Identity Theft Red Flag Rules

Identity theft has been defined as "The fraudulent acquisition and use of a person's private identifying information, usually for financial gain."

Recently, the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") adopted the Identity Theft Red Flag Rules ("Red Flag Rules"). The Red Flag Rules are the SEC and CFTC versions of the "Red Flags" rule that was adopted by the Federal Trade Commission ("FTC") and banking regulators in 2007 also known as the ("Joint Red Flag Rules"). The new Red Flag Rules in effect transfer jurisdiction from the FTC to the SEC and CFTC for all entities that are under their regulation.

Although the Red Flag Rules and the Joint Red Flag Rules are similar, many entities that may not have been subject to the Joint Red Flag Rules under the direction of the FTC will have to reevaluate their position under the new rule. Minimal changes are needed if entities are already in compliance with the Joint Red Flag Rules.

This article is intended to provide a summary of 1) important definitions; 2) who is subject to the Red Flag Rules; and 3) the required elements of a Red Flag Program if it applies to your firm.[1]

Important Definitions

The Red Flag Rules require a written identity theft prevention program (the "Program") designed to prevent, detect, and mitigate identity theft for certain "covered accounts". To determine if your firm is required to implement such a Program, you need to answer affirmatively two questions:

1. Are you a "financial institution" or "creditor", and
2. Do you offer or maintain "covered accounts"

If you answer yes to both questions, your firm is required to create and implement a written Program. If you only answer yes to the first question, you will need to regularly assess your business to identify if you offer covered accounts, which would fully subject you to the Rule.

To make this determination you must understand some key definitions:

What is a Financial Institution?
A financial institution is any entity or "certain banks and credit unions, and any other person that, directly or indirectly, holds a "transaction account" belonging to a consumer."[2]

What is a Transaction Account?
A transaction account is "a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders or withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third parties or others."[3]

What is a Creditor?
A creditor includes "any futures commission merchant, retail foreign exchange dealer, commodity trading adviser, commodity pool operator, introducing broker, swap dealer, or major swap participant that regularly extends, renews, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit."[4]

What is a Covered Account?
Covered account(s) include the following:

1. Any account(s) held by the financial institution that is used for personal, family, and household purposes. These account(s) are designed to allow multiple payments and transactions.
2. Any account(s) that poses a high risk of identity theft of a customer's personal information.

If you determine that your firm meets the definition of a financial institution or creditor, you need to determine if

[1] This article does not address the Red Flags Rule on CFTC firms.

[2] Defined in Section 19(b) of the Federal Reserve Act
[3] Defined in the Fair Credit Reporting Act
[4] Defined in Section 19(b) of the Federal Reserve Act

you offer or maintain a covered account, or if there is a foreseeable risk of identity theft that may exist in connection with accounts opened or maintained. This includes accounts that are opened through the internet or by telephone. You should periodically (i.e., at least annually or upon a business model change) conduct a risk assessment that includes the following:

1. the methods used to open accounts;
2. the methods used to access client accounts; and
3. your previous experience with identity theft.

Even if it is determined that there is no need to establish a Program, you must periodically reassess that decision. Firms should incorporate this assessment or review into their required reviews under 206(4)-7, 38a-1 and 3012, as applicable.

Who is Subject to the Rules

The SEC's adopting release includes the following examples of an SEC regulated entity that may fall under the definition of a "financial institution": [5]

1. 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;
2. a registered investment company that enables investors to make wire transfers to other parties or that offers check-writing privileges; and
3. a broker-dealer that offers custodial accounts;

For example, advisers who have the ability to direct transfers or payments from accounts belonging to individuals to third parties or who act as agents on behalf of the individuals who bear the risk of identity theft. If an adviser does not have a program in place to verify investors' identities and detect identity theft red flags, an imposter may deceive the adviser by posing as a client, or deceive the custodian by posing as the adviser.

Be careful, the definition of "transaction account" is so broad that it will encompass advisers even if they do not have custody of client assets. If your firm does have custody of client assets (e.g., trustee to client accounts), you will be subject to the full provisions of the Rule and need to create and implement a Program.

The SEC clearly states that even when an investor's assets are held with a qualified custodian, an adviser that has authority by power of attorney or otherwise, to withdraw money from the investor's account and direct payments to third parties according to the investor's instructions would hold a "transaction account." However, an adviser that only deducts advisory fees from an investor's account is not deemed to have a "transaction account" because the adviser does not have access or authority to transfer payments to third parties. To ensure your specific authority with your custodian, check your agreement – can the custodian accept your direction to move money from a client's account to a third party account without a Letter of Authorization ("LOA") from the client? Whose responsibility is it to verify the client's signature on a LOA?

Under certain circumstances, registered investment advisers to private funds may directly or indirectly hold a "transaction account." For example:

1. Directly - A private fund adviser would hold a transaction account if it has the authority to direct an investor's redemption proceeds to other persons upon instructions received from the investor.
2. Indirectly - An adviser to the fund has the authority, per an arrangement with the private fund or an investor, to direct the investment proceeds (e.g., redemptions, dividends, or other proceeds related to the individual's account) to third parties, then that adviser would indirectly hold a "transaction account".

[5] 17 CFR Part 248 Release Nos. 34-69359, IA-3582, IC-30456; File No. S7-02-12

Broker-dealers and entities that are already in compliance with the Joint Red Flag Rules should update their policies and procedures to reflect changes to rule citations. For example: changing rule citations from FTC to SEC.

The Program

The Red Flag Rules require a written identity theft prevention program ("Program") designed to prevent, detect, and mitigate identity theft for certain "covered accounts." At a minimum the Program should include the following:

1. Identification of the relevant and possible identity theft red flags;
2. Methods for detection of the occurrence of the red flags;
3. Methods for responding to any detected red flag; and
4. Periodic review and update of the program.

A "red flag" is an alert that some event his occurred that requires attention, perhaps a warning of a possible problem. This includes patterns, and activities that are out of the ordinary. For example, inconsistencies in personal identifying information, incomplete account opening information, changes in account information or usage, undeliverable mail for an active account, addition of authorized users after account opening, etc.

The Program should be tailored to cover the size, complexity, structure, activities, and service products of the business. In addition, the administration of the program should include appropriate service provider oversight, staff training, and must be approved by a member of senior management or the board of directors.

When is the Compliance Date?

Covered financial institutions and creditors that offer or maintain a "covered account" are to comply with the Identity Theft Red Flags Rule by **November 20, 2013.**

Conclusion

In summary, non-compliance with the Red Flag Rules will not only expose your firm to regulatory risk but also the very real business and reputational risk associated with identity theft. Entities that have already adopted the Joint Red Flag Rules under the direction of the FTC should review the Identity Theft Red Flag Rules and make any necessary changes to conform to the SEC requirements. Those who believe that they were not subject to the FTC Joint Red Flag Rules should reassess their business, client relationships, and accounts to determine if a Program should be established and implemented.

If you are unsure if you are subject to the rules, please contact us for a consultation.

By: Rayma A. Christy, CAMS, MAC
Article Date: July 29, 2013

Rayma A. Christy is a Compliance Consultant at Renaissance Regulatory Services, Inc., specializing in AML Program creation and testing, written supervisory policies and procedures, and FINRA/SEC compliance for broker-dealers, investment companies, and investment advisers.

Mrs. Christy can be reached in our main office or via email at raymachristy@rrscompliance.com.

Renaissance Regulatory Services, Inc.
Compliance Consultants
To Broker-Dealers and Investment Advisers
(561) 368–2245
350 Camino Gardens Blvd.
Suite 105
Boca Raton, FL 33432
www.RRSCompliance.com
Offices in:
Boca Raton, FL – Washington, DC