9 Common Weaknesses in a BSA/AML Program-
And How to Find Them before Examiners Do

Over the last several months, there have been headlines warning of increased scrutiny by examiners on BSA/AML and dire consequences for banks unprepared for their exams. Many financial institutions, both big and small, are being hit with enforcement actions and severe penalties.

What should you be looking for and what can you do to shore up your BSA/AML program to ensure you don't fall under the regulator's lash? Let's address 9 of the most common weaknesses.

The first four weaknesses all address lack of structure or organization. Many institutions have been criticized for not having an effective suspicious activity monitoring program. It must be risk based, but to be effective it must also include four basic components.

Weakness #1- Identification or alert of unusual activity including:

- **employee identification**
- **law enforcement inquiries or other referrals**
- **transaction and surveillance monitoring system output**

A good program uses a combination of methods to effectively identify suspicious activity. (See the FFIEC BSA/AML Exam manual for more detail).

The decision of which method(s) to use is risk based, but don't just rely on system reports or alerts. If frontline employees are not reporting any activity, an examiner may take that as a sign that staff training is inadequate. (See #9- Training below).

Weakness #2- Managing alerts: Focus on the processes used for investigation and evaluation. Procedures must include a clearly defined escalation process from point of initial detection to completion of the investigation. Adequate and well trained staff needs to be assigned to the identification, evaluation, and reporting of suspicious activity.

If you have a significant concentration of a higher risk product, service or entity, you may need to employ additional staff to comprehensively monitor suspicious activity.

Weakness #3- SAR decision making: The findings after research and analysis should be forwarded to the final decision maker. This process should be clearly written in your policy and procedures, in addition to defining whether it is an individual or a committee who makes the final decision. The final decision to file or not file must be thoroughly documented with the inclusion of a solid justification for that decision. “This is the way the customer has always behaved” is **NOT** a solid justification. Instead, document the reason why the activity is not suspicious for that customer. Examiners are instructed to not criticize individual no-SAR decisions, unless the failure was significant or accompanied by evidence of bad faith. Instead, they are asked to concentrate on whether the institution has an effective SAR decision making process.

Weakness #4- SAR Completion and Filing: Policies and procedures must be in place to ensure that SARs are not only filed in a timely manner, but are complete and accurate with a narrative that provides a sufficient description of the activity along with the reason of why it is suspicious.

SAR rules require that a SAR be filed “**no later than 30 days from the date of the initial detection of facts that may constitute a basis for filing a SAR,**” (or 60 days if no suspect was identified). In simple English, this means no later than 30 days from the date you determined it to be suspicious and SAR reportable. The institution’s AML system or initial discovery of the activity may flag the transaction; however, this should not be considered “initial detection.” The countdown does not begin until an appropriate review has been conducted and the “SAR decision maker” has determined it to be SAR reportable. The review should still be completed within a reasonable period of time to assist law enforcement, but what constitutes as “reasonable” will vary. The key factor is that the bank has established adequate written procedures and that those procedures are being followed.

If the activity is ongoing, FinCEN’s guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days. A clarification was provided by FinCEN in the “SAR Activity Review-Trends Tips & Issues” (Issue 21- Section 4) regarding the deadline for the filing of ongoing SARs. The clarification reads: “Financial institutions may file SARs for continuing activity **after a 90-day** review with the actual filing deadline being **120 days** after the date of the previously related SAR filing.”

The absence of any of the four components above could make the effectiveness and structure of your program fall apart and fail. Look closely at your existing program and ensure that your policies and desktop procedures clearly document all four processes.

Weakness #5- Risk Assessment Does Not Justify the Conclusions: Examiners need more facts, justifications and documentation in the risk assessment. They may not disagree with your overall conclusions, but to properly examine that you have a sufficient BSA program, they have to understand the risks at your institution. Without any supporting documentation, they will not know how you came to that conclusion.

Provide documentation and data to back up your conclusions. For example; if you say you have low geographic risk, explain where your institution and your customers are located. Is it a high intensity drug trafficking area or a high financial crime area? Do you have significant international activity and is it with high risk jurisdictions? If you have identified any significant risks, what types of mitigations are set in place at your institution?

Update your risk assessment on a periodic basis. Periodic may mean more frequent updates than annually if your institution has major events such as mergers or acquisitions.

Weakness #6- Monitoring Program Has Not Been Updated Recently or Independently Validated:

After updating the risk assessment, management should review the suspicious activity monitoring procedures and programs established along with filtering criteria and thresholds to ascertain they are still effective for the risk at your institution. Ensure you are keeping up with new current technology trends and emerging threats.

In addition, the monitoring system's programming methodology and effectiveness should be independently validated to ensure that they are detecting potentially suspicious activity.

Have a periodic data validation conducted of the data importing into your systems to ensure you have the data you need to monitor suspicious activity.

Weakness #7- Customer Due Diligence (CDD) Process Not Effective: Having a strong and capable CDD process is more than just collecting CIP info with verification upon proper ID. The purpose of CDD is to enable the bank to predict with relative certainty the type and volume of activity the customer will be conducting. An institution is obligated to collect sufficient customer information to implement an effective suspicious activity monitoring system. This information should also provide the institution with the ability to differentiate between lower-risk and higher-risk customers at account opening. (*This is now being identified as the 5th pillar of a suspicious activity program, along with the collection of beneficial ownership information on certain business entities starting in May 2018.)*

When opening a business account, identify the business type. If it is determined they are a higher risk entity (i.e. nongovernment organization, professional service provider or nonbanking financial institution), ask for additional enhanced due diligence information. When opening a consumer account, identify the resident status, if they are a politically exposed person, or if they will be using their account for business purposes or conducting any international activity.

Remember customer due diligence is the cornerstone of an effective suspicious activity program. If you don't really know or understand your customer, how will you determine if their activity is unusual or suspicious?

Weakness #8- Identification and EDD of High Risk Accounts:
It is critical to identify your high-risk accounts. Although any type of account may be susceptible to money laundering or terrorist financing, some customers may pose more specific risks by the nature of their business, occupation, or transaction activity. The FFIEC manual provides guidance that during the risk assessment process, it is important that banks exercise judgment and not treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, banks should consider other variables, such as services sought, transaction activity and geographic locations.

Keeping this is mind, it is recommended that accounts are risk rated initially at account opening and then on a periodic basis to take into consideration the actual activity being conducted.

Once you have determined that a customer poses a higher risk, the bank should conduct further enhanced due diligence. Remember the goal of having a list of high risk customers is not simply to identify them. They are rated high risk because they pose a higher risk for fraud or money laundering, and therefore, you have an obligation to review them more closely and frequently to ensure they are not conducting suspicious activity or putting your institution at risk. The detail and scope of review will vary depending on the level of risk at your institution or the type of customer. A high-risk consumer may require collecting source of wealth/funds and for you to review their account for unusual activity, whereas an MSB may require a site visit and increased scrutiny to ensure that their activity is not unusual.

Weakness #9-Training Not Effective:

Oftentimes when a weakness in a BSA program is identified, it is tied back to training. Training is crucial as it is one of the original 4 pillars to an effective program. Hot buttons include:

- BSA training/policies and procedures should be provided to new employees as part of employee orientation prior to hitting the trenches.
- BSA/AML training is critical to all business lines including branch staff, loan department, trust department, back-shop operations, etc.
- Training should be tailored to the employee’s specific duties.
- Training should include not only BSA and how to identify suspicious activity but also include the bank’s internal policies, procedures, systems and how to escalate any suspicious activity to the appropriate department.
- BSA officer should receive periodic training that is relevant and incorporates current developments, emerging risks/trends and changes to the BSA and related regulations.

- The Board of Directors needs BSA training to understand the importance of BSA/AML regulatory requirements, ramifications of noncompliance, and risks posed to the bank.
- Staff utilizing BSA/AML monitoring systems need to be provided with comprehensive and ongoing training to maintain their expertise.
- Banks should document and maintain training and testing materials, dates of training and attendance records, and should be made available for examiner review.

Over the last few years, regulators and examiners had been concentrating their efforts on problems stemming from the recent financial crisis. But now the trend has turned back to money laundering and the Bank Secrecy Act. So be warned that even if your last exam went well or was a non-event, don't have the same expectations for the upcoming BSA/AML exams. Remember to evaluate and review your program for any weaknesses on a periodic basis.