Riveles Law Group

SEC and CFTC Establish Identity Theft Detection Guidelines for Registered Entities

In an effort to reduce the ever-increasing threat of identity theft, the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") (together, the "Commissions") recently adopted the Identity Theft Red Flag Rule (or Regulation "S-ID"). Broadly speaking, S-ID requires entities regulated by the Commissions that maintain "transaction accounts" to develop and implement a written identity theft prevention program (a "program") designed to identify, detect and respond to red flags and mitigate identity theft.

A "transaction account" is defined as an "account on which the account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others." Examples of-regulated entities that maintain transaction accounts include a registered investment company that enables investors to make wire transfers to other parties or that offers check-writing privileges and an investment adviser that directly or indirectly holds transaction accounts and that is permitted to direct payments or transfers out of those accounts to third parties.

As far as the requirements of a program, S-ID is flexible by allowing each firm to design a program that is appropriate to its unique size, the nature and scope of its activities, and the complexity of the institution itself. The rules are designed to be scalable, by permitting a program to take into account the operations of smaller institutions. Each firm must establish effective detection methods and responses to red flags. A red flag is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." Rather than requiring specific policies or procedures to achieve that end, S-ID provides a set of elements that act as general guidelines, which are highlighted below.

- **Written Authorization**. Each program must be in writing and formally approved by a board of directors, designated senior management, or an appropriate committee
- **Senior Involvement**. The firm must involve the board of directors, senior management, or appropriate committee in the development, implementation and administration of the program. Further, a designated individual or committee must report to the board or other senior management at least annually to report compliance results and address any needed changes.
- **Staff Training**. There must be an affective staff-training program in place to implement the Program.
- **Relevant Red Flags**. The program must include reasonable policies and procedures to identify relevant red flags for the covered accounts that the financial institution or creditor offers or maintains.
- **Effective Detection**. There must be reasonable policies and procedures to detect the red flags that the Program incorporates. This element does not provide a specific method of detection. Instead, section III of the guidelines provides examples of various means to detect red flags.
- **Effective Response to Red Flags**. The program's policies and procedures must have reasonable methods to respond to any red flags that are detected. Section IV of the guidelines set out a list of aggravating factors and examples that a firm should consider in determining an appropriate response.

- **Period Review and Updating**. The program must have policies and procedures that periodically update the Program to reflect changes in risks of potential identify theft.
- **Ultimate Responsibility**. The firm must maintain effective oversight over and remain ultimately responsible for the program, even if it outsources any portion of it to an independent service provider.