

## Compliance Review

Ongoing Compliance Updates for Investment Advisors

### IN THIS ISSUE

Regulation S-P Compliance Tips .....	1	Regulation S-P Proposed Rule Change .....	3
--------------------------------------	---	---	---

## Regulation S-P: Now More Important Than Ever

By Todd E. Schwartz

July 1, 2007, marked the six-year anniversary of the Securities and Exchange Commission's (SEC) adoption of Regulation S-P. Regulation S-P requires SEC-level investment advisory firms ("firms") to implement privacy policies to protect their clients' "non-public financial information."<sup>1</sup> Additionally, the regulation requires firms to give clients a privacy notice when they first engage the firm and annually thereafter. Finally, under certain circumstances, Regulation S-P requires firms to give clients an opportunity to opt out of disclosures described in the privacy notice. State-based investment advisory firms are held to essentially the same standards by regulations adopted by the Federal Trade Commission.

Privacy policies, or the lack thereof, have become a common area of deficiency detected during SEC examinations. Adding further gravity to the six-year anniversary of Regulation S-P, the SEC is currently engaged in an investigation which may result in the first enforcement action involving a violation of Regulation S-P.<sup>2</sup> Simultaneously, the SEC and other federal agencies have proposed a rule ("Proposed Model Privacy Form Rule") which, if implemented,

would have a significant impact on investment advisory firms' current privacy policies.

This article provides tips to bolster your firm's current privacy policy and ensure your firm is in compliance with Regulation S-P. Finally, this article summarizes a Proposed Model Privacy Form Rule that could be problematic for all firms, but particularly for those firms using language in their privacy notices from Regulation S-P's current sample clauses.<sup>3</sup>

### Tips

- **Ensure your privacy policy is in writing and is being used on a consistent basis.** Written policies do little or no good, and can be the cause of great harm, if they are ignored. Do not place yourself in a position where an SEC examiner dusts off your privacy policy and proceeds to use it against you. In a worst-case scenario, the SEC could find that your firm's failure to protect your clients' confidential information is a breach of your fiduciary duties.
- **Do not mistake your privacy notice for your privacy policy.** A privacy notice must be provided

to clients upon initial engagement and annually thereafter. A privacy policy is a stand-alone internal document providing a methodology for keeping confidential client information secure. Both the privacy notice and privacy policy are required under Regulation S-P.

- **Always leave a paper/electronic trail.** Compliance is 99% documentation. As your firm upholds the requirements of your privacy policy throughout the year, be sure to keep electronic or paper records of your efforts. For instance, a privacy policy should include certain internal testing requirements to ensure clients' confidential information is truly safe. At a minimum, create a privacy policy file and write a memo to the file describing the manner of testing performed, as well as the testing results (including successes and any corrective actions taken). Document other compliance-related work in the same manner. Documentation will also ease the task of writing the annual compliance report required under SEC regulations.

- **Require certain third-party service providers potentially having access to clients' confidential information to sign a non-disclosure agreement.**

Note that non-disclosure agreements should be considered even where direct access to confidential information is not contemplated. If the third party *could* access the information, whether in good faith or bad, a non-disclosure agreement should be required. Examples of third parties who should sign a non-disclosure agreement include, but are not limited to: 1) information technology (IT) consultants, 2) bookkeepers and 3) temporary workers. A confidentiality agreement would not normally be necessary with respect to a broker-dealer or bank custodian who is in contractual privity with clients, and also bound by Regulation S-P's requirements.

- **Use IT consultants to successfully implement and maintain your privacy policy.** Many investment advisory firms do not have the in-house

technological expertise to properly implement a privacy policy. Consider hiring an IT consultant to do the heavy lifting related to the technological requirements of your privacy policy. An IT consultant can design and test major components of your policy. For instance, an IT consultant can set up your Internet firewall and conduct annual tests (which should be documented and placed in the privacy policy file, as discussed above) to confirm the invulnerability of your firewall to hackers. The same process should take place regarding your data back-up and recovery system and password-protection practices.

- **Include no-phishing language in your privacy policy.** "Phishing" is the illegal attempt to trick consumers into providing personal, confidential or financial information, including account numbers, passwords and Social Security numbers. Phishing is becoming more common.<sup>4</sup> Phishing might include, for example, sending an email to a user falsely claiming to be a person of authority in an attempt to deceive the user into surrendering confidential information that will be used for identity theft. In the good old days, bad guys would typically attempt to scam you in person. Nowadays, incidents involving personalized swindling seem less frequent. Today the instruments of choice are the telephone, the Internet (including fraudulent websites) and email. Ensure your privacy policy includes procedures to confirm the identity of any individuals requesting clients' confidential information. Most firms require a request for confidential information by a third party to be escalated and authorized by the firm's chief compliance officer (CCO).

- **Turn your weaknesses into strengths.** If there are any problems or vulnerabilities discovered relating to your firm's privacy policy, describe the problem in writing and state how the issue was remedied. Documentation of your firm's successful resolution of compliance problems will greatly

increase your firm's credibility in the eyes of the SEC. Advisors should be aware that lack of documentation, or 100% positive documentation, will only increase SEC scrutiny.

- **Conduct privacy policy trainings.** Ideally, trainings related to protection of clients' confidential information should be conducted no less than annually. Conclude the training by asking each employee to sign a statement indicating that they participated in the training, have read and understand the firm's privacy policy, and appreciate the importance of keeping clients' confidential information secure and the consequences of failing to do so.

#### **Regulation S-P proposed rule change**

As mentioned above, on March 29, 2007, the SEC and other federal agencies responsible for enforcing the provisions of Regulation S-P issued proposed rule changes. The core of the proposed rule is the Proposed Model Privacy Form Rule.<sup>5</sup>

Under the Proposed Model Privacy Form Rule, investment advisory firms using the model privacy

form will be granted "safe harbor." In other words, firms using the model privacy form will be considered in compliance with the notice requirements of Regulation S-P. Under the current rules, firms are granted safe harbor if they use language included in sample clauses contained in the rules. However, this safe harbor might disappear if the Proposed Model Privacy Form Rule is enacted. If it is enacted as proposed, one year following the enactment, investment advisors formerly relying on the current sample clause language would lose the safe harbor protections offered by the current rules.<sup>6</sup>

If your firm has used the language from the sample clauses contained in the current rules, you are in danger of having the safe harbor rug pulled out from under you. CCOs should closely monitor the Proposed Model Privacy Form Rule. If it is adopted as proposed, a complete overhaul of your privacy notice will be required. Because of other changes to the current rules, such an overhaul will also likely be necessary for investment advisory firms which chose not to use the sample clause language.

#### **About the Author**

Todd E. Schwartz is a partner in Carr Schwartz Butterfield, LLC, a law firm specializing in regulatory and compliance issues facing registered investment advisors. Mr. Schwartz has years of experience providing ongoing compliance and legal services to a national clientele of investment advisory firms. Mr. Schwartz regularly advocates for his clients during SEC examinations and state audits. For more information, visit [www.csb-llc.com](http://www.csb-llc.com), or contact Todd E. Schwartz by email at [tschwartz@csb-llc.com](mailto:tschwartz@csb-llc.com) or by phone at 1-866-730-5244.

---

### Compliance Resources on [www.schwabinstitutional.com](http://www.schwabinstitutional.com)

Visit the compliance site on [www.schwabinstitutional.com](http://www.schwabinstitutional.com) for compliance and regulatory information and solutions. Schwab works with third-party firms to provide select resources that help keep you informed of certain regulatory and compliance developments. The site features Compliance Hot Topics, Templates and Guideline Documents, a Rulemaking Calendar, archived issues of *Compliance Review*, Third-Party Resources and Discounts. As a unique resource, this single-destination compliance site is complimentary and exclusive to advisors who work with Schwab Institutional®

Visit [www.schwabinstitutional.com](http://www.schwabinstitutional.com) > **Resource Center** > **Compliance** today!

---

<sup>1</sup> For the purposes of this article, "non-public financial information" means sensitive information reasonable individuals would consider confidential.

<sup>2</sup> NEXT Financial Group, an independent broker-dealer, has confirmed it is currently the subject of an SEC investigation in a surprising context. Allegedly, Regulation S-P was violated when NEXT hired a registered representative from another broker-dealer who intended to use confidential client information from his or her former broker-dealer firm to generate new business at NEXT. See Financial Services Institute's SEC comment letter, May 29, 2007, at <http://sec.gov/comments/s7-09-07/s70907-14.pdf>.

<sup>3</sup> See "The Interagency Proposed Rule for Model Privacy Form Under the Gramm-Leach-Bliley Act," SEC Rel. No. 34-55497, IA-2598, IC-27755, File No. S7-09-07, available at <http://sec.gov/rules/proposed/2007/34-55497.pdf>.

<sup>4</sup> In May 2007, the SEC issued a release stating that individuals had contacted firms by phone, identified themselves as SEC staff and demanded immediate access to confidential records. The SEC's warning about the imposters is available at [www.sec.gov/about/offices/ocie/imposteralert.htm](http://www.sec.gov/about/offices/ocie/imposteralert.htm).

<sup>5</sup> See above, footnote 3.

<sup>6</sup> The Proposed Model Privacy Form Rule, which is apparently intended to simplify the privacy notice requirements under Regulation S-P, poses a number of other potential problems for investment advisory firms. For an excellent discussion of these issues, see the Financial Services Institute's SEC comment letter, May 29, 2007, at <http://sec.gov/comments/s7-09-07/s70907-14.pdf>.

The information available through the compliance resources page of the Schwab Institutional website is for general information only, and is not intended to provide specific compliance, regulatory or legal advice. For further information, contact your legal and/or compliance counsel.

The services and opinions of the authors are independent of Charles Schwab & Co., Inc. Neither the author nor his firm is affiliated with or an employee of Schwab. The articles and opinions in this publication are for general information only, and are not intended to provide specific compliance, regulatory or legal advice. Schwab makes no representations about the accuracy of the information in the publication or its appropriateness for any given situation. For further information, please contact your legal and/or compliance counsel.

©2007 Charles Schwab & Co., Inc. All rights reserved. Member SIPC.  
Schwab Institutional is a division of Charles Schwab & Co., Inc. FTA 03809 (0807-1092) NWS15120AUG07 (08/07)