 3-13181 (Sept. 11, 2008), http://www.sec.gov/litigation/admin/2008/34-58515.pdf.
17. Commonwealth Equity Services, LLP, SEC File No. 3-13631 (Sept. 29, 2009), http://www.sec.gov/litigation/admin/2009/34-60733.pdf.
18. Merriman Curhan Ford & Company, SEC File No. 3-13681 (Nov. 10, 2009), http://www.sec.gov/litigation/admin/2009/34-60976.pdf.
19. Sec. & Exch. Comm'n v. Mondschein, Civil Action No. C-07-6178 SI (N.D. Cal., Dec. 6, 2007). *See also* http://www.sec.gov/litigation/litreleases/2007/lr20386.htm

NSCP CURRENTS

is published by the
National Society of Compliance Professionals, Inc.
22 Kent Road, Cornwall Bridge, CT 06754
(860) 672-0843 / info@nscp.org

NSCP Board of Directors

Editor & Layout
Frederick D. Vorck, Jr.

Editor
Joan Hinchman