



One Maritime Plaza ♦ Eighteenth Floor
San Francisco, California 94111-3598

September 26, 2013

VIA E-MAIL

To Our Investment Adviser Clients and Other Friends

Re: SEC and CFTC Identity Theft Regulations Action Items Before November 20, 2013

Earlier this year the CFTC and the SEC adopted identity theft rules and guidelines (the “Regulations”) that require certain CFTC and SEC regulated entities that offer or maintain accounts that are susceptible to identity theft to implement a red-flags program (a “Program”) designed to detect, prevent and mitigate identity theft. Advisers that are subject to the Regulations must comply by November 20, 2013.

Advisers that are not regulated by the CFTC or the SEC are subject to the Federal Trade Commission’s existing identity theft prevention rules, which are similar to the Regulations, but which lack clear compliance guidelines for advisers. Such advisers should consider whether it is appropriate to adopt identity theft policies and procedures that follow the compliance guidelines outlined below.

1. The Regulations.

The Regulations apply to an adviser only if:

- The adviser is an SEC-registered investment adviser or a CFTC-regulated entity, such as a commodity pool operator or commodity trading adviser (each, a “Covered Adviser”);
 - The Covered Adviser is a “Financial Institution” or “Creditor”; and
 - The Covered Adviser offers or maintains “Covered Accounts.”
- a. Financial Institution. The SEC included certain investment advisers in the definition of Financial Institution, reasoning that investment advisers can face identity theft risks similar to banks and other financial institutions. Each Covered Adviser should analyze the following factors to determine if it is a Financial Institution: (1) whether an investor or client can direct the payment of funds from its accounts to third parties, including in connection with any redemption or withdrawal; (2) whether the

Covered Adviser acts as an agent (for example, pursuant to a power of attorney in a fund's governing documents) to issue instructions, either directly or indirectly through a custodian, with respect to the client's or investor's account; and (3) whether the Covered Adviser can pay fund expenses and other third-party expenses from the investor's or client's account. If a Covered Adviser answers "yes" to any question above, it is likely a Financial Institution.

Covered Advisers that use qualified custodians are not excused from compliance with the Regulations. In the Regulations' adopting release, the SEC noted that, even if a qualified custodian holds a client's or investor's account, a Covered Adviser that has authority to direct the custodian to withdraw or transfer money pursuant to the client's or investor's instructions is still susceptible to identity theft and would be considered a Financial Institution.

A Covered Adviser that has authority only to deduct money from an investor's or client's account to cover its advisory fees is not a Financial Institution, however, because it is transferring money only to itself and identity theft is unlikely.

- b. Creditor. A Creditor is a person or entity who regularly extends, renews or continues credit. The SEC's definition covers brokers offering margin accounts, short selling services and securities lending services, but excludes any person or entity that indirectly extends credit or regularly borrows money from third-party credit providers. A Covered Adviser may be a Creditor if it allows an investor to participate in a fund before the investor's capital contribution payment clears.
- c. Covered Account. Any Covered Adviser that is a Financial Institution or Creditor must periodically assess whether it offers or maintains Covered Accounts. Practically, for Covered Advisers a "Covered Account" is any account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Covered Adviser from identity theft, including any material risk to the Covered Adviser's reputation or goodwill.

The assessment must consider how investors can open, access and close accounts, as well as any of the Covered Adviser's previous experiences with identity theft. Accounts in the names of funds and separately managed accounts will likely be considered Covered Accounts. While a Covered Adviser may assume that it does not offer Covered Accounts because its withdrawal and redemption processes limit the likelihood of identity theft, if such Covered Adviser experiences identity theft and does not have a Program in place, it may be difficult to establish that its accounts were not reasonably susceptible to identity theft.

- d. Compliance Program. A Covered Adviser that is subject to the Regulations must adopt and implement a Program that is designed, after taking into consideration the size, complexity and scope of the Covered Adviser's business, specifically to detect, prevent and mitigate the types of identity theft likely to affect the Covered Adviser.

Each Covered Adviser has flexibility to determine the types of red flags relevant to its business and the types of policies and procedures that will appropriately and effectively address those risks. All Programs, however, must contain policies and procedures that (i) identify relevant red flags that indicate the possibility of identity theft, (ii) help personnel detect such red flags in day-to-day operations, (iii) ensure appropriate responses to each detected red flag, and (iv) call for periodic review and update of the policies and procedures to address evolving risks. Covered Advisers are also required to oversee service provider arrangements through which any of the required elements of the Program are outsourced.

A Covered Adviser's board of directors, or, if there is no board, a designated senior management employee (such as the Chief Compliance Officer), must approve the Program in writing. The board of directors or senior management employee must be involved in the development, implementation and administration of the Program.

2. Compliance Steps Before November 20, 2013.

Covered Advisers that are subject to the Regulations must implement compliant Programs before November 20, 2013. The following are some practical steps that each Covered Adviser should consider taking:

- *Update Policies and Procedures to Include a Program* - Each Covered Adviser should review and update its policies and procedures to add identity theft policies and procedures that comply with the Regulations.
- *Train Personnel* - Each Covered Adviser should undertake and document appropriate training to ensure that personnel understand the applicable Regulations and are following the Covered Adviser's Program.
- *Ensure that Third-Party Service Providers Have Appropriate Programs* - A Covered Adviser that uses an administrator, custodian or other third-party service provider that handles redemption or withdrawal requests or other disbursements of funds must ensure that such provider has its own compliant Program. Covered Advisers should review and supplement their agreements with such providers to include representations regarding the providers' Programs. Each Covered Adviser should also review its fund offering and organizational documents, separate account agreements and third-party service contracts to determine whether it has the power to instruct any applicable third-party service provider regarding redemptions, withdrawals or transfers from Covered Accounts. Such powers may require both the Covered Adviser and its providers to have Programs.
- *Consider Revising Investor Withdrawal and Redemption Process* - Covered Advisers should consider (i) revising current withdrawal, redemption or disbursement procedures to delegate responsibility and authority for handling such requests to service providers that have compliant Programs, (ii) restructuring withdrawal and redemption request methods or practices to limit identity theft

risks, and (iii) revising subscription policies so that contributions are not credited to investors until their subscription payments clear. A Covered Adviser should also consider notifying investors that it will not facilitate, approve or otherwise handle any withdrawal or redemption request, and that such requests should be made directly and exclusively to the administrator, custodian or other appropriate service provider.

* * * * *

This letter only generally summarizes action items in preparation for the November 20, 2013, effective date for the Regulations, is not intended as specific or complete advice, and is subject to change as the industry develops best practices for compliance with the Regulations. For further assistance, including assistance updating your policies and procedures, please contact Doug Hammer, John Broadhurst, Geoff Haynes, Chris Rupright, Carolyn Reiser, Neil Koren, Jim Frolik, Christina Hamilton, Joan Grant, Ellyn Roberts, Anthony Caldwell or David Suozzi.

SHARTSIS FRIESE LLP