HinckleyAllenSnyder LLP
ATTORNEYS AT LAW

UPDATE
April 2013

SECURITIES

SEC and CFTC Adopt Identity Theft Red Flag Rules

On April 10, 2013, the Securities and Exchange Commission (the "SEC") and the Commodity Futures Trading Commission (the "CFTC" and together with the SEC, the "Commissions") jointly adopted rules and guidelines that require certain entities subject to their enforcement authorities to develop compliance programs to protect investors from identity theft (the "Red Flag Rules"). These new rules implement certain requirements of the Dodd-Frank Wall Street Reform and Protection Act and are similar to existing identity theft rules enforced by the Federal Trade Commission and federal banking regulators.

The Red Flag Rules require financial institutions and creditors that hold certain "covered accounts" to develop and implement a written identity theft prevention program. The program must provide for identification and detection of and responses to patterns, practices, or specific activities - known as "red flags" - that could indicate identity theft.

The Red Flag Rules will become effective May 19, 2013, and **the compliance date is November 19, 2013.**

Covered Entities

The Red Flag Rules apply to "financial institutions"[1] and "creditors."[2] The entities regulated by the SEC that are most likely to be covered by the Rules are broker-dealers, investment companies, investment advisers, and any other entities that are registered or that are required to register under the Securities Exchange Act of 1934. The entities most likely to be covered within the CFTC's regulatory scope include futures commission merchants, retail foreign exchange dealers, commodity trading advisers, commodity pool operators, introducing brokers, swap dealers, and major swap participants.

Covered Accounts

Under the Red Flag Rules, a financial institution or creditor must establish a red flag program if it offers or maintains any "covered accounts." The Commissions define a covered account as (i) an account that is maintained primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, or (ii) any other account for which there is a reasonably foreseeable risk of identity theft.

Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this periodic determination, a covered entity must conduct a risk-assessment that considers (i) the methods it provides to open its accounts; (ii) the methods it provides to access its accounts; and (iii) its previous experience with identity theft. The Commissions recommend that a covered entity consider whether, for example, a reasonably foreseeable risk of identity theft exists in connection with accounts offered or maintained that may be opened or accessed remotely. The Commissions further instruct that covered entities with a history of identity theft factor such experiences into their risk assessment.

The Commissions acknowledge that certain covered entities may determine, after conducting a preliminary risk assessment, that they do not need to implement a red flag program because the accounts offered do not pose a reasonably foreseeable risk of identity theft. Alternatively, covered entities may determine that only a limited range of accounts present such a risk, and therefore may develop and implement a program applicable only to those accounts or types of accounts.

Elements of Identity Theft Prevention Program

The Red Flag Rules require a written program designed to detect, prevent and mitigate identity theft in connection with opening a covered account or any existing covered account. The Rules are intended to provide a covered entity with the flexibility to design and implement a program that is appropriate to its size and the nature of its business activities. Notwithstanding the foregoing, the program must include reasonable policies and procedures addressing the following four elements:

- Identification. Identification of relevant patterns, practices and specific forms of activity that signal possible identity theft. Categories of red flags that covered entities should consider including in their programs, as appropriate, include: alerts, notifications, or other warnings received from consumer reporting agencies or service providers; presentation of suspicious documents, such as documents that appear to have been altered or forged; presentation of suspicious personal identifying information, such as a suspicious address change; unusual use of, or other suspicious activity related to, a covered account; and notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.
- Detection. Detection of the red flags that the program incorporates. Such policies and procedures may include (i) obtaining identifying information about, and verifying the identity of, an individual opening a covered account; and (ii) authenticating customers, monitoring transactions and verifying the validity of change-of-address requests, in the case of existing covered accounts.
- Response. Provide an appropriate response to any red flags that are detected. This element incorporates the requirement that a covered entity assess whether detected red flags evidence a risk of identity theft and, if so, determine how to respond appropriately based on the degree of such risk.
- Review. Procedures to periodically update the program, and address new and evolving threats.

Importantly, an entity that initially determines that it does not need a red flag program must periodically reassess whether it must develop and implement one in light of changes in the accounts it offers or maintains.

An entity that outsources elements of its operations must still comply with the Red Flag Rules. Therefore, a program must specify how the covered entity will ensure and monitor compliance with the program by external service providers.

Program Administration

The program must be initially approved by the covered entity's board of directors, or an appropriate committee thereof, or by a senior-level manager in the event the entity does not have a board. The same party or parties must be involved in the ongoing oversight, development, implementation and administration of the program. Finally, the program must include appropriate staff training.

The Red Flag Rules do not prescribe the specific manner of effective oversight. As mentioned above, the Rules are intended to be flexible and to provide covered entities the ability to design programs that meet their specific needs and circumstances.

1. A financial institution is defined by reference to Section 603(t) of the Fair Credit Reporting Act. This Section defines a financial institution to include certain banks and credit unions and "any other person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer." The Commissions' guidance provides that investment advisors may be financial institutions subject to the Red Flag Rules to the extent that such advisors have the ability to direct transfers or payments from accounts belonging to individuals to third parties upon such individuals' instructions, or act as agents on behalf of individuals. However, an investment advisor is not considered to be holding an investment account (and therefore is not subject to the Red Flag Rules) solely because such advisor has the authority to withdraw money from an investor's account to pay such advisor's own advisory fees.

2. A creditor is defined by reference to the Equal Opportunity Credit Act (i.e., a person that regularly extends, renews or continues credit, or makes those arrangements).

LINKS OF INTEREST

Securities >
People >
Publications >
Our Services >

SHARE THIS PAGE

Our Firm · Our Practices · Our People · News & Events · Contact · Join Email · HASLAW.COM