Regulatory Notice 19-18

Anti-Money Laundering (AML) Program

FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations

May 6, 2019

Notice Type
- Guidance

Suggested Routing
- Compliance
- Legal
- Operations
- Senior Management

Key Topics
- Anti-Money Laundering
- Compliance Programs

Referenced Rules & Notices
- Bank Secrecy Act
- FINRA Rule 3310
- Notice to Members 02-21

Summary

FINRA is issuing this *Notice* to provide guidance to member firms regarding suspicious activity monitoring and reporting obligations under FINRA Rule 3310 (Anti-Money Laundering Compliance Program).

Questions concerning this *Notice* should be directed to:

- Victoria Crane, Associate General Counsel, Office of General Counsel, at (202) 728-8104 or *victoria.crane@finra.org*; or
- Blake Snyder, Senior Director, Member Regulation, at (561) 443-8051 or *blake.snyder@finra.org*.

Background and Discussion

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires each member firm to develop and implement a written anti-money laundering (AML) program reasonably designed to achieve and monitor the firm's compliance with the requirements of the Bank Secrecy Act (BSA),[1] and the implementing regulations promulgated thereunder by the Department of the Treasury (Treasury).

FINRA Rule 3310(a) requires firms to "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under [the BSA] and the implementing regulation thereunder." The BSA authorizes Treasury to require that financial institutions file suspicious activity reports (SARs).[2]

FINRA
Financial Industry Regulatory Authority

Under Treasury's SAR rule,[3] a broker-dealer must report a transaction to the Financial Crimes Enforcement Network (FinCEN) if it is conducted or attempted by, at or through a broker-dealer, it involves or aggregates funds or other assets of at least $5,000, and the broker-dealer knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA;
- has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- involves use of the broker-dealer to facilitate criminal activity.[4]

Broker-dealers must report the suspicious activity by completing a SAR and filing it in accordance with the requirements of Treasury's SAR rule.[5] Broker-dealers must maintain a copy of any SAR filed and supporting documentation for a period of five years from the date of filing the SAR.[6] FinCEN has provided guidance[7] to the industry advising that if the activity that was the subject of a SAR filing continues, firms should review any continuing activity at least every 90 days to consider whether a continuing activity SAR filing is warranted, with the filing deadline being 120 days after the date of the previously related SAR filing.

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers must immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR. The firm may call FinCEN's Hotline at (866) 556-3974.

Money Laundering Red Flags

FINRA published a list of "money laundering red flags" in *Notice to Members 02-21* (NTM 02-21). Since NTM 02-21 was published, guidance detailing additional red flags that may be applicable to the securities industry have been published by a number of U.S. government agencies and international organizations.[8] FINRA is issuing this *Notice* to provide examples of these additional money laundering red flags for firms to consider incorporating into their AML programs, as may be appropriate in implementing a risk-based approach to BSA/AML compliance. This could include, as applicable, incorporation into policies and procedures relating to suspicious activity monitoring or suspicious activity investigation

and SAR reporting. Upon detection of red flags through monitoring, firms should consider whether additional investigation, customer due diligence measures or a SAR filing may be warranted.

The following is not an exhaustive list and does not guarantee compliance with AML program requirements or provide a safe harbor from regulatory responsibility. Further, it is important to note that a red flag is not necessarily indicative of suspicious activity, and that not every item identified in this *Notice* will be relevant for every broker-dealer, every customer relationship or every business activity.

Firms should also be aware of emerging areas of risk, such as risks associated with activity in digital assets. Regardless of whether such assets are securities, BSA/AML requirements, including SAR filing requirements apply, and firms should thus consider the relevant risks, monitor for suspicious activity and, as applicable, report any such activity.

This *Notice* is intended to assist broker-dealers in complying with their existing obligations under BSA/AML requirements and does not create any new requirements or expectations. In addition, this *Notice* incorporates the red flags listed in NTM 02-21 so that firms can refer to this *Notice* only for examples of potential red flags.

I. Potential Red Flags in Customer Due Diligence and Interactions With Customers

1. The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
2. The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
3. The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
4. The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
5. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
6. The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).

7. The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
8. The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
9. The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
10. The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
11. The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
12. The customer's background is questionable or differs from expectations based on business activities.
13. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
14. An account is opened by a politically exposed person (PEP),[9] particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company[10] beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
15. An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.[11]
16. An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.[12]
17. An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
18. An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
19. An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

II. Potential Red Flags in Deposits of Securities

1. A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
2. A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
3. A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
   - were recently issued or represent a large percentage of the float for the security;
   - reference a company or customer name that has been changed or that does not match the name on the account;
   - were issued by a shell company;
   - were issued by a company that has no apparent business, revenues or products;
   - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
   - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
   - were issued by a company that has been the subject of a prior trading suspension; or
   - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.
4. The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.
5. A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.
6. The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.
7. The customer deposits physical securities or delivers in shares electronically, and within a short time-frame, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
8. Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

III. Potential Red Flags in Securities Trading[13]

1. The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
2. There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
3. The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.
4. A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.
5. Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.
6. A customer accumulates stock in small increments throughout the trading day to increase price.
7. A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.
8. A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.
9. A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.
10. A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of "spoofing").
11. A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of "layering").
12. Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.
13. The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

14. The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.
15. The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.
16. The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.
17. The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.
18. The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depository Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.
19. The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.
20. The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

IV. Potential Red Flags in Money Movements

1. The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
2. The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
3. The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
4. The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.

5. The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
6. The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
7. Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
8. Incoming payments are made by third-party checks or checks with multiple endorsements.
9. Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
10. Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
11. Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.
12. Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.
13. The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
14. The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
15. Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.
16. There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.
17. The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).
18. Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

19. The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.
20. The customer uses a personal/individual account for business purposes or vice versa.
21. A foreign import business with U.S. accounts receives payments from outside the area of its customer base.
22. There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
23. Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).
24. The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.
25. Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.
26. A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).
27. Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
28. There is unusually frequent domestic and international automated teller machine (ATM) activity.
29. A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.
30. Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.
31. Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

V. Potential Red Flags in Insurance Products

1. The customer cancels an insurance contract and directs that the funds be sent to a third party.
2. The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.
3. The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.
4. The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
5. The customer purchases an insurance product with no concern for the investment objective or performance.

VI. Other Potential Red Flags

1. The customer is reluctant to provide information needed to file reports to proceed with the transaction.
2. The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.
3. The customer tries to persuade an employee not to file required reports or not to maintain the required records.
4. Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
5. Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
6. The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
7. The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.
8. The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.
9. The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

10. The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.
11. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
12. The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).
13. A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
14. There is an unusual use of trust funds in business transactions or other financial activity.

Endnotes

1. 31 U.S.C. 5311, *et seq*.
2. *See* 31 U.S.C. 5318(g).
3. *See* 31 CFR 1023.320.
4. *See* 31 CFR 1023.320(a)(2).
5. *See* 31 CFR 1023.320.
6. *See* 31 CFR 1023.320(d).
7. *See* FinCEN SAR Activity Review Issue 21 (May 2012).
8. *See, e.g*, Financial Action Task Force (FATF), Guidance for a Risk-Based Approach for the Securities Sector, October 2018; FATF, Money Laundering and Terrorist Financing in the Securities Sector, October 2009; FATF, Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002; FATF Report, Laundering the Proceeds of Corruption, July 2011; FATF Report, Risk of Terrorist Abuse in Non-Profit Organisations, June 2014; FinCEN Advisory FIN-2010-A001: Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade Based Money Laundering, February 2010; U.S. Department of State, Money Laundering Methods, Trends and Typologies, March 2004; Securities and Exchange Commission (SEC) National Exam Risk Alert on Master/Sub-accounts, September 2011; SEC National Exam Risk Alert on Broker-Dealer Controls Regarding Customer Sales of Microcap Securities, October 2014; and SEC Responses to Frequently Asked Questions about a Broker-Dealer's Duties When Relying on the Securities Act Section 4(a)(4) Exemption to Execute Customer Orders, October 2014. *See also Regulatory Notices 09-05* (January 2009) and *10-18* (April 2010); and Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering, Money Laundering and Terrorist Financing "Red Flags."
9. A "Politically Exposed Person" is defined by FATF as an individual who is or has been entrusted with a prominent public function, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, or important political party officials. *See* FATF Guidance, Politically Exposed Persons, June 2013.
10. A "shell company" is an issuer of securities for which a registration statement has been filed with the SEC that has: (1) no or nominal operations; and (2) either: (i) no or nominal assets; (ii) assets consisting solely of cash and cash equivalents; or (iii) assets consisting of any amount of cash or cash equivalents and nominal other assets. *See* 17 CFR 230.504.
11. The FATF Report on Risk of Terrorist Abuse in Non-Profit Organisations (FATF Report), June 2014, defines "terrorist threat" as: A person or group of people, object or activity, with the potential to cause harm. Threat is contingent on actors that possess both the capability and intent to do harm.
12. The FATF Report defines "terrorist entity" as a terrorist and/or terrorist organization identified as a supporter of terrorism by national or international sanctions lists, or assessed by a jurisdiction as active in terrorist activity. *See id*.
13. These red flags could also be indicative of securities law violations.
14. Nostro accounts are accounts that a financial institution holds in a foreign currency in another bank, typically in order to facilitate foreign exchange transactions.