



## Risk Management Update November 2009

### FINAL MODEL PRIVACY FORM ADOPTED BY THE SEC & REGULATION S-P UPDATES

On November 16, 2009, the Securities and Exchange Commission (“SEC”), together with several other regulatory agencies, published amendments to privacy rules that require financial institutions to provide initial and annual privacy notices to their customers, as required by Subtitle A of Title V of the Gramm-Leach-Bliley Act (the “GLB Act”).<sup>1</sup> Importantly, the SEC adopted “a model privacy form that financial institutions may rely on as a safe harbor to provide disclosure under the privacy rules.”<sup>2</sup> The model forms are designed to meet all the requirements of the GLB Act and are intended to be easier for consumers to understand.

#### *Background on Regulation S-P*

On November 13, 2000, the SEC adopted Regulation S-P in accordance with the GLB Act, which 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.”<sup>3</sup> Specifically, Rule 10 of Regulation S-P requires those financial institutions registered with the SEC to deliver a Privacy Notice to consumers providing important disclosures pertaining to:

- The firm’s privacy policies;
- The conditions in which the firm may disclose nonpublic personal information to nonaffiliated third-parties; and
- Methods in which the consumer has a reasonable opportunity to opt-out of the sharing of nonpublic personal information with such nonaffiliated parties.<sup>4</sup>

In addition, Rule 30 requires financial institutions to develop safeguards for consumer records and information. These policies and procedures must be reasonably designed to achieve the following objectives:

- Insure 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.<sup>5</sup>

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.<sup>6</sup> Notably, the most recent release does not address these areas, but rather, focuses exclusively on the Model Privacy Form.

#### *The New Model Form*

Under the GLB Act, institutions must notify consumers of their information-sharing practices and inform consumers of their right to opt out of certain sharing practices. The new model form can be used by financial institutions regulated by the SEC to satisfy their privacy notice obligations under the GLB Act and Regulation S-P. The form is designed to make it easier for consumers to

understand how financial institutions collect and share information about consumers. The model privacy notice form comes in two versions, one containing opt-out language in a section titled “to limit our sharing,” and another version without such opt-out language.

Use of this 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. Important features of the model form 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.

If a financial institution elects to use the Model Form, it must determine whether or not their 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.

### ***Recent SEC Enforcement Actions***

In recent years, there has been an increase in SEC enforcement actions related to Regulation S-P. For your quick reference, CCLS is providing some of the most noteworthy cases – both historically and as of late. We strongly recommend that you review the following administrative proceedings to be aware of safeguards for your firm to consider.

- Next Financial Group, Inc. – Registered representatives were found to aid and abet the firm in violating Regulation S-P by taking clients’ personal information when leaving the firm and not disclosing to customers that their non-public personal information, which was being shared with nonaffiliated third parties.<sup>7</sup>
- LPL Financial Corporation – The firm was found to (1) violate 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.<sup>8</sup>
- Commonwealth Equity Services – The firm was found to violate 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.<sup>9</sup>
- Merriman Curhan Ford – The firm was held liable for the conduct of its associated persons in disseminating confidential customer information to nonaffiliated parties.<sup>10</sup>
- SEC v. Sydney Mondschein – The firm was found to be liable for its registered representative’s activities in violation of Regulation S-P by his failing to disclose to his customers that he intended to sell, and did sell, their confidential personal information to insurance agents.<sup>11</sup>

### ***Privacy Best Practices***

In order to help ensure your firm is in compliance with Regulation S-P, consider the following best practices.

- 1. 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.
- 2. 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.
- 3. Make Certain the Privacy Policy Includes "No Phishing" Language.** Include procedures to confirm the identity of any individual requesting clients' confidential information.
- 4. 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.
- 5. 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.
- 6. 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.
- 7. 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 you have questions on Regulation S-P or this article, please contact us at (619) 278-0020. We are here to assist you with updating and authoring your privacy notice and related privacy policies as well as testing the efficacy of your Regulation S-P safeguards and controls.

For more information, or to learn about how CCLS may be of assistance, please do not hesitate to contact us at (619) 278-0020.

**Author: Michelle Jacko, CEO, Daneen Wolf, Compliance Analyst, Zachary Rosenberg, Legal Assistant; Editors: Michelle L. Jacko, CEO, Compliance Consultant, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues. For more information about this topic and other compliance consultation services, please contact us at (619) 278-0020, [info@corecls.com](mailto:info@corecls.com) or visit [www.corecls.com](http://www.corecls.com).**

*This article is for information purposes and does not contain or convey legal or tax advice. The information herein should not be relied upon in regard to any particular facts or circumstances without first consulting with a lawyer and/or tax professional.*

---

1 See 17 C.F.R. Part 248A (2009).

2 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 at 2 (Nov. 16, 2009), available at <http://www.sec.gov/rules/final/2009/34-61003.pdf>.

3 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).

4 17 C.F.R. § 248.10 (2009).

5 *Id.* § 248.30.

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. 13692 (proposed Mar. 13, 2008). For more information, see [http://www.corecls.com/files/CCLS\\_Risk\\_Management\\_Update\\_05.2008\\_-\\_Newly\\_Proposed\\_Changes\\_To\\_Regulation\\_S-P.pdf](http://www.corecls.com/files/CCLS_Risk_Management_Update_05.2008_-_Newly_Proposed_Changes_To_Regulation_S-P.pdf).

7 Next Financial Group, Inc., SEC File No. 3-12738 (June 18,2008), <http://www.sec.gov/litigation/aljdec/2008/id349jtk.pdf>.

8 LPL Financial Corp., SEC File No. 3-13181 (Sept. 11, 2008), <http://www.sec.gov/litigation/admin/2008/34-58515.pdf>.

9 Commonwealth Equity Services, LLP, SEC File No. 3-13631 (Sept. 29, 2009), <http://www.sec.gov/litigation/admin/2009/34-60733.pdf>.

10 Merriman Curhan Ford & Company, SEC File No. 3-13681 (Nov. 10, 2009), <http://www.sec.gov/litigation/admin/2009/34-60976.pdf>.

11 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>