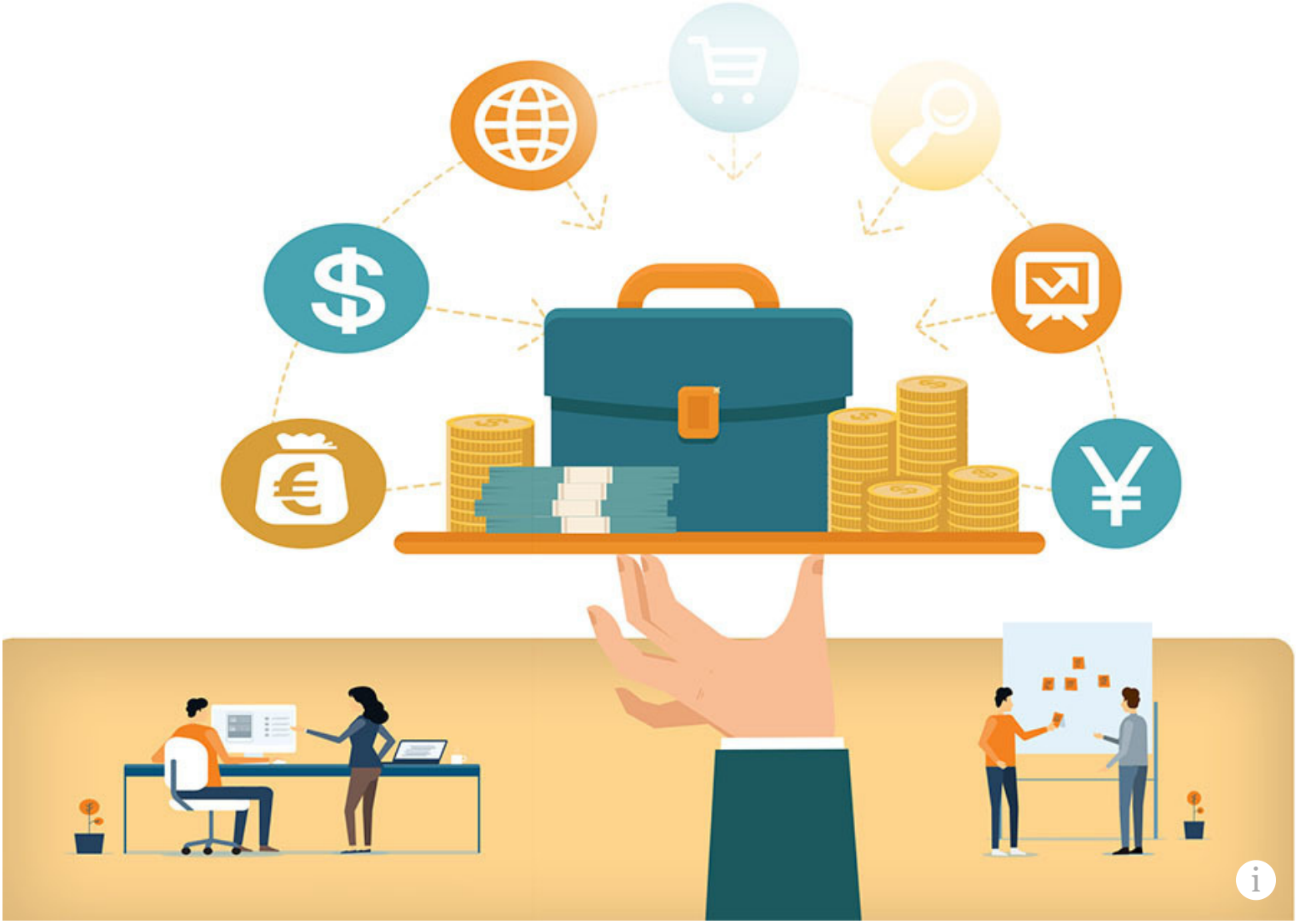
Mitigating Risks of Banking Money Service Businesses

Building an Appropriate BSA/AML/OFAC Compliance Program

BY JIM TREACY, CPA



NON-BANK FINANCIAL INSTITUTIONS—including money services businesses (MSBs)—are extremely diverse, ranging from large multi-national corporations to small,

independent businesses that offer financial services only as an ancillary component of their primary business. The range of products and services offered, and the customer bases served, are equally diverse. As a result of this diversity, the risk to bank these entities may be higher because of their potential of money laundering.

When banks offer services to an MSB, the banks must ensure they appropriately assess the risks associated with offering these services to the MSB and that the bank is prepared to take steps necessary to comply with applicable Bank Secrecy Act/Anti-money laundering (BSA/AML) regulatory requirements. An institution that fails to comply with BSA/AML regulations when banking MSB customers will be exposed to regulatory scrutiny, including the possibility of civil money penalties.

Traditionally, an MSB is defined as a person or entity providing any of these five types of financial services: a dealer in foreign exchange, a check casher, an issuer or seller of traveler's checks or money orders, a provider of prepaid access cards, and/or a money transmitter. In particular though, check cashers, dealers in foreign exchange, and issuers or sellers of traveler's checks or money orders must exceed the $1,000 per person per day rule in order to meet the Financial Crimes Enforcement Network's (FinCEN's) definition of an MSB. This distinction may become relevant when assessing your institution's overall MSB risk appetite and the risk associated with individual MSB customers. Moreover, FinCEN has also augmented the definition of money transmitter to include administrators or exchangers of virtual currency. (See **www.fincen.gov/money-services-business-definition#:~:text=The%20term%20%22money%20services%20business,more%20of%20the%20following%20capacities%3A&text=(4)%20Seller%20or%20redeemer%20of.**)

BSA/AML Compliance Program

Banks are required to perform an enterprise-wide BSA/AML/Office of Foreign Assets Control (OFAC) risk assessment to ensure the BSA/AML/OFAC program in place adequately mitigates the risks related to money laundering and terrorist financing. The inherent risks considered include the products and services offered, the bank's customer base, and geographies served. If the bank allows MSBs to open bank accounts and use the bank's products and services, it must include them in the enterprise-wide risk assessment. Other information to be considered at the enterprise level includes the number of MSB customers the bank has, the types of products and services offered by these entities, and the geographies they serve.

Non-bank Financial Institutions (including MSBs) are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component of their primary business (e.g., grocery store that offers check cashing). The range of products and services offered, and the customer bases served, are equally diverse. As a result of this diversity, some of these entities may be at lower risk and some may be at higher risk of money laundering.

The control environment established at the bank should then be assessed to determine if policies and procedures appropriately mitigate the inherent risks related to MSB customers. The BSA/AML/OFAC residual risk for the MSB portfolio or business segment can be calculated once a determination is made on the effectiveness of the control environment offsetting inherent risks.

After the BSA/AML/OFAC risk assessment process is completed, management must assess whether it is comfortable with the overall level of residual risk related to banking MSBs, and confirm this risk is consistent with the overall risk appetite of the institution. As noted above, MSBs vary widely in size and products and services offered and therefore the related risks will differ depending on these factors.

Another important consideration is the bank's strategy with regard to its MSB clients. For example, is the bank's goal to provide services only to smaller local MSB businesses which offer limited products and services? Or is the goal to serve more complex MSB customers, that may offer diverse products and services, potentially internationally? Bank management should understand its MSB customers and only accept those that are within its risk appetite and can properly manage the BSA/AML risk of those customers.

Ongoing evaluation of the BSA/AML Program related to MSBs will provide management with assurance that controls are effective and the attendant risks related to these customers remains commensurate with the bank's risk appetite. Banks should ask themselves:

- Does the program factor in any changes to technologies used or geographies covered?
- Have MSBs offered new products and services to its customers and is the bank adequately monitoring this new activity?

- Has there been an increase in the filing of suspicious activity reports (SARs) related to MSB customers?

The program then should be adjusted as needed to ensure it addresses current and emerging BSA/AML/OFAC risks.

It's critical that a bank's BSA/AML program is consistent with the risk profile of the bank's higher risk customers—such as MSBs—to avoid regulatory scrutiny. While civil money penalties typically occur after BSA/AML violations are noted by examiners, there have been recent penalties assessed to banks for having an inadequate BSA/AML/OFAC program, given the bank's higher risk customer base.

Because MSBs often conduct a high volume of cash transactions and may offer international transfers of funds, they can represent a higher risk of being involved in money laundering and terrorist financing-related activities and so the risk assessment and mitigation controls are especially important. These BSA/AML/OFAC risks can be mitigated through implementation of a strong BSA/AML/OFAC program, starting with due diligence and the development of customer risk profiles.

Initial Customer Due Diligence and Client Level Risk Assessment

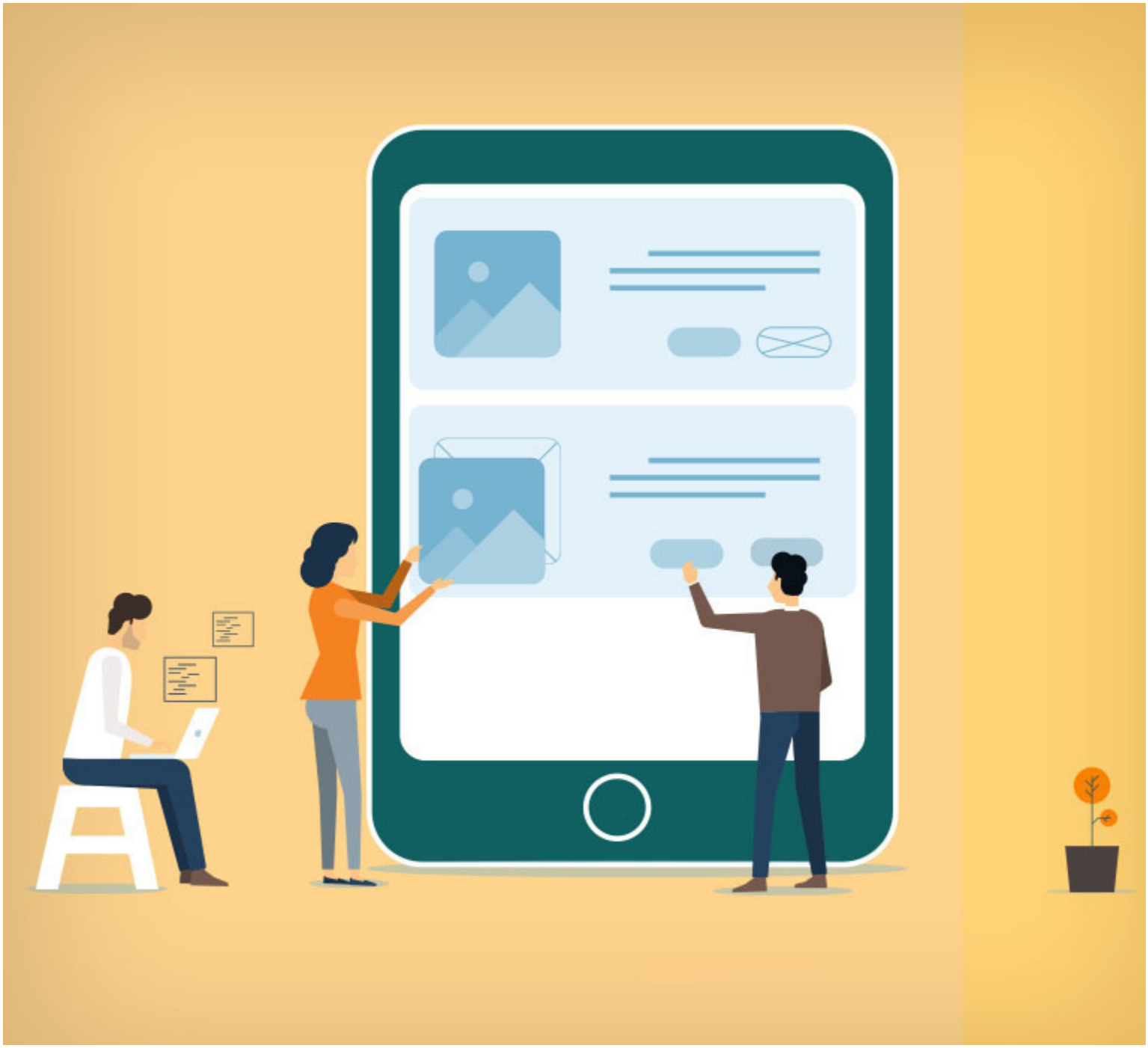
In addition to performing an MSB risk assessment at the enterprise-wide level, the bank must also develop a customer risk profile for each individual MSB. This can be accomplished through the initial customer due diligence and risk assessment processes performed at the time the account is opened. These steps are critical to properly identifying and controlling the risks associated with each individual MSB relationship.

Typically, this can be accomplished by establishing a series of questions for all new business customers regarding the types of activities they will engage in and determining whether this activity falls into the definition of an MSB. The customer due diligence (CDD) process needs to include gaining an understanding of the purpose of the account as well as the nature and volume of transaction activity that will occur. For example, will the activity include sending funds to foreign-based agents and what dollar transaction limits will apply to the MSB's customers? Additionally, it may be important to differentiate between those that meet the FinCEN definition (i.e. the threshold $1,000 rule) and those that simply provide MSB type services but fall short of the regulatory definition.

Other minimum CDD expectations for MSBs also include applying the bank's customer identification program (CIP) procedures; confirming proper registration with and licensing by state, local and federal agencies (e.g. FinCEN); determining whether the MSB is an agent of a larger MSB; and based on results of the risk assessment, whether further due diligence is required.

If the bank determines that the risks presented by the MSB are sufficiently elevated, the bank will want to consider performing additional CDD or even enhanced due diligence (EDD). This may include:

- Reviewing the MSB's BSA/AML/OFAC program and their operational procedure;
- Determining if appropriate compliance training is being provided to the MSBs employees;
- Reviewing agent lists (if applicable);
- Reviewing the results of the most recent independent BSA/AML audits or state agency exams performed; and
- Conducting site visits.



When banks offer services to an MSB, the banks must ensure they appropriately assess the risks associated with offering these services to the MSB and that the bank is prepared to take steps necessary to comply with applicable BSA/AML regulatory requirements.

Employees performing CDD/EDD should also consider visiting the MSB's physical business location, if there is one. This allows the bank to confirm the products and services offered based

on the signage and pamphlets available at the site. This may also allow the bank to observe the practices being followed, such as how the business engages with its customers and whether these practices follow customary procedures established for the industry.

Another CDD/EDD risk assessment process the bank might want to include is negative news searches on the business and the principal owners as well as any third parties with whom the MSB works. This process will help identify any legal or potential reputational concerns that should be considered prior to opening the account. For example, if the primary owner has a history of lawsuits or negative coverage in the media, then the institution should strongly consider not opening the account.

MSBs should be risk-rated, and risk rating can be performed in an automated manner. One way is through BSA/AML software that determines the risk, based on customer information entered into the system, as well as by considering the transaction activity occurring through the customer's accounts. A manual process can also be used to determine the risk rating based on a set of predetermined factors that assign a score based on the answers. Banks with lower risk appetites may automatically consider any MSB customer to be a high-risk customer. Banks with higher risk appetites will likely have a more granular process in place to discern the risk rating to be assigned to MSBs based on the:

- Types of activity;
- Volumes of transaction activity;
- Other bank services used;
- Customer base;
- Geographies served; and
- Any SARs that may have been previously filed by the bank.

Regardless of how the risk rating is performed, it should be documented and properly supported to justify the ultimate risk level assigned. Establishing a sound risk rating process will help to ensure that the level of oversight performed by the bank is commensurate with the level of BSA/AML risks faced from each MSB. This is a key aspect in properly managing risks related to MSBs.

The risk assessment should consider whether the customer is acting as an MSB on its own behalf or whether the entity is acting as an agent for another MSB. Entities that are engaging in MSB activities on their own behalf and fit the FinCEN definition are required to register with

FinCEN. Banks can confirm this registration on FinCEN's website. If the entity is acting as an agent, the entity should be listed as such on the MSB's list of agents that BSA regulations require the MSB to maintain and update annually and retain for a period of five years. For the MSBs acting as an agent, banks should ensure that the customer is not engaging in activities outside of the agent relationship that would require the customer to register as an MSB itself. Banks should also ensure MSBs who are serving as agents for another MSB are provided policies and procedures from the MSB and expected to follow them.

It is also critical that the bank document its CDD/EDD efforts to evidence it was performed and to assist in determining if any significant changes have occurred in future reviews. This could include using a written or electronic checklist to ensure that all relevant elements are considered at the time of account opening. It is also a good practice to have the BSA/AML Officer, senior management, or a committee including representatives from these areas review all information collected and decide whether an account should be opened for the MSB. However, the size of the financial institution will dictate whether or not this practice should be implemented. Larger institutions will want to focus on having well-defined MSB policies and solid risk tolerance statements to guide their MSB customer decisions, rather than the committee approach.

Regardless of the method chosen, the bank will need well-defined processes to maintain control of the number and the types of MSBs it banks and limit the risk of opening an account for an MSB that is not consistent with the bank's risk appetite.

The CDD information gathered on the MSB at account opening should be sufficient to allow the bank to form an expectation regarding the dollar amounts and types of transaction activity that will occur. This expected activity level will then serve as a baseline to assess whether any potentially suspicious or unusual activity has occurred. After the account has been opened for a specific period of time (e.g., three months), the bank should review the MSB's transaction activity to confirm that actual activity is consistent with the expected activity. This allows for timely detection of activity that is inconsistent with the stated purpose of the account or that is not consistent with the products or services offered by the entity.

Ongoing Monitoring of MSB Customers

The frequency of ongoing monitoring of MSBs should be based on the assigned BSA/AML/OFAC risk rating. The higher the risk rating, the more frequently monitoring should be performed. Each periodic review should: verify that transaction activity is consistent with the expectations developed when the account was opened; assess whether the products and services offered by

the customer are consistent with what was disclosed at account opening; provide an understanding of the cause of any material changes in transaction activity; and determine whether any activity appears to warrant the filing of a SAR. If the actual activity exceeds management's BSA/AML/OFAC appetite, then management should consider whether to close the account.

For example, if an MSB indicated it will only cash checks for consumers up to a dollar limit (less than $1,000 per person per day), but the periodic review detects that the MSB is cashing larger checks, or checks for unknown business entities, then management should determine whether the filing of a SAR is warranted. Additionally, if management is not comfortable with this activity, the bank should consider what steps to take, including possibly closing the account.

Ongoing monitoring should also confirm the MSB continues to maintain any licenses required to legally operate. If warranted, the bank should obtain an updated BSA/AML/OFAC Program from the MSB to verify it remains appropriate and any changes to its business practices are properly documented. It should also confirm the MSB provided employee training and completed an independent BSA/AML audit. Failing to perform periodic monitoring of these customers could lead to the bank failing to identify or report suspicious activity, which has the potential to lead to further regulatory scrutiny.

The frequency of ongoing monitoring of MSBs should be based on the assigned BSA/AML/OFAC risk rating. The higher the risk rating, the more frequently monitoring should be performed.

Based on the results of the periodic review, the risk rating for the MSB should be reassessed as necessary. This will help ensure that periodic monitoring is occurring at appropriate intervals. Additionally, the ongoing monitoring of MSBs through the normal "tripwires" that the bank has in place should continue throughout the year in order to detect any potential unusual or suspicious activity, and may include the use of automated alerts set up in the bank's BSA/AML software and by having employees report any potentially suspicious activity that they observe.

While FinCEN has stated that it does not expect that banks serve as de facto regulators for these entities, and will not hold banks responsible for their MSB customers' compliance with BSA and other applicable Federal and state laws and regulations, banks are expected to manage risk associated with all accounts, including MSBs.

In addition to the above, adequate automated or manual monitoring should be performed to identify any customers who are acting as an MSB but have not reported this fact to the bank. This could include reviewing the core system's high-dollar activity report that identifies customers who may be engaging in MSB-related activities, such as through the cashing of checks for customers, based on the level of cash activity through the customer's accounts. Other potential approaches include keyword searches, or North American Industry Classification System (NAICS) code-driven analysis.

Including information on MSBs in periodic BSA/AML management and Board reporting will help management assess whether it is comfortable with the activity for MSB customers and understand the overall BSA/AML risks faced by offering these services. The topics to be covered with management include new MSBs opened, a discussion of the general nature of activity that caused the bank to file a SAR, the status of the ongoing periodic monitoring performed on MSBs, any challenges or issues noted with this periodic monitoring, as well as any other significant developments with MSBs. As stated in BSA/AML regulations, the Board is ultimately responsible for compliance with these regulations and therefore it needs to be provided enough information regarding MSB activities so it can ensure appropriate oversight is occurring and take action when required.

MSB Red Flags

While performing periodic monitoring or investigating BSA/AML system generated alerts, the bank should be on the lookout for red flags that raise potential concerns for MSB customers. These red flags include:

- Insufficient or suspicious documentation provided by the customer;
- Suspicion that efforts are being made to avoid BSA/AML recordkeeping requirements;
- Activity that is outside of the expected activity for the entity based on the CDD/EDD performed;
- Transactions that involve jurisdictions posing heightened risk for money laundering or the financing of terrorist activity;
- Activity with international jurisdictions that are not expected;
- Deposit or withdrawal of currency significantly in excess of expected amounts without any justifiable explanations; or
- An unusual pattern of transactions.

The bank should determine whether the facts and circumstances involved in these red flags warrant the filing of a SAR. If a SAR is filed, the bank must continue to review the activity for the next 90 days to determine if the suspicious activity has continued and thus, whether to file a continuing report. As noted above, failing to detect and report suspicious activity has the potential to lead to criticisms from examiners.

In conclusion, management must be confident its BSA/AML/OFAC Program adequately identifies and mitigates risks faced from MSB customers and monitor for any changes to the level of risks faced from these customers over time. It is critical that the overall BSA/AML/OFAC risk assessment and the BSA/AML Compliance Program are updated as needed to reflect any changes that occur. Although banking MSB customers comes with BSA/AML risks, these risks can be managed through a strong and effective BSA/AML/OFAC Program.

ABOUT THE AUTHOR

JIM TREACY, CPA, is a director with CrossCheck Compliance LLC and a regulatory compliance and internal audit professional with over 20 years of operational, financial, and compliance experience in the financial services industry. Jim is also a Certified BSA Officer. His clients include financial services organizations of all sizes, from small community banks to large national organizations. Prior to joining CrossCheck, Jim was a manager with Jefferson Wells International where he was responsible for execution and management of client engagements. He previously held positions with Witkowski & Associates (a CPA firm), Metavante (now FIS), U.S. Bank, and Fleet Mortgage. Jim can be reached at **jtreacy@crosscheckcompliance.com**.