Schulte Roth&Zabel

Alert

Reminder for Fund Managers on the November 20 Identity Theft Red Flags Rules Deadline

November 6, 2013

On April 10, 2013, the U.S. Securities and Exchange Commission and the Commodity Futures Trading Commission approved joint final identity theft rules, codified as Regulation S-ID ("Identity Theft Red Flags") by the SEC and as new subpart C ("Identity Theft Red Flags") to Part 162 by the CFTC.[1] Managers registered with the SEC or the CFTC must make determinations of coverage (and may have to implement responsive policies) by Nov. 20, 2013.

Are You Covered?
Whether a manager is covered by these SEC and CFTC Red Flags Rules — and what the manager's obligations are under those rules — depends in large part on the answers to two questions:

1. Whether the manager would be categorized as a "financial institution" or a "creditor"[2] under the Red Flags Rules and, if so,
2. Whether the manager holds "covered accounts."

Financial Institution Determination. A "financial institution" is a person that offers and maintains "transaction accounts" (i.e., accounts that permit withdrawals for the purpose of making payments or transfers to third persons) for "consumers" (i.e., natural persons). In issuing the Red Flags Rules, the regulators expressly directed private fund managers to review whether they are covered financial institutions; the adopting release states that if a registered investment adviser to a private fund "has the authority . . . to direct [redemption proceeds] . . . to third parties, then that adviser would indirectly hold a transaction account."

Following the issuance of the final rule text, a number of managers initially determined that they were not covered by the rule because their managed accounts and fund interests do not constitute transaction accounts. This initial conclusion was often supported by the general prohibition against sending redemption proceeds to a person or account not reflected on the subscription agreement or a similar document. However, many of these managers subsequently concluded that they would likely permit transactions to accommodate investors' estate planning, charitable giving, and other requests and that those transactions could cause a fund interest to fall within the definition of "transaction account."

[1] The SEC and the CFTC were mandated to issue identity theft regulations by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which transferred identity theft rulemaking responsibility and enforcement authority over registered investment advisers and commodity pool operators (and commodity trading advisors) to the SEC and CFTC. Prior to Dodd-Frank's amendment of the Fair Credit Reporting Act, identity theft regulatory responsibility for these entities resided with the Federal Trade Commission.

[2] In our experience, few managers have satisfied the definition of a "creditor" (i.e., a person that "regularly extends, renews or continues credit . . . [and] advances funds to or on behalf of a person . . .") with respect to its advisory clients and investors.

Covered Account Determination. Managers that may qualify as covered financial institutions and that have natural persons as clients or investors in funds that they manage would have obligations under the Red Flags Rules if they maintain "covered accounts" (i.e., accounts primarily for personal, family or household purposes that permit multiple payments or transactions or accounts for which there is a reasonably foreseeable risk of identity theft). Managers concluding that they are (or might be) financial institutions generally have also concluded that the private fund interests that they directly or indirectly manage could satisfy at least one of the prongs of the covered account definition (and, therefore, that the manager may be covered by the Red Flags Rules).

What Obligations Do Covered Managers Have?
Managers covered by the Red Flags Rules have to design, adopt and manage an identity theft prevention program, which — among other things — must include policies and procedures designed to:

- Identify;
- Detect; and
- Respond appropriately to identity theft "red flags."

A covered manager also has an express obligation to actively administer, review and update the program. This would generally be expected to include training, periodic reviews and testing (all of which would generally be directed at the manager's personnel and at third-party service providers, such as administrators, who directly or indirectly participate in the identity theft prevention effort).

As with all compliance policies, a good identity theft prevention program will be tailored to the manager's specific business and the risks that it presents.

What Are My Next Steps?
Managers who have not adopted an identity theft prevention program should review their assumptions and confirm whether their initial conclusions are still valid. **All managers must either implement a prevention program (or confirm that they are exempt) by Nov. 20, 2013.**

For private fund managers, an important part of an identity theft prevention program will be clear communication with the administrator for any private funds. Managers should review the administrator's identity theft procedures (or get representations as to their key provisions and protections) and ensure that the administrator will not take any unilateral actions that would require further investigation or other actions under the manager's policies. For many managers, this means that they will require the administrator to agree not to take, *without the specific approval of the manager,* actions such as the following:

- Not to direct any redemption proceeds to an account not listed in the original subscription document;
- Not to change wire instructions;
- Not to partition, retitle, or otherwise change any indicia of ownership of an investment or account (including changes purportedly for estate planning and domestic relations reasons); or
- Not to consent to liens or control agreements being placed on an investment or account.

Our experience to date is that many managers already have arrangements in place with their administrators (albeit often informal and undocumented) that approximate these safeguards.

As a related matter, managers may also want to review, update or formalize their information security program in conjunction with the implementation of an identity theft prevention program.

What Resources Are Available?
SRZ's *Alert*, "Update on Privacy Requirements Affecting Private Investment Fund Managers" (published in 2010 prior to the Dodd-Frank changes), discusses much of the substance covered by the identity theft rules. The firm also conducted a webinar on May 14, 2013 regarding the rules. SRZ clients who were not able to log in to the webinar, or would like a refresher, can contact their SRZ attorney for access to a replay of the

webinar. SRZ also has a team of attorneys drawn from our investment management and bank regulatory practices available to assist clients on interpreting the Red Flags Rules and in designing, reviewing and applying responsive policies. Clients should feel free to contact their SRZ attorney or one of the authors of this *Alert* with any questions or requests for assistance.

Authored by Brian T. Daly, Marc E. Elovitz, Brad L. Caswell and Jessica Sklute.

New York
Schulte Roth & Zabel LLP
919 Third Avenue
New York, NY 10022
+1 212.756.2000
+1 212.593.5955 fax

Washington, DC
Schulte Roth & Zabel LLP
1152 Fifteenth Street, NW, Suite 850
Washington, DC 20005
+1 202.729.7470
+1 202.730.4520 fax

London
Schulte Roth & Zabel International LLP
Heathcoat House, 20 Savile Row
London W1S 3PR
+44 (0) 20 7081 8000
+44 (0) 20 7081 8010 fax

www.srz.com