COMPLIANCE UPDATE

Final Rule: Identity Theft Red Flags Rule (Reg S-ID)

Release Date: April 10, 2013
Effective Date: May 20, 2013
Compliance Date: November 20, 2013

The Securities and Exchange Commission (“SEC”) in conjunction with the Commodities Futures Trading Commission (“CFTC”) recently released final regulations known by the SEC as Regulation S-ID (“Reg S-ID”). Reg S-ID requires certain investment advisers, broker-dealers, investment companies and other entities subject to the Commissions’ enforcement authority to establish programs to address the risks of identity theft.

Who does Reg S-ID apply to?

There is a two-pronged test to determine whether a financial services entity needs to adopt an identity theft prevention program under Reg S-ID. The entity must assess (1) if it is a “financial institution” (defined as a bank, credit union, or any other person that, directly or indirectly, holds a transaction account belonging to...an individual consumer) or “creditor” (defined as a person that regularly extends, renews, or continues credits or arranges for or participates in the decision as an assignee of a creditor to extend, renew, or continue credit); and (2) if any of the accounts held by the entity are “covered accounts.”

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. A “covered account” is defined as an account that a financial institution offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions.

If an entity meets both prongs, then it will need to adopt a program. However, even if an entity only meets the first part of the test, it will still need to annually assess its accounts and relationships to determine whether it has covered accounts (and, if so, at that point adopt a program).

Can an RIA rely on the custody rule to determine whether it needs to comply with Reg S-ID?

No. The SEC has stated that even investment advisers who do not accept actual custody of their clients’ accounts will be subject to the new rule as “financial institutions” if they have the ability to direct transfers or payments to third parties from a client account, or if they act as agents on behalf of individual clients. So, if an investment adviser facilitates or directs bill payments for its clients or otherwise acts as their agent for financial purposes, the rules will likely apply whether or not the investment adviser otherwise has custody of client assets. For advisers to private funds, holding accounts could include directing investors’ proceeds from the private fund to third parties by arrangement (such as arrangements in the fund documents) or upon the investor’s instructions.

In order to confirm continuing compliance with Reg S-ID, an RIA should periodically assess the types of client accounts it offers, the methods used to open accounts, the methods used to provide access to its client accounts, and any past experiences with identity theft.
What does Reg S-ID require?

SEC and CFTC-regulated “financial institutions” or “creditors” that offer or maintain “covered accounts” must establish a red flags program designed to detect, prevent and mitigate identity theft of those accounts. A “red flag” is a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of red flags include: inconsistencies in personal identifying information, incomplete account opening information, changes in account usage, mail being returned as undeliverable although transactions continue, adding an authorized person to an account shortly after the account address has changed, and other suspicious activity or unusual use of a covered account.

Each firm’s program must address four elements as a part of the firm’s reasonable policies and procedures to: (1) identify relevant red flags; (2) detect red flags; (3) respond appropriately to any red flags detected to prevent and mitigate identity theft; and (4) periodically update the program to reflect changes in risks to customers and to the safety of the firm.

The rules require each affected adviser to develop a program that is appropriate to the adviser’s size, complexity, and nature and scope of its activities. The program could either be a standalone document or part of the adviser’s policies and procedures manual. The release of the rule offers guidance to assist advisers in crafting their red flags program, including suggestions for preventing and mitigating identity theft and assessing when the program should be updated.

For example, appropriate responses to red flags may include: (1) contacting the customer; (2) changing any passwords, security codes, or other security devices that permit access to a covered account; (3) re-opening a covered account with a new account number; (4) not opening a new covered account; (5) closing an existing covered account; (6) not attempting to collect on a covered account or not selling a covered account to a debt collector; and (7) notifying law enforcement.

Investment advisers with such a program must: (1) obtain approval of the initial written program from either the board of directors, an appropriate committee of the board of directors, or if the entity does not have a board, from a designated senior management employee; (2) involve the board of directors, an appropriate committee thereof, or a designated senior management person in the oversight, development, implementation, and administration of the program (the designated senior management employee may be the Chief Compliance Officer); and (3) train staff, as necessary, to effectively implement the program and exercise appropriate and effective oversight of service provider arrangements. Firms remain legally responsible for compliance with the rules, irrespective of whether they outsource their identify theft red flags detection, prevention, and mitigation operations to a service provider.

While there has been some debate as to whether certain investment advisers meet the definition of a financial institution and whether, therefore, those investment advisers are subject to the regulation, the practical and very present risks of identity theft for advisory clients suggests that investment advisers should seriously consider the appropriateness of adopting an identity theft prevention program.

The text of the rule release is available through the SEC’s website at https://www.sec.gov/rules/final/2013/34-69359.pdf. For further clarification on how these changes affect you or for assistance in complying with the new rule, please contact:

Advisor Solutions Group, Inc.
949.250.1855
info@advisorsolutionsgroup.com