FIRE SOLUTIONS
FIRE On Your Side
A monthly newsletter of industry developments and trends

Provided by FIRE Solutions Inc.

Identification of Red Flag Activities

Three opportunities to circumvent illegal activities in the life of a new account

A variety of red flags may arise during the life of an account. These red flags could be identified by the retail representative, the supervisor, or the operations department during three points in the life of a new account: 1) During the account opening process; 2) after the account is opened; and 3) when transactions are processed.

Not all red flags are reportable or cause for immediate concern, but you should make note of them and document your efforts to obtain a reasonable explanation for the activity, with notification to and under the guidance of your AML compliance officer.

❖ Red Flags During Account Opening

Red flags that may arise during the account opening process include:

- The customer wishes to invest in a product without concern for the risks or costs associated with it.
- The customer has no qualms about investing, yet lacks investment sophistication.
- The customer is evasive about disclosing the identity of other account owners.
- The customer is overly concerned about the firm's reporting requirements regarding deposits.
- A business customer is reluctant, when establishing a new account, to provide complete information about the nature and purpose of the business, anticipated account activity, prior banking relationships, the names of officers and directors, or information on the business location.
- A business customer is a trust, a shell company, or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- An unusual number of accounts are opened in the same name.

During the customer identification procedures (CIP) you find that:

- The customer uses unusual or suspicious identification documents that cannot be readily verified.
- The customer is unwilling to provide required information.
- Documentation for the account looks suspicious, or as if it came from a graphic design program.
- The customer provides an individual tax identification number after having previously used a Social Security number.
- The account owner (or its representative) is apprehensive or delays in providing required account documentation without an adequate explanation.
- Customers use different tax identification numbers with variations of their name.
- The customer's home or business telephone is disconnected.

- The customer's background differs from that which would be expected based on his or her business activities.
- The customer, or one of the beneficial owners of an account, appears on the FinCEN watch list.
- The customer lives in a restricted geographic area that appears on the FinCEN watch list.

❖ Red Flags After the Account Is Opened

In addition to monitoring client accounts and fulfilling fiduciary responsibilities, retail brokers and operations specialists should be alert to certain types of account activity that may arouse suspicion.

Red flags that may arise after the account is opened include:

- Wire transfers to/from countries on FinCEN's watch lists (e.g., Iran, Sudan, Burma, and Nigeria)
- Wire transfers to/from a financial secrecy haven (e.g., Gibraltar and Andorra)
- Wire transfers of a large size or with a pattern or frequency, particularly from foreign sources
- Wire transfer to multiple accounts
- Asset transfers/deposits into the account appear beyond the means of the client's resources or status
- Structuring of deposits or withdrawals in an attempt to evade currency transaction reporting requirements
- Inflow of money that appears beyond the means of the person's stated income
- Closing an account soon after opening
- Deposits of suspicious physical certificates

❖ Red Flag Transactions

As with the wire transfer activity mentioned above, specific transaction types have been identified as a high risk for money-laundering activities.

Transactions that may be considered red flags include:

- The customer makes a long-term investment, then shortly thereafter liquidates the transaction and transfers the money out.
- For no explainable reason, the customer wishes to invest in high-risk products such as penny stocks, Regulation S stocks, or bearer bonds.
- The customer trades just before newsbreaks about a firm, and especially when the news is impactful enough to move the stock's price.
- The customer engages in prearranged trading — coordinating the purchase/sale of a security with an associate(s) to manipulate the stock price. Be especially aware of such transactions in penny stocks (typical of "pump and dump" schemes).

- The customer engages in wash sales — the process of selling a stock at a loss in order to report the loss for tax purposes, then repurchasing the same or similar stock within 30 days.
- The customer engages in fictitious trading — parking securities and maintaining fictitious accounts to hold or hide securities in another person's or a fictitious account.

Maintaining effective anti-money laundering controls continues to be a top priority for FINRA. Financial services professionals must follow appropriate AML policies and procedures, adhere to regulatory reporting requirements, remain alert to possible suspicious activity, and understand the customer's motivations before opening new accounts. By doing so, they will be better equipped to recognize telltale symptoms related to money laundering and will be prepared to take the next step — reporting the activity to their supervisor or AML compliance officer.

Was this excerpt everything that you thought it would be? Are there *anti-money laundering* issues that FIRE could report on or investigate for you? FIRE wants to hear all feedback regarding this excerpt. Click here to let us know your thoughts.