COMPLY ADVANTAGE®

ComplyAdvantage.com

A guide to

Anti-Money Laundering for US Broker-Dealers

Contents

Overview

Regulators and enforcement attorneys have targeted the effectiveness of AML programs as an area of ongoing regulatory concern. Even if a firm believes it is carrying out its AML program diligently and regulators have performed their annual review, regulators can take enforcement action if it looks again and finds deficiencies.

As Robert Warner, former OFAC and FinCEN director, stated in a talk at a virtual global AML roundtable on April 17, 2020:

> "...after the fact, regulators, historically, have shown the ability to time-travel and to tell the financial institutions they regulate...'your program was inadequate and it should have been better at the time and you should have known at the time.' And so, institutions should expect that they are going to have a retrospective view applied to everything that they do today that is going to be with 20/20 hindsight. And so... it has been my advice to my clients [to] put resources into... the personnel and the technology that you have, into executing these programs, but do not compromise your standards [and] well-known risk assessment and mitigation processes, because if you do, it's going to bite you in a year or two when everything is settled and all of the auditors come running in to look and see how these programs were executed.

Notice

This guide is intended to provide firms and their employees with practical advice to build an effective AML program or enhance an existing one, including policies and procedures for dealing with customer accounts and transactions. However, it is not an all-inclusive compendium of AML rules addressing every conceivable situation businesses may face while conducting business, nor is it a treatise on the field of AML regulation.

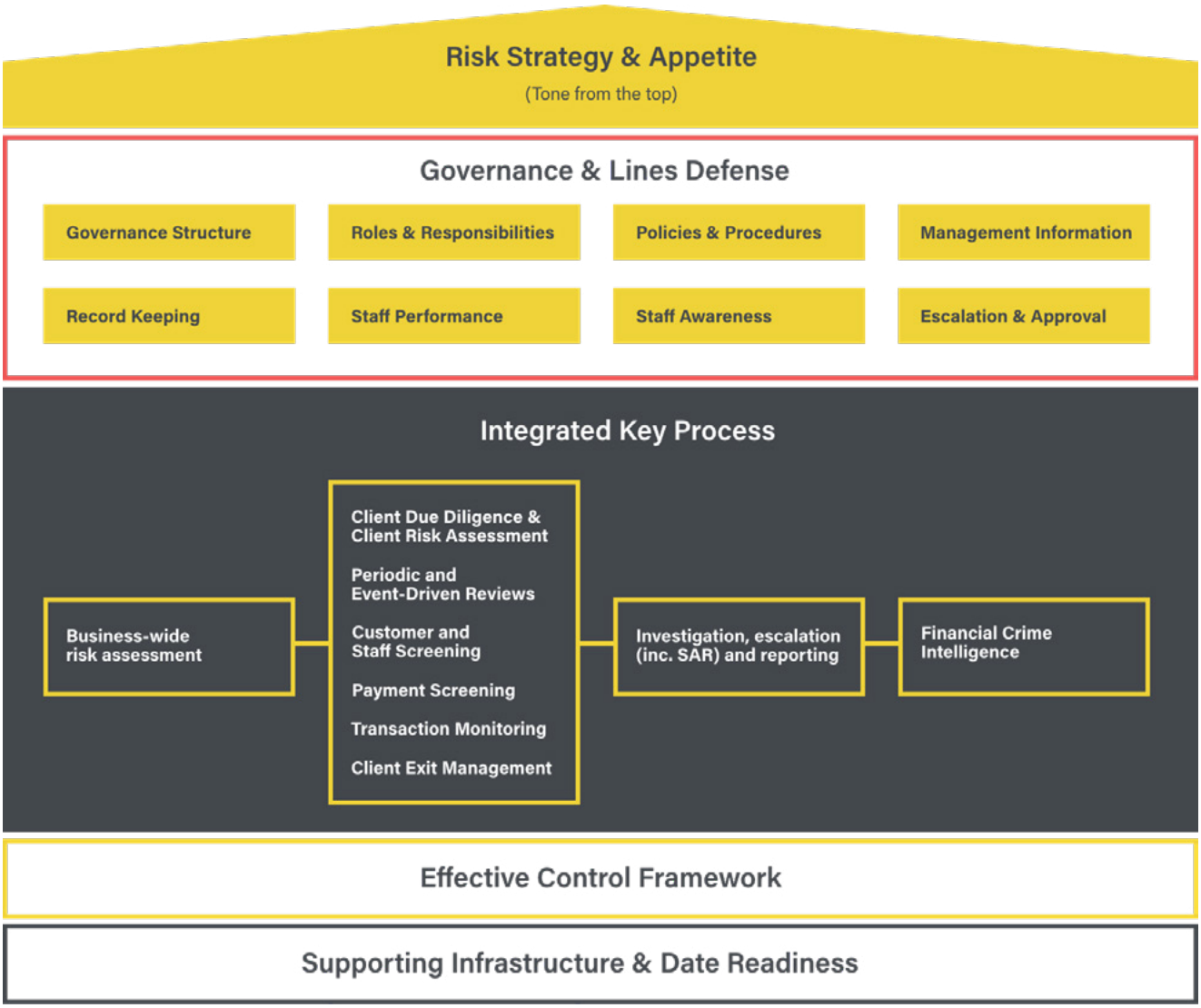
Any questions this guide does not sufficiently address should be referred to an appropriate supervisor, officer, or legal counsel. In addition, if rules or regulations come to light that may apply to a firm's business, it should contact its legal department or one of its officers. Even if it is unclear whether such rules or regulations apply, the firm's management or counsel should review and consider such information.

AML Procedures and Processes

AML Risk Assessment of the Organization and Risk Appetite Statement

AML is highly regulated and governed by a multiplicity of rules, regulations, and laws administered by various regulatory authorities. A violation of any of the applicable laws, rules, and regulations can result in the imposition of penalties, fines, censures, or other adverse actions against the firm, its officers, and employees. Although most firms and their staff members are aware of the regulatory framework's complexity and seriousness, and the need to exercise care in conforming their conduct to both the letter and the spirit of the law, it is vital to assess the firm's current and continuing AML risk.

The firm should draft a risk appetite statement, conduct a formal AML risk assessment, and identify the tools and processes it has in place to address that risk. Formalize a written risk assessment of the firm, including desktop or operational procedures within each AML unit, to maintain uniformity in the processes and analyses within the AML group. The operating procedures should detail the day-to-day operations aligned with specific tasks, such as conducting investigations and reviewing specific surveillance reports.



Workload and Staffing

Regulators expect that firms designate specific individuals solely responsible for the AML function and that a specially-designated AML group carry out its processes. Regulators have criticized firms whose AML function is fulfilled by a surveillance department or a department devoted to other functions.

When firms designate an AML group or department, they should also organize the program to include separate AML units. These might include units for:

- Quality assurance (QA)
- Financial intelligence
- Know Your Customer (KYC)/Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD)
- Sanctions and Lists Screening
- Training
- AML Risk Assessment – reporting to the Chief AML Officer

Ensuring an Efficient and Effective Process

Firms should sufficiently staff their AML group in proportion to the volume of transactions and business conducted. Adequate staffing ensures teams can complete all their reviews and daily assigned tasks on time. Leadership should also track all periodic and recurring tasks under their group's supervision, ensure they are completed on time, and assess the firm's AML staffing levels as its volume of business changes.

Using a dedicated AML case management system, a firm's analysts can identify prior alerts across multiple reports connected to specific customers, accounts, or securities, keeping a record of the screens or tools they used during review and documenting that information in the review's resulting notes.

The AML case management system should allow the AML analyst to see a holistic view of customer information and activity when they conduct AML surveillance. The review and analysis of customer activity can be used to enhance the design of report parameters and add new parameters to identify specific customer activity.

Ensure Staff is Highly Trained to Keep Ahead of Enforcement Actions

Firms should provide mandatory Anti-Money Laundering training to applicable personnel at the time of onboarding and annually. The training should include rule updates such as the Customer Due Diligence rules on beneficial ownership of legal entities. In addition, firms should keep AML staff informed of any changes in AML regulations. It is also beneficial to inform staff of current AML enforcement actions so they can avoid the perils that have resulted in other firms' enforcement matters. In addition to annual AML training, an AML manager should be assigned the task of monitoring public information sources (exchanges and regulatory websites and notices) for rule changes or changes in guidance and recent enforcement matters and distributing AML alerts to train staff members continuously. Firms should implement a Quality Assurance function to ensure decisions made by compliance analysts are in accordance with their policies and procedures, as well as regulatory guidance.

Risk Assessment of Each Customer

Firms should implement a quantitative customer risk-ranking system that will take into consideration factors including, but not limited to:

- The type of account
- Geographical factors - legal residence, current residence, country of citizenship in a prohibited, high-risk, medium-risk or low-risk location
- Financial information
- Source of wealth
- Occupation
- Banking information
- Length of relationship
- Publicly available information - including, but not limited to, negative news

The geographical factors indicate the level of risk but also may affect the other risk factors. For example, a high-risk geographic location may increase the banking risk. A low-risk geographic location may diminish the banking risk. The account type should be designed to consider the possibility of higher risk in certain account types with more opaque ownership and control structures. For example, all else being equal, individual and joint accounts are generally assigned a lower risk score than a legal entity account in an offshore location or an entity registered in one country but located in a different country.

The risk-ranking system should be used as the basis for setting review thresholds on surveillance reports and also for the following purposes:

1. By new accounts staff when reviewing an application
2. By AML surveillance staff when reviewing a customer's activity
3. By the firms' systems in establishing the level and frequency of Enhanced Due Diligence to conduct on a customer either at account opening or periodically after the account becomes active.

Firms should conduct ongoing EDD based on the customer risk-ranking system score.

Politically Exposed Persons

BSA/AML regulations do not define PEPs. Still, the term is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates of that individual. Due to this public position or relationship, these individuals may present a higher risk that their funds may be the proceeds of corruption or other illegal activity. However, the level of risk associated with PEPs varies, and not all PEPs are automatically higher risk.

US regulators do not interpret the term Politically Exposed Persons to include US public officials. US regulations do not specifically require firms to implement enhanced due diligence steps for PEPs or for US public officials. Nonetheless, the level and type of Customer Due Diligence (CDD) should align with the customer risk, consistent with the risk-based approach to AML specified by regulators.

When using a risk-based approach, a financial institution may consider the risk posed by a relationship with a PEP as one factor when determining the appropriate risk controls. Additional factors must be integrated into the financial institution's customer risk assessment, rather than being considered in isolation. These factors may include:

- The political environment and potential for corruption in the PEP's country of residence
- The reason for maintaining an account in a jurisdiction outside of the PEP's country of residence
- The products and services requested
- The individual circumstances of the customer
- The source and amount of the customer's funds

The Importance of Technology and Automated Methods of Detection

Regulators expect firms to use technology to prevent and detect financial crimes. AML reviews must analyze a vast sea of financial and personally identifiable information. Technology alone cannot solve this complexity, but firms can use Machine Learning and Artificial Intelligence to simplify the process, highlighting transactions and information buried within the data.

Machine learning can teach computers to find and reveal patterns firms want to identify. To build the best systems to detect and discourage financial crime, firms need sound systems logic and the ability to train the system using relevant data.

To have a beneficial system, organizations should use solutions that allow humans to understand the internal processes and outcomes of the machines. Firms can use machines to sort and filter data, but keep people in the loop by having them judge the quality of the findings and the outcome of the investigations.

Technology will enable financial institutions to identify threats with increasingly precise measurements that will enhance security and privacy. Better systems based on existing technologies are available to generate good data and help keep us safe from financial crimes.

In an increasingly digital world, financial institutions must also consider their cybersecurity arrangements, employing monitoring technologies such as Web Application Firewalls to deter external malicious actors from attempting to access customer accounts.

Central Records Management Systems Play an Increasingly Critical Role in AML Programs

Identification information records obtained from the customer must be retained for five years following account closure. Information used to verify a customer's identity should also be retained for five years following the creation of the record.

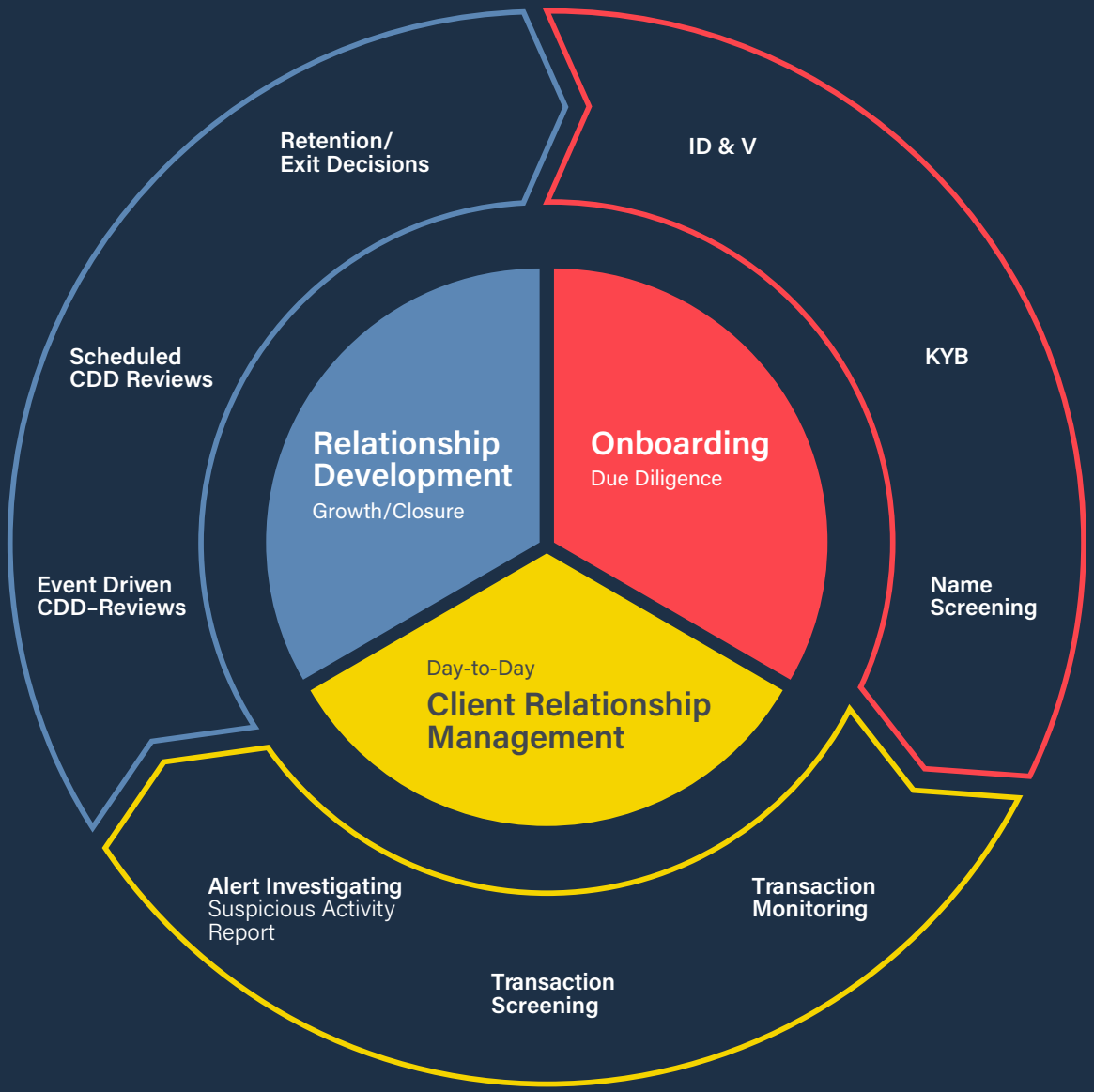
AML case management systems, where used, should be capable of managing and archiving regulatory and law enforcement inquiries related to similar activity conducted by other customers, cross-reference and index regulatory inquiries that the firm receives from regulators with its own surveillance reviews and investigations, and review essential information about past and current inquiries.

Firms must retain originals of all communications received from and sent to customers for at least three years following the date of the communication. For this reason, they should ensure that no communications are sent or received via unofficial or unrecorded channels.

Customer Due Diligence (CDD)

FinCEN requires financial institutions to obtain certain specified information regarding the ultimate beneficial owner or owners of legal entity customers. Covered firms are required to obtain, verify, and record the identities of the beneficial owners of such legal entity customers. A firm's records must include descriptions of any documentation relied on to verify the customer's identity. This would capture any relevant identification numbers contained in the document, the type of document used, its place and date of issuance, and any related expiry date.

The CDD rule requires understanding the nature and purpose of the customer relationship. On a practical level, firms should establish that the intended activities of the customer make 'business sense.' They also ensure that there is a coherent underlying investment strategy by conducting ongoing monitoring to identify and report potentially suspicious transactions and, on a risk basis, maintaining and updating customer information.



The rule defines the term beneficial owner as either of the following:

- Each individual, if any, who, directly or indirectly, owns **25% or more** of the equity interests of a legal entity customer
- A single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions. This list of positions is only an example as there are significant differences in how legal entities are structured

In August 2020, FinCEN issued some clarifications in the form of FAQs regarding Customer Due Diligence requirements to address ongoing challenges in three specific areas faced by firms trying to comply with the rule: (1) customer information gathering, (2) customer risk profiles and (3) ongoing customer monitoring. The overall theme underlying each FAQ answer is that firms should use prudent judgment under applicable circumstances, leveraging risk-based criteria to guide their efforts. FinCEN neither prescribes nor excludes any specific conduct or procedure. In other words, FinCEN expects firms and their AML staff to use their best judgment.

FinCEN guidance does not specifically require firms to obtain information about the customer's "expected activity," conduct media searches and review news articles, or collect information about "underlying transacting parties" if the financial institution offers correspondent banking or omnibus accounts to another financial institution (i.e., the customer's customer). However, unless the customer's risk profile is low, firms should collect such information, which can sometimes alert firms to important information, such as historical criminal or regulatory findings against prospective customers. Obtaining more information on a customer can often also help firms better understand the relationship and, therefore, better serve the customer's needs.

Any Customer Identification Program should include consideration of non-documentary verification measures, e.g., through reference-checking with other financial institutions or consumer reporting agencies, obtaining financial statements, checking public databases, and so on. Whichever verification method programs use, they should keep a documented record capturing how any substantive apparent discrepancies were resolved while verifying information obtained from customers.

FinCEN did provide a response regarding whether it is necessary to "use a specific method or categorization to risk rate customers" or to "automatically categorize as 'high risk' products and customer types that are identified in government publications that could potentially expose the institution to risks." Yet the response did not offer any specific methodology – or even require any action based on the government's own categories. The FinCEN response stated, "[t]here are no prescribed risk profile categories, and the number and detail of these categories can vary…even within the same risk category."

FinCEN guidance states that due diligence measures may vary on a case-by-case basis. FinCEN remarks that the financial institution's AML program should be sufficiently detailed to risk-rank customers and distinguish between significant variations in the risks of its customers. Accordingly, firms should create a risk-ranking system using their best judgment, reasonably designing it to identify customers with higher risk and use that information in reviewing customer activity.

FinCEN also addressed whether the CDD Rule requires firms to update customer information on a specific schedule. It said there "is no categorical requirement that financial institutions update customer information on a continuous or periodic schedule." That said, securities and commodities regulators require firms to verify and update account information, as applicable, at least annually for commodities accounts and at least every three years for securities accounts. It is reasonable to request that customers review and update their personal contact information and financial information annually and whenever the financial institution becomes aware of a change in customer information (including beneficial ownership information). The firm should then reassess the risk factors and recalculate the customer risk rating as needed.

Enhanced Due Diligence

The assessment and execution of enhanced due diligence should be done both at account opening and on an ongoing basis. The financial institution should implement a customer risk ranking program designed to capture the overall AML risk posed by individual customers by evaluating a variety of factors. Firms should use the customer risk-ranking system to assess the need for enhanced due diligence and perform enhanced due diligence based on perceived customer risk when reviewing new customer information and surveillance reports. The risk ranking system should consider, among other things, the geographic location of the customer, the nature and complexity of the customer's underlying business, and any criminal history or adverse published news.

The level and frequency of Enhanced Due Diligence should be determined by the firm's systems periodically after the account becomes active, based on an EDD assessment tied to the Customer Risk Ranking.

Information Sharing

Section 314(b) of the USA PATRIOT Act provides a safe harbor for information-sharing, protecting financial institutions from liability so they can better identify and report suspicious activities that may involve terrorist financing or money laundering. Financial institutions may share information regarding individuals, entities, organizations, and countries in order to help identify and, as appropriate, report activities that may involve terrorist financing or money laundering.

FinCEN strongly encourages financial institutions to participate so that firms can alert other participating financial institutions of customers whose suspicious activities may not have come to their attention. The Financial Crimes Enforcement Network (FinCEN) has provided the following guidance on information sharing.

Financial institutions may share information relating to activities that they suspect may involve the proceeds of a Specified Unlawful Activity (SUA). Financial institutions do not need to have specific information that these activities directly relate to an SUA or have identified specific proceeds of an SUA being laundered.

The financial institutions do not need to have made a conclusive determination that the activity is suspicious. Financial institutions may share information about activities as described, even if such activities are not classified as a transaction. Such information may relate to an attempted transaction or an attempt to induce others to engage in a transaction.

Significantly, Section 314(b) does not limit the sharing of personally identifiable information or the manner in which information can be shared, including oral information sharing.

Several characteristics distinguish EDD from regular CDD policies:

Rigorous & robust

EDD processes for establishing ultimate beneficial ownership, business nature and purpose, and customer identification must draw on significantly more detailed evidence.

Quality assurance

Onboarding quality assurance audits should verify a greater percentage of high-risk customers as compared to lower-risk ones.

Detailed documentation

The EDD process must be documented in detail, with scrutiny on how data is captured and validating the reliability of information sources

PEPs

Special attention should be paid to PEPs, who are in positions that can be potentially abused for money laundering.

The Travel Rule

In October 2020, FinCEN and the Federal Reserve Board issued a joint Notice of Proposed Rulemaking to amend the recordkeeping and travel rule regulations under the Bank Secrecy Act. Under the current recordkeeping requirements, regulated firms must collect, retain, and transmit certain information related to transmittals of funds above $3,000, such as the name and address of the transmitter, any payment instructions received from the transmitter with the transmittal order, the identity of the recipient's financial institution, and, if provided, the name and address of the recipient.

- The proposed rule lowers the applicable threshold from $3,000 to $250 for transactions that begin or end outside of the United States
- The threshold for domestic transactions remains at $3,000

The proposed rule also further clarifies that those regulations apply to transactions above the applicable threshold involving convertible virtual currencies, as well as transactions involving digital assets with legal tender status, clarifying the meaning of the word "money" as used in the regulations.

Customer Due Diligence and Ultimate Beneficial Ownership (CDD/UBO)

It is essential to maintain written procedures reasonably designed to comply with the Bank Secrecy Act, including the May 2018 update to the Customer Due Diligence rule. The account application process should capture Ultimate Beneficial Ownership (UBO) information for new legal entity customers per the CDD rule amendment. Legal entity customers can be presented with a "Certification of Beneficial Owners of Legal Entity Customer Accounts" that they must complete during the account application process.

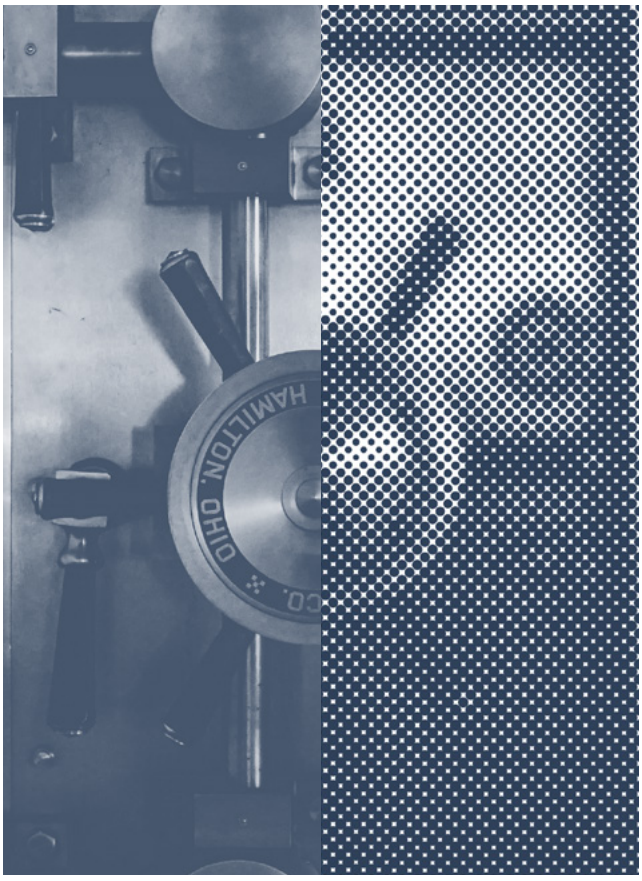
When completing a new account application, applicants should be required to indicate the type of account they request to open. Account applications for institutional or organizational accounts should require completing the Certification of Beneficial Owners form to identify individuals that own 25 percent or more of the legal entity for which the account is being opened. The information provided should be retained with the customer account data and kept on file for at least six years after account closure. Customers should agree in writing to notify the firm whenever there are changes in account ownership and update the account information.

The firm should also request the identity of the individuals with authority to manage the customer account, which includes individuals with significant responsibility for managing the legal entity for which the account is being opened.

Do not accept omnibus accounts or accounts where the account ownership is not disclosed unless the firm receives KYC and customer identification program (CIP) documentation from the underlying customers.

For all applicants, including legal entities, the firm should require the customer to complete an account application that collects the required information on the account's nature and purpose. This includes details about the type of business conducted for legal entity customers.

Individuals disclosed to the firm as beneficial owners of legal entities or individuals with managerial authority over legal entities should be subject to similar screening controls as nominee owners. This includes screening the disclosed individuals through negative public information databases and comparing against the OFAC Specially Designated Nationals And Blocked Persons List and other international sanctions lists.



Suspicious Activity Report (SAR) Filing

Firms should evaluate the number of SARs filed annually compared to the growth of their business. They should develop suspicious activity reporting frameworks with continuous regard to regulatory guidance around red flags. This document refers to many such red flags, although it should be noted that regulators frequently add to their red flag guidance.

Broker-dealers should tailor their SARs on a case-by-case basis to reflect the specific circumstances reported. They should avoid using pre-written 'boilerplate' content. Further, broker-dealers must not place reliance on third parties such as Introducer or Clearance firms to file SARs on their behalf. Higher-volume firms that are likely to submit SARs regularly will benefit from a dedicated end-to-end case management system to track progress, from the initial detection of suspicion through the SAR filing and any follow-up contact from law enforcement.

Regulators have stated that firms should file SARs whenever they receive inquiries indicating that a customer has violated securities regulations or may have conducted illegal or suspicious activities. Firms should file a SAR whenever one or more of the following occur during the course of responding to a regulatory inquiry, law enforcement request or subpoena regarding customer activity:

01 Any time the firm identifies activity, while reviewing customer activity in response to a regulatory inquiry, that would have led the firm to file a SAR if identified before receiving the inquiry. Such a discovery may result from a more targeted review of the activity than the firm had already done or may result from the regulatory inquiry indicating additional facts that the firm was not aware of, such as an indication in the regulator's inquiry that there is a connection between two apparently unrelated customers or a between a customer and an outside individual that is not a customer.

For example, suppose that during a review in response to a regulator or law enforcement official, an AML staff member identifies suspicious activity that may indicate money laundering, a legal violation, or a violation of a securities regulation – such as market manipulation, insider trading, pre-arranged trades or intentional cross trades, fraud, or theft. In that case, they should escalate the facts to a supervisor with a recommendation to file a SAR regarding the activity.

02 Any time the firm learns additional information from a regulator or law officer that indicates a customer has engaged in suspicious or illegal activity. If the information cannot be verified or if it is outside of the firm's knowledge, the firm should still file a SAR. The SAR should be filed even if it is clear that the law officer or regulator is already aware of the activity.

03 A regulator obtains a court order (including a temporary restraining order) restricting or freezing the assets in an account due to activity that is alleged to be criminal or was otherwise deemed to be suspicious by the regulator.

04 Whenever a regulator requests that the firm place a freeze on account assets (even temporarily), notify them of any withdrawals from the account or other account activity, or provide them with monthly account statements because they suspect aillegal activity or other information that would have prompted the firm to file a SAR (e.g., market manipulation, trading in concert, theft, fraud).

The facts should be escalated to a supervisor with a recommendation to file a SAR regarding the activity. The basis of the SAR filing would depend on the information provided at the time of the inquiry or the AML investigator at the firm should ask questions regarding the reason for the inquiry or asset freeze. If the AML group cannot determine the underlying reason for the regulator's inquiry, the firm should still file a SAR based on the fact that the regulator requested a temporary asset freeze or requested information due to suspicious activity conducted by the customer.

Any transactional activity (either single transaction or pattern of transactions) of $5000 or more must result in a suspicious activity report from the broker-dealer where they know, or have reason to suspect, the following:

01 The transaction involves funds derived from illegal activity, or is being performed to disguise such funds

02 The transaction has been structured to evade Bank Secrecy Act requirements

03 The transaction has no apparent business or lawful purpose, the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, or it does not align to a particular customer's normal pattern of activity

04 The transaction involves the use of the broker-dealer to facilitate criminal activity

SARs must be submitted no later than 30 days post-detection of the activity in question. A 30-day extension can be sought in some circumstances, to allow for 60 days total. However, this must be done with consent and represents the maximum permitted time for reporting.

Digital Currency/Cryptocurrency

Technology makes it easy to hide identities and illegal activity, creating a platform that can be exploited by the black market, criminals, terrorists, and foreign governments. Regulators and law enforcement are increasingly focused on cryptocurrency businesses' AML compliance programs, as well as cryptocurrency businesses that facilitate money transfers.

Broker-dealers should prepare for tracking and reviewing activity related to digital currency. A few decades ago, it was unimaginable that customers would keep their fortunes in digital currency and check their digital wallets. However, decentralized systems such as Bitcoin are especially vulnerable to anonymity risks. Bitcoin addresses, which function as accounts, have no names or customer identification, and the system has no central service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions associated with real-world identities. No central oversight body exists, and law enforcement cannot target one central location or administrator for investigations or asset seizures. For these reasons, the US government is likely to increase its enforcement of KYC/AML/CFT rules, create additional financial regulations regarding cryptocurrency, and issue large penalties to firms they deem deficient. In addition, other countries are likely to follow along by increasing comprehensive global standards regarding cryptocurrency.

In 2019, FinCEN announced that the US government would begin strictly enforcing the travel rule for cryptocurrency transfers. This required firms handling cryptocurrency to maintain procedures to know their customers, verify their identities, record the names of originators and recipients of cryptocurrency transfers in accordance with the travel rule, and transmit that information to counterparties, as applicable. This was in contrast to prior beliefs that digital currencies were not classified as money and that the travel rule did not apply to virtual currency transfers.

In April 2019, FinCEN imposed a fine against a cryptocurrency trader for willfully violating the Bank Secrecy Act and for noncompliance with AML practices. The trader failed to register with FinCEN as a money service business (MSB); develop, implement, and maintain an effective written AML program; report suspicious transactions conducted by, at, or through the trader; and file currency transaction reports – all requirements of the BSA and implementing regulations.

In October 2020, FinCEN imposed its first civil penalty against a cryptocurrency money service business for violating AML regulations. FinCEN found that the MSB willfully violated the MSB registration requirements, that the firm failed to implement an effective anti-money laundering program as required by the BSA and its implementing regulations, and that the firm failed to file mandatory Suspicious Activity Reports on highly questionable transactions.

KYC, CFT, and AML rules require regulated firms to identify participants and track transactions so criminal activity can be monitored and prosecuted. Still, these are difficult to enforce in the digital world. By design, it is difficult to track customers, sources of revenue, and the owners, originators, and recipients of funds. In addition, virtual currencies are mined by individuals connected to servers worldwide, and the electronic trading of currencies leaves an enormous potential for market manipulation. Because cryptocurrency provides anonymized, secure transactions, it is ideal for criminal activities such as cybercrime, drugs, illegal goods, funding terrorism, money laundering, and tax avoidance. All of this has produced an environment where the prices of cryptocurrencies are prone to wild fluctuation and speculation.

Many individuals are watching to see how regulators in the US and other countries will enforce cryptocurrency regulations and whether any country will endorse a national digital currency. Regulators' role in controlling monetary policy is critical to their ability to combat economic downturns, inflation, and trade wars. Regulators have almost no choice but to increase their enforcement of AML/CFT regulations.

Financial institutions will likely continue to promote and use digital currencies and should treat cryptocurrency like a traditional currency, tradable commodity, or other asset. Regulators' actions regarding cryptocurrency indicate that the following issues are crucial:

1. Financial institutions that accept cryptocurrency need to be increasingly focused on cryptocurrency business KYC/AML/CFT compliance programs and continuous monitoring of cryptocurrency transfers.

2. Financial institutions that conduct a cryptocurrency business should implement and maintain strong and effective AML and sanctions compliance programs to avoid regulatory scrutiny and corresponding penalties.

3. Financial institutions should perform ongoing risk management, including automated data analytics, and monitoring, using dashboards that display key risk indicators and management reporting.

4. Financial institutions that seek to do business or partner with other cryptocurrency businesses should ensure that their due diligence efforts are robust.

5. Financial institutions conducting a cryptocurrency business should implement procedures for reporting cryptocurrency-related suspicious transactions.

Detecting Suspicious Activity

In addition to detecting activity conducted by an individual customer, it is vital to be able to detect and identify suspicious activity conducted by more than one individual acting together. Important information can be recognized by reviewing activities conducted by seemingly unrelated customers that may have similar or identical addresses, phone numbers, other contact information, bank account numbers, or internet access data.

IP/MAC Address Combination

Firms should have a systematic way to check their customers' ongoing Internet Protocol/Machine Access Code (IP/MAC) logins to detect unusual activity. Suspicious Activity related to IP/MAC address may include:

- Customer logins for apparently unrelated customers that occur from a single device or IP address, often within a short period.
- The IP address associated with a login does not match the country of the stated address in identity documentation.
- Customer logins that occur within a pattern of high network traffic with decreased login success rates and increased password reset rates.

Trading Activity

By reviewing customer trading, it may be possible to detect apparently unrelated customers that conduct substantially similar trading. This may indicate that the customers are acting in concert, that one customer is managing the account of another (perhaps as an undisclosed financial advisor), or that a third party is managing both unrelated accounts. Contacting such customers may help determine whether the activity is suspicious or if there is a reasonable explanation for the trading activity.

In addition, a careful review of trading activity can detect cross trading and other manipulative trading, such as "money pass" trading where money is moved from one account to another by conducting trades at prices that do not reflect the market prices at the time of the trade. "Money pass" trading is a form of non-competitive trading in which one trader loses money to another trader, typically where one trader buys a quantity of contracts at a high price from another trader, and sells back the same quantity of contracts at a low price opposite the same trader, leaving neither trader with a resulting position. This type of trading may also indicate two individuals colluding to make a payment (including as part of a money laundering scheme), or one individual manipulating another account – such as an advisor extracting money from an account he advises. Many exchanges have express prohibitions against executing transactions designed to pass money between accounts.

> Over the past few years, exchanges have increased their focus on manipulative trade orders such as spoofing and layering. Both spoofing and layering are the practice of bidding or offering one or more prices to buy or sell a product with intent to cancel the orders before execution.

Spoofing is the pattern or practice of entering an order on one side of the market and immediately canceling the order before it is filled. Spoofing is conducted to change the demand in a security and influence the price, only to enter an order on the other side of the market based on the new price. Spoofing is a form of disruptive market manipulation.

Some regulators use the terms spoofing and layering almost interchangeably. However, others use layering to describe entering multiple non-bona fide orders at multiple price tiers that are canceled before they are filled to give the appearance of multiple layers of interest in a security. Regardless of the terms used, firms must be wary of customers who engage in large-volume trading via multiple issuers, or trading in thinly traded, low-priced securities that accompanies sudden spikes in price.

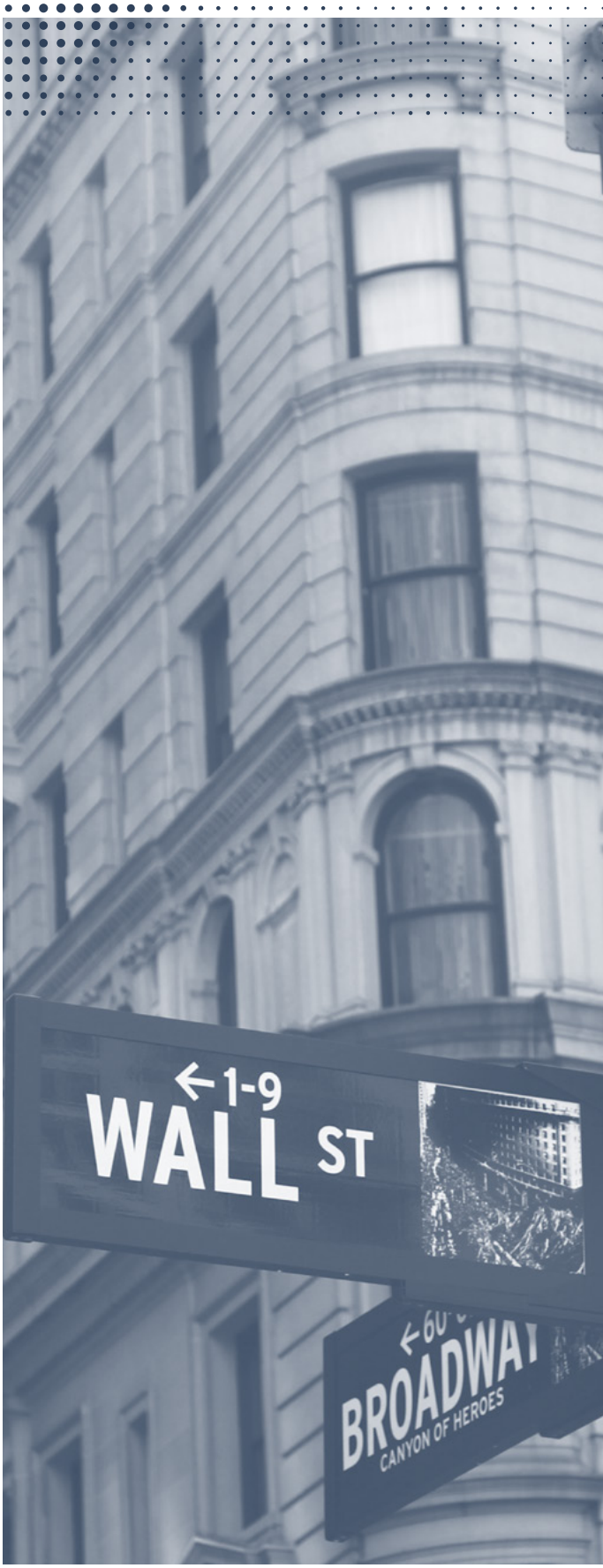
Marking the open/marking the close is another form of market manipulation. Marking the open or marking the close is an attempt to influence the price of a stock by executing purchase or sale orders – either at the open, or at or near the close of the market. An individual or a fund may place a buy order on stocks they already own. That will cause the share price of their stocks to increase and make their account's performance look better than it otherwise would. This may be done to affect a fund's performance figures or to prevent margin calls in an account heavily invested on margin in the manipulated shares.

As broker-dealer firms grow, so will the volume and complexity of the trading activities they are involved with. Firms should consider implementing automated monitoring systems where conducting manual analysis of transactional activity is not feasible. Where manual analysis is thought to be feasible, it cannot solely focus on reviews of 'daily blotters' and must look at trading activity over the long term to detect patterns not visible via a day-by-day view. By extension, at the inception of a new customer relationship, firms should seek to understand the type of transactions in which their prospective customer wishes to engage and determine the level of monitoring required.

Once automated monitoring is in place, firms should perform regular system assurance to prove that the monitoring system is working as intended. Firms must update their assurance programs accordingly where the monitoring system or its underlying rules are changed or updated. This includes documenting the changes made with an accompanying rationale and retaining evidence of any testing undertaken to ensure the system works effectively.

Cashiering Activity

By reviewing customer cashiering activity, it may be possible to detect suspicious activity, including activity conducted by apparently unrelated customers. This activity may include the movement of funds between customer accounts, deposits to unrelated accounts from the same bank account, third-party deposits, frequent deposits/withdrawals, and deposits that exceed the customer's stated net worth. In addition, activity involving withdrawals to a country other than the customer's country of residence may be deemed suspicious unless a reasonable explanation is provided after an inquiry with the customer.



Microcap or Low-Priced Stock

Trading in low-priced or microcap stocks typically poses a higher-than-average risk because of the possibility of low trading volumes and a relative lack of information regarding the issuers. The US Securities and Exchange Commission (SEC) has warned firms and investors that, while many microcap stocks are issued by legitimate businesses with real products and services, microcap stocks may be easily manipulated by fraudsters who distribute false information about the issuer in order to create an artificial demand for the shares. After trading in the stock increases and the price rises, the fraudsters sell their shares at inflated prices, discontinue promoting the stock, and the stock price falls while investors lose their investment.

Regulators have taken disciplinary action against several firms regarding trading in microcap stocks. Automated monitoring of penny stock trading is essential. Firms should also have procedures to address all of the following potential findings to avoid similar findings.

Regulators' AML findings regarding microcap stocks included the following:

The firm did not have policies and procedures reasonably designed to monitor microcap and low-priced stocks trading.

- The firm accepted the deposit of shares of microcap and low-priced securities (penny stocks) with a large aggregate notional value.
- The firm's AML program did not conduct surveillance targeting transactions in microcap or securities trading outside of the traditional exchanges.
- The firm permitted trading that constituted a large percentage of the microcap security's trading on the days that it traded. The customer also purchased small amounts of the microcap security to support the stock's price when it faced downward pressure. Those transactions lacked an economic purpose as the customer immediately liquidated the shares at lower prices.
- The firm did not have sufficient procedures regarding customer sales at or near the close of business.

The firm's AML analysts failed to identify red flags of manipulative microcap securities trading by its customers.

- The firm conducted microcap stock transactions on behalf of customers in known bank secrecy havens, including Switzerland and Guernsey and other offshore tax havens.
- The firm's customers included introducing brokers and known toxic debt or death spiral financiers known for depositing and selling microcap stocks, which presented risks including market manipulation, money laundering, fraud, and lack of SEC registration.
- The firm facilitated these transactions, while some of the securities were subject to "pump and dump" schemes or other manipulation or fraud.
- Some customers were depositing, and shortly thereafter selling, large blocks of low-priced securities.
- The firm processed thousands of wires for customer accounts associated with high-risk jurisdictions.
- The firm processed foreign currency-denominated wire transfer activity related to the purchase and sale of micro-cap stocks.
- The firm's AML surveillance focused solely on wire transfers conducted in US dollars. The firm did not review wires conducted in foreign currency or determine whether they involved high-risk entities or jurisdictions.

The firm's AML program was not reasonably designed to identify wire transfers (or a pattern of wire transfers) conducted in amounts that were designed to avoid attention or reporting.

- The firm's AML program failed to adequately monitor brokerage execution and custodial banking activity involving microcap stock transactions, including Delivery versus Payment (DVP) transactions.

- The firm facilitated the purchase and sale of low-priced shares for undisclosed customers through an omnibus account. The firm allowed these omnibus accounts to conduct microcap stock transactions for undisclosed underlying customers of the foreign banks, even though the firm could not generally obtain crucial information such as the identity of the stock's beneficial owner, the beneficial owner's relationship with the issuer, or how the seller obtained the stock.

- Despite the volume of microcap stock activity conducted through the firm, it failed to develop and implement a written AML program regarding the sale of microcap stocks that could reasonably be expected to detect and cause the reporting of potentially suspicious activity.

- The firm's AML program was understaffed, and its personnel lacked access to information critical to determining whether the wire activity they reviewed was suspicious, such as the customer's background and historical account activity, or receipt of proceeds derived from the deposit or liquidation of microcap stocks.

- **The firm's AML program failed to ensure that suspicious activity was reported in instances where the firm had already responded to regulatory requests regarding information deemed to be suspicious and failed to update prior Suspicious Activity Report (SAR) filings when activity continued through the firm more than 90 days after a previous SAR was filed.**

Some methods of avoiding findings like the ones listed above regarding micro-cap stocks involve limiting the stocks offered to customers. OTC Markets marks certain stocks in their system as "NO INFORMATION". This categorization means that the companies are not able or willing to provide current disclosure to the public, to a regulator, an exchange, or to OTC Markets Group. The category includes companies that may have ceased operations as well as those deemed to be 'dark,' as they may have questionable management and inadequate market disclosure practices. Publicly traded companies not willing to provide information to the public market should be considered highly risky and prone to manipulation.

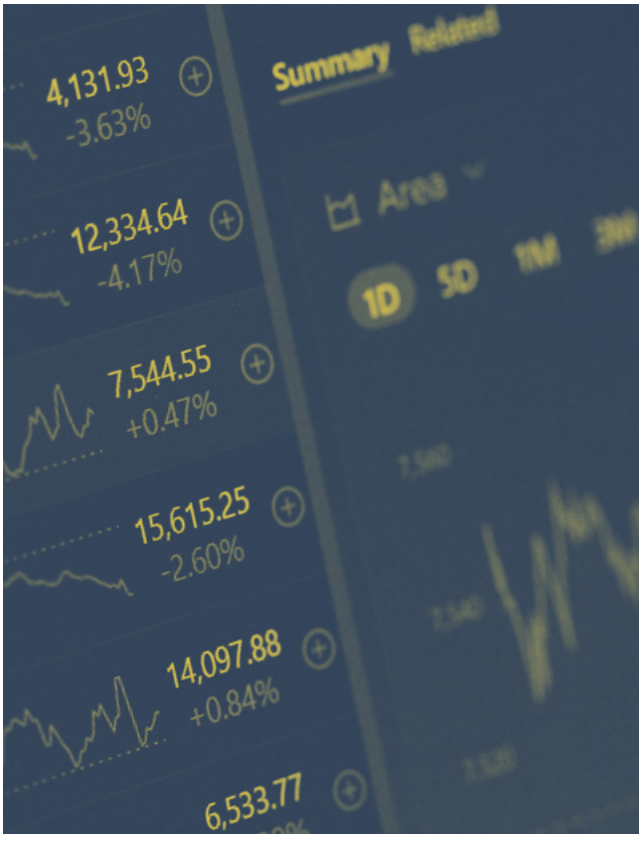
In addition, a firm can restrict the purchase or sale of shares in companies that are marked in the OTC Markets system as:

1. Currently or previously indicated as "Shell Risk"
2. Previously marked "Caveat Emptor"
3. Currently, or recently, subject to a stock promotion (a likely indication of a "pump and dump" attempt).
4. Subject to a name change in the past year, or had more than 1 name change in the past 2 years or had more than 2 name changes in the past 5 years.
5. Subject to a trading halt or suspension (currently or in the recent past)

Management may want to consider restricting transactions in microcap stocks with one or more of the above factors.

AML staff should review a daily report of incoming shares to confirm that restrictions placed by the firm on shares of microcap securities are enforced and that no customers have transferred in a large block of low-priced stock unless the shares were purchased on the open market (i.e., on a public market center through another broker-dealer) or are registered with the SEC (i.e., through an S-1 registration statement). However, as noted above, daily 'blotter reviews' are insufficient for detecting longer-term trends or concerning patterns of activity.

> If AML staff identify a large transfer of shares of a microcap security that does not meet the above conditions, they should promptly restrict the shares from being sold and contact the customer to have them transfer the shares out of the firm.



Firms can enforce certain policies to mitigate the risks associated with microcap stock. To enforce the requirements of Section 5 of the Securities Act of 1933 and FINRA Notice to Members 09-05, firms may set policies such as the following:

- Refuse to accept the delivery of restricted physical stock certificates presented to the firm or transferred to the firm through Depository Trust Company's (DTC) "window service."
- Only allow transfers of stock through DTC from accounts designated as "free accounts," from which shares are freely transferable.
- Do not accept automated customer account transfer service (ACATS) transfers of shares for which its clearing system does not recognize the Committee on Uniform Securities Identification Procedures (CUSIP) number of the shares that are delivered or that have a CUSIP number that identifies the shares as restricted shares.
- Accept restricted shares only from transfer agents that issue such shares in connection with a mandatory corporate reorganization that specifies the issuance of restricted shares to current shareholders and the firm currently holds such position for one or more of its customers.
- Implement a restriction in the firm's clearing system or at its clearing broker to prevent customers from transferring any microcap stocks into their accounts. A microcap stock is generally a stock that is (1) traded on over-the-counter bulletin board (OTCBB) or PINK Open Market or (2) listed on any NASDAQ and NYSE American exchange with a market cap of less than $300 million with a trading price of less than $5 per share.
- Do not allow Delivery Versus Payment (DVP) customers to trade microcap stocks.
- Allow transfers of shares of microcap stocks that the customer can prove were purchased on the open market (i.e., on a public exchange through another broker) or that are registered with the SEC (i.e., through an S-1 registration statement). Restrict the sale of such stocks until the receipt of appropriate documentation.
- Do not rely on legal opinions that state that the shares do not need to be registered or are subject to exemptions from registering the shares.
- Do not rely on a transfer agent for the shares to attest that the shares are registered and freely transferable.

Wire Transfers and Currency Conversion

Regulators have specifically targeted activity as suspicious if it involves:

Withdrawal to a currency other than the native currency of that location

Wires for customer accounts associated with high-risk jurisdictions

Significant withdrawals quickly deposited into different accounts

Foreign currency-denominated wire transfer activity related to the purchase and sale of penny stocks

Large currency deposits via ATMs into offshore accounts with no apparent business rationale

Bank secrecy havens, including offshore tax havens

Conversion to a currency and withdrawal to a jurisdiction designated by the US government as representing a high risk of money laundering

Avoiding such activity to the extent possible will help strengthen a firm's AML program. If it cannot avoid conducting this activity, the firm should report such transactions as suspicious. Naturally, this is where it is important to have a risk-based process for the review of trades and wire transfers. Businesses with significant volumes of transfers should not rely on manual processes for such reviews.

Annual Review

In order to comply with regulations, firms should retain a third-party firm to conduct its annual independent AML program testing. Firms should also perform an annual gap review of the AML topics handled by their groups, taking primary responsibility for identifying any gaps between regulations, written supervisory procedures, and the procedures their groups actually conduct. Whenever gaps come to teams' attention, whether through the annual review or at another time, they should be reported to firm leadership and/or legal counsel, as necessary.

Establishments should also review all findings raised by any regulatory requests or examinations relevant to their area(s) and investigate whether the regulator's inquiry or exam has highlighted any gaps in the firm's procedures. They should appoint an AML staff member to track each finding from their annual audit, annual gap review, and regulatory requests or examinations and the resolution to each.

The Role of Internal Audit

Internal audit departments face the challenge of being able to provide evidence to regulators that they are helping to promote strong governance by having applicable methods of testing, documenting, and reporting on the effectiveness of a sufficiently defined and transparent AML governance structure that includes a well-defined AML issue escalation protocol.

> The audit department needs to verify that adequate AML oversight is in place in the compliance group of the corporate office, in each of the regional and affiliate offices, and in each line of business. Each of these offices should also have AML-designated individuals in senior management roles.

Regulatory guidance also establishes the importance of senior management being responsible for communicating and reinforcing the AML compliance culture as established by the board of directors, and provides guidance that committees can be used to assess the effectiveness of the AML program and regarding significant AML compliance matters.

Effective Governance Structure

Regulators' disciplinary actions against financial institutions have stated that an effective AML program must have:

- A sufficiently defined and transparent governance structure with clear lines of responsibility
- A defined escalation protocol for AML risk control decisions and AML issues, beginning with senior management and including each affected line of business that is required to comply with the policies
- Accountability for AML compliance that is clearly communicated and enforced
- Clear lines of authority and responsibility for AML and OFAC compliance with respect to lines of business and corporate functions and within corporate oversight functions
- A sustainable governance framework that ensures that AML issues are appropriately tracked, escalated, and reviewed by senior management

The institution should have a main AML compliance committee, with the purpose of discussing the AML program's status and issues. The members should include AML compliance-designated senior management from the corporate office, each of the company's regional and affiliate offices, and each line of business. Firms must designate and identify a senior manager or managers from the AML compliance committee as ultimately responsible for implementing the board-approved AML program. This information must be reported to FINRA, and verified annually within 17 working days of the end of each calendar year. Any changes to the designated individual or individuals must be updated and reported within 30 days of the change.

FinCEN's 2014 Bulletin Advisory to U. S. Financial Institutions on 'Promoting a Culture of Compliance' also states a financial institution can strengthen its BSA/AML compliance culture by ensuring that:

1. Its leadership actively supports and understands compliance efforts;
2. Efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests;
3. Relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts;
4. The institution devotes adequate resources to its compliance function;
5. The compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party; and
6. Its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used.

> While staff training, effective tools and organizational processes must be reasonably designed to achieve compliance with the BSA, the importance of culture cannot be understated. A financial institution's leadership is responsible for promoting a culture that supports BSA compliance at all levels of the business.

The commitment of an organization's leaders should be visible within the organization, as such commitment influences the attitudes of others within the organizationn.

Several firms have received consent orders regarding the financial institution not having a sufficiently defined and transparent governance structure that includes a defined AML issue escalation protocol. Financial institutions spend significant amounts of time, money, and resources addressing these regulatory matters.

Demonstrating a strong AML program includes having an effective AML governance structure as well as applicable escalation and responses by senior management. An effective AML governance structure is only possible when a firm's leaders are kept informed of the issues related to AML compliance within the institution.

AML Enforcement Trends

Federal agencies specify four pillars that make up an adequate BSA/AML compliance program:

BSA/AML compliance program

1. A designated individual or individuals responsible for monitoring BSA/AML compliance
2. A system of internal controls to assure ongoing compliance
3. Adequate independent testing
4. Appropriate AML training for personnel

Regulators require that the AML compliance program also include a Customer Identification Program with risk-based procedures so that the company has a reasonable belief that it knows the identity of its customers, vendors, and others with whom it conducts financial transactions

Regulators expect to continue to focus on AML compliance using new tools, assessing increased monetary penalties, and making rigorous efforts to monitor AML compliance programs.

October 2021:

FINRA issued a guidance note urging member firms (i.e., broker-dealers) to consider how they will incorporate the U.S. Treasury Department's eight government-wide AML / CFT priorities into their risk-based AML compliance programs. The priorities are:

- Corruption;
- Cybercrime, including relevant cybersecurity and virtual currency considerations
- Foreign and domestic terrorist financing
- Fraud (including securities and investment fraud and internet-enabled fraud)
- Transnational criminal organization activity
- Drug trafficking organization activity
- Human trafficking and human smuggling
- Proliferation financing

March 2022:

The SEC has proposed a new rule that, if adopted, will widen the circle of players required to register as dealers. This is because the new rule provides greater granularity around the definition of those engaged in securities sales/purchases "as part of regular business".

According to the rule, businesses that control <$50m assets would not be captured, nor would investment companies registered under the 1940 Investment Company Act (ICA. The expectation across the industry is that it will be adopted with few alterations.

> Regulators have highlighted the need for robust AML programs. In September 2022, a company agreed to pay $450,000 for, among other things, failing to design and implement its AML program, implement a Customer Identification Program, and preserve and maintain business-related electronic communications.

Earlier, the FDIC fined one company $12.5 million for AML violations, while FinCEN fined another company $390 million. The FDIC said the $12.5 million civil penalty imposed in one consent order was appropriate because of the gravity of the violations and the company's prior AML violations. The regulator imposed the penalty after asking the company to enhance its anti-money laundering compliance program and finding that it failed to comply with the FDIC order timely. The company agreed to settle the allegations that it failed to comply with anti-money laundering rules and consented to both orders without admitting or denying the findings.

> FinCEN levied a $390 million penalty on another company for failures that they termed "egregious" including failure to file Suspicious Activity Reports, failure to file Currency Transaction Reports, and failure to implement and maintain an effective Anti-Money Laundering program.

Key Takeaways

Broker-dealers looking to bolster or revamp their risk management processes should bear in mind several key considerations.

AML Procedures and Frameworks

Follow financial sector best practices for AML/CFT, aligning all components with regulatory requirements and guidance. This means laying the groundwork with solid **enterprise-wide risk assessments** and then establishing a framework aligned with the firm's unique **risk profile**.

Key AML components broker-dealers should align with their risk profile include:

- **Customer due diligence**, which includes:
  - **Customer risk assessments**
  - **Enhanced due diligence** for high-risk customers such as PEPs
  - **Thorough tracing and capture of Beneficial Ownership information**
  - **Transaction screening and monitoring**
  - **A structured, compliant reporting process**
- **Appropriate technological resources and personnel**, including:
  - **An appropriately-sized risk team**
  - **Thorough risk personnel training**
  - **Robust technological tools to support the team**, designed to handle the data volumes and risk types inherent in the compliance program
- **Governance, accountability, and escalation structures**

Sector-specific Risks

Certain risks are specific to the broker-dealer industry and should be given special consideration in a firm's risk assessment and AML/CFT framework. Each firm should evaluate risks specific to its operations, but key areas to consider include:

- **Digital Currency/Cryptocurrency**
- **Microcap and low-priced stock**
- **Wire transfers and currency conversion**
- **Suspicious trading and cashiering activity**

Ongoing Regulatory Updates & Enforcement Trends

Any risk-based AML program should harmonize with continually-updated regulatory information to ensure changing requirements are not overlooked. During their regular risk assessments, broker-dealers should take into account areas impacting their operations that have recently been subject to enforcement trends. In this way, firms can tailor their risk management to the most current AML/CFT landscape.

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 1000 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Our Customers

Santander GEMINI OakNorth Bank CURVE

raisin. Munich RE Lydia OANDA

Get in Touch

EMEA
London

+44 20 7834 0252
Demo Request

AMER
New York

+1 (646) 844 0841
Demo Request

APAC
Singapore

+65 6304 3069
Demo Request

COMPLY ADVANTAGE®

ComplyAdvantage.com

For details on the source materials used in this guide, please visit complyadvantage.com/insights