DataWalk

Avoiding AML Enforcement Actions: Three Best Practices for Financial Institutions

DataWalk

Executive Summary

As the compliance officer for a bank's AML/BSA program, you know that getting penalized with a regulatory enforcement action has a profoundly negative impact on the reputation of your financial institution. Depending on their severity, enforcement actions may also result in personal fines, suspension, or other actions against you that may end up costing you your career.

In this whitepaper we recommend three best practices for AML/BSA compliance officers to minimize their risk of being subject to regulatory enforcement actions:

- Establishing quantitative risk assessments and profiles
- Maintaining AML program sustainability
- Implementing advanced AML alerting software

The last of these practices is especially effective when such software can be customized and updated to meet rapidly changing regulatory requirements, while supplementing and enhancing existing AML software.

Introduction: AML Requirements

The Federal Financial Institutions Examination Council ("FFIEC") and Financial Crime Enforcement Network ("FinCEN") describe in detail the requirements of implementing an effective AML program. The basic building blocks include:

1. Designating an AML Compliance Officer (AMLCO)
2. Establishing a risk profile through an AML risk assessment
3. Implementing a system of internal controls to ensure ongoing BSA compliance
4. Establishing a Customer Due Diligence (CDD) Program
5. Training appropriate personnel in compliance requirements
6. Engaging in independent testing for compliance

A financial institution that fails to adequately address any of these requirements puts itself at risk of an enforcement action.

This paper focuses on *requirements 2, 3, and 4* in particular, which are the areas most likely to trigger an enforcement action. Fortunately, these are also the areas that can benefit most from newer AML software solutions currently on the market that are built with advanced graph and AI/ML technology. These solutions target the areas of oversight and vulnerability among those three requirements that frequently lead to AML enforcement actions.

Causes & Factors Contributing to AML Enforcement Actions

Inadequate Assessment of AML Risk

One primary cause for AML enforcement actions against financial institutions is the simple failure to properly implement an effective AML program to begin with. Without an effective program, a bank is unlikely to establish an effective risk profile and will therefore fail to properly assess the risks associated with the products and services it offers, which in turn often results in enforcement actions against that bank. There can be many reasons for an improper assessment, but they tend fall to into just a few categories:

- Incomplete inventory of the products and services offered
- Inadequate inventory of source systems that contain client information and transactions
- Insufficient understanding of the AML risks associated with all of the products and services offered

Ineffective Internal, Ongoing Controls

Another cause for AML enforcement actions is an institution's AML transaction monitoring system being unfit for the relevant products and services it offers. Some examples of how this system might fall short are:

- Basic AML scenarios (e.g., structuring, rapid movement of funds, etc.) are unable to identify enterprise-wide AML trends, patterns, and emerging risks.
- Large banks with complex business models that rely on non-customizable AML transaction monitoring scenarios and KYC databases are unlikely to capture more sophisticated money laundering schemes (e.g. money laundering via syndicate loan products).
- Improper tuning and optimization of AML scenarios leads to an excessive number of false positive and non-productive transaction monitoring alerts. When combined with chronic understaffing and staff turnover, this creates an unsustainable environment of backlogs, poor alert clearance processes, and most importantly, missed suspect activity.

In addition to the technical shortcomings of its transaction monitoring system, an institution's organizational structure might exacerbate its vulnerability to AML enforcement actions. For example, if departments or business lines are siloed, as they are in many banks, staff will be effectively unable to share information about clients, investigations, fraud, or suspicious activities. As a result, emerging threats are likely to go undetected, such as when multiple clients operating across multiple business lines act in concert to launder money without being detected. Understaffing, staff turnover, and inadequate training can also lead to inadequate review of AML transaction alerts and incohesive KYC risk profile information.

Inadaptability of CDD Program

A third cause for AML enforcement actions might be that a bank's existing transaction monitoring system is not flexible enough to adapt to new regulatory requirements nor enhanced to respond to emerging risks. For example:

- The FinCEN CDD Rule requires financial institutions to "conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information." However, most existing AML transaction monitoring systems are unable to link client KYC data to transaction monitoring (e.g. generate an alert to update customer information when the actual account activity does not match the expected activity as noted in the client new account forms).
- Real world events, such as the Russian invasion of Ukraine, can disrupt normal daily processes such as AML alert clearing or KYC profile updates. In this instance, existing investigators may need to be reassigned to evaluate the financial institutions' exposure to Russia. This disruption to normal activities can result in problematic backlogs of AML and KYC processes.

A CDD program that fails to adapt to such new requirements may result in enforcement actions.

How to Minimize the Risk of AML Enforcement Actions: 3 Best Practices

Establish Effective Risk Assessments & Profiles

Performing a comprehensive AML risk assessment is a crucial first step in developing an effective AML program. Without a proper evaluation of AML risks associated with the products and services it offers, your financial institution is more likely to be subject to regulatory enforcement actions.

To attain a proper risk assessment, input is critical from subject matter experts (SMEs) who understand how to run a robust AML operation and can provide specific guidance on the inherent AML risks associated with each individual product or service your financial institution offers. What's more, your AML and KYC systems must be flexible enough to ingest the data that SMEs deem necessary to evaluate those risks.

Due to the size and complexity of many banks, along with the sheer number of transactions processed, SMEs may not be able to fully grasp the extent of the risks using their existing tools. It's important for your institution, therefore, to have technology in place that's sophisticated enough to detect possible gaps in your existing AML program and to quantify the level of risk associated with each product and service your bank offers.

Maintain AML Program Sustainability

A second important practice to help minimize your likelihood of being subject to AML enforcement actions is to ensure the long-term sustainability of your AML program. One step to doing so is to implement a risk-based approach to your AML program. This will allow your institution to allocate resources more effectively to areas where there is a higher risk of money laundering.

Another step to ensuring your AML program's sustainability is to implement an AML software solution where repeatable, high-volume activities occur. It's important to be aware, however, that the vast majority of existing AML software scenarios are not easily customized to a bank's unique business model. This often leads to an excessive frequency of false positive and non-productive alerts. Clearing these types of alerts is an expensive process that also leads to staff turnover, backlogs, and missed suspect activity.

An effective way to address the limitations of your existing AML software is by supplementing it with the latest generation of AML software solutions, which leverage technologies such as graph and AI/ML. Graph technologies enable you to more easily detect suspicious conditions by considering relationships between entities within your data. With the AI/ML capabilities of such a solution, any error points or inefficiencies in your existing AML scenarios can be tuned out (on an ongoing basis) to ensure that your transaction monitoring scenarios are both effective and cost efficient.

Implement AML Alerting Software with Enhancement Capabilities

A third best practice to help you minimize enforcement actions against your AML program is to ensure that it can be upgraded and enhanced over time, with minimal cost and without disruption. Your AML program stays effective only if it's continuously up-to-date with current regulations and able to respond to newly emerging threats.

As many institutions have made significant investments in existing systems, in many cases the most practical approach is to supplement your existing systems with newer ones that are more flexible. Highly desirable are such solutions that can be quickly deployed and easily tuned for a variety of scenarios. This is another area where the latest generation of AML software solutions can help. Such a supplementary software solution can, for example, effectively integrate the data from your existing AML transaction monitoring and client KYC software to meet all the requirements of the FinCEN CDD Rule.

Using an AI-driven AML software solution, you can also implement customized processes to:

- Generate scenarios that monitor activity specific to your bank's business.
- Enhance the client onboarding process by generating instantaneous client risk profiles, which can be adjusted in real time and without human intervention. The methodology used in generating profiles can be customized according to regulatory requirements or the specific trigger events selected (e.g., SAR filings, subpoena, negative news).

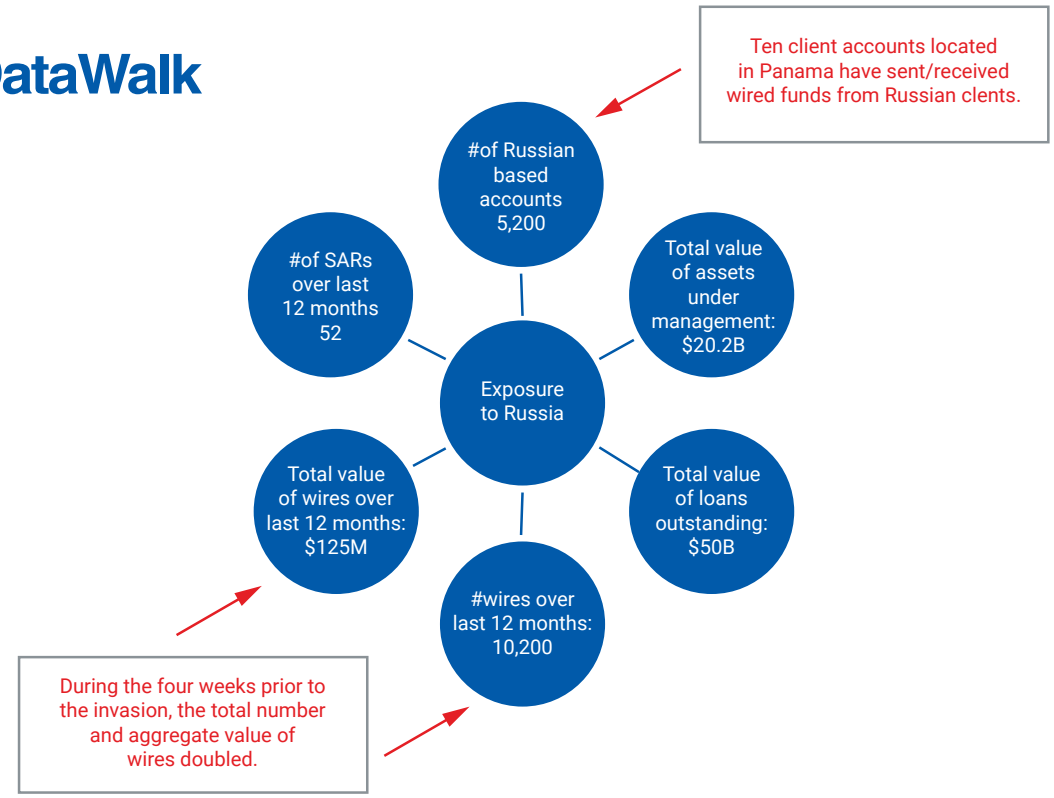
Such supplementary AML Software can also enhance a number of your current AML program's other capabilities. It can, for example, accelerate your bank's investigative process by automating link visualizations and integrating your existing workflows with enriched data (e.g., public data, enterprise-wide client data, and transactions) to create 360-degree graphical views of a client being investigated.

Scenarios Where AML Enhancement Capabilities Come Into Play

Below are a few examples of how these newer AML software solutions can improve your financial institution's AML Program.

Investigations

Following the Russian invasion of Ukraine, an AMLCO might have been compelled to conduct a quick risk assessment of their bank's exposure to Russia. Using advanced AML software, an analyst could quickly generate an easy-to-read snapshot of risk without complex coding. Specifically, the investigator could quickly grab data from systems for client onboarding, wire transfers and other transactions, or AML investigations in order to create a visualization to present to the AMLCO and other senior management, as shown in the figure below. The investigator could also add material findings, as indicated by the annotations in red.



Customer Due Diligence

A corporate client involved in the paint contracting business is onboarded by a local branch of a financial institution. Because the purpose of the account is coded for basic business operations with no planned offshore or 3rd-party wires, the risk profile is systematically designated as “Low Risk”. However, several months after account opening, the client sends a 3rd-party wire to Panama. The AI-driven AML software, which monitors all activity and flags any that’s unexpected, immediately increases the risk profile to “High Risk” and sends an alert to the bank’s AML Compliance Office for further review, as shown in the table below. This ongoing transaction monitoring is a key requirement of the CDD Rule that may be lacking in existing AML Programs.

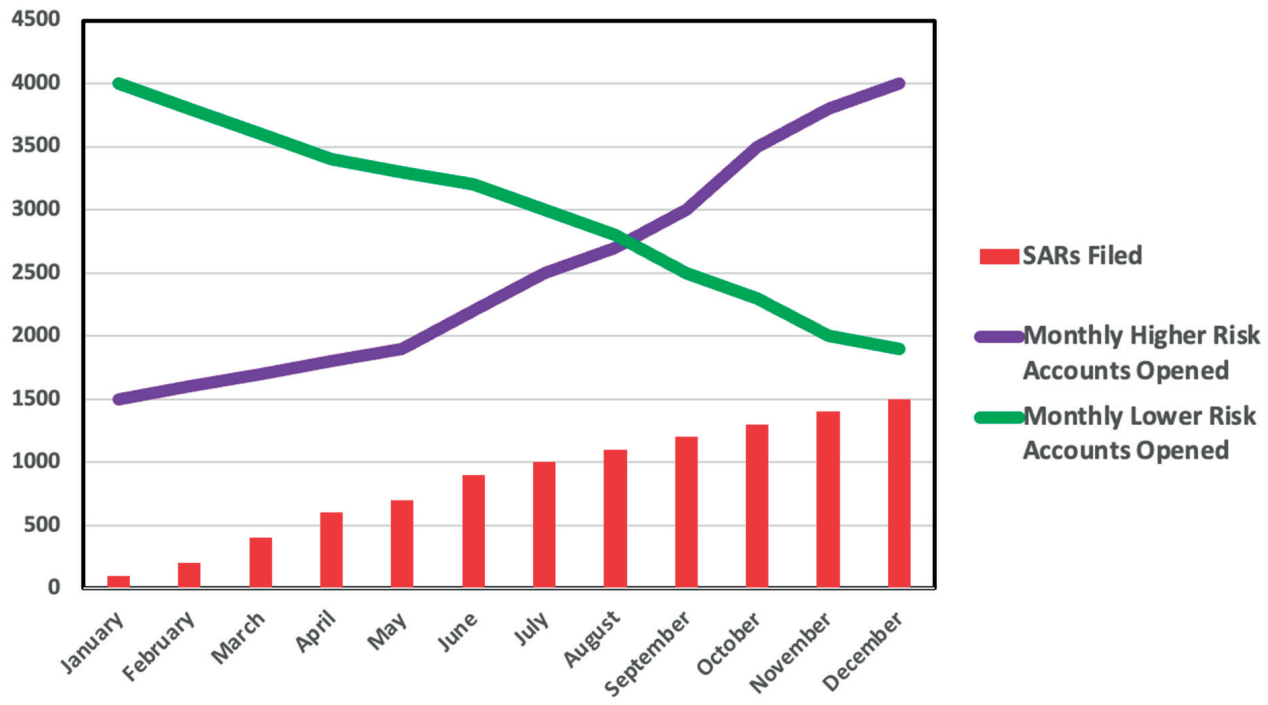
Client Profile		Previous Risk Rating	New Risk Rating	Reason for Change	Action Required
Category	**Response**	Low	High	Client sent offshore wire transfers to a 3rd party in breach of expected activity noted in Client Profile.	1. Confirm with client purpose of new activity 2. Obtain Manager Approval for New Activity 3. Add to Enhanced Monitoring
Client Type	Corporation	**Transaction Details:**			
Purpose of the Account	Business Banking	**Date**	**Account#**	**Account Name**	**Sender/Beneficiary**	**Amount**	**Country**
Client Business	Paint Contractor	2/2/23	123-ABCD	Painter Inc	Pixel Inc	$100,00	Panama
Client Source of Wealth	Business Income						
Location of the Client	USA						
Products/Services	Checking, Wires						
Reputation	No Negative News						
Located Offshore	No						
Offshore Wires	No						
3rd Party Wires	No						
Risk Event	No						

DataWalk

Risk Trending

In the process that AML compliance offices use to obtain information in a preferred format, those wishing to examine trending metrics generally would need to submit a Business Requirement Document (BRD) to their IT department, which would include cost estimations along with approvals, prioritizations, and months of testing. However, modern AML software solutions enable users to easily integrate and view relevant AML data sources into an easy-to-read and flexible visual chart, such as a knowledge graph. With the visualized data that a knowledge graph provides, emerging risks and trends are easy to identify. The chart below illustrates that with an increase in the number of high-risk clients, the number of suspicious activity reports (SARs) has also increased. An argument could then be made to request that senior management approve additional headcount to handle the increased workload and avoid backlogs.

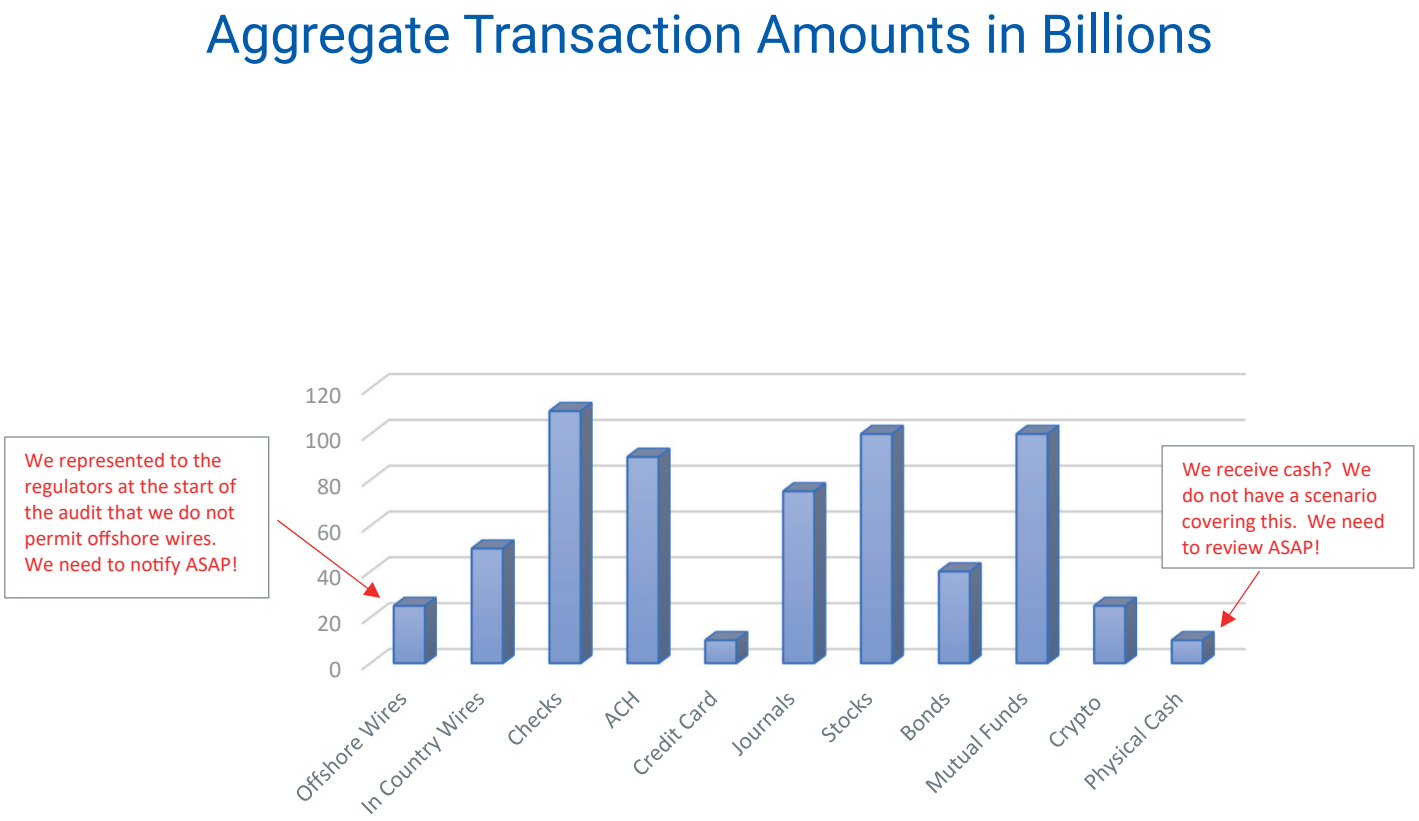
Monthly Account Opening Trends vs SARs Filed



DataWalk

Holistic Analysis

A standard practice for financial institutions is to perform AML risk assessments annually. Such assessments are typically done by non-SMEs, often resulting in the failure to identify potential gaps in AML coverage. However, modern AML software solutions can be used by AML SMEs to perform ongoing risk assessments, ensuring that transactional activity is in line with their institution's stated business model. This can dramatically help in avoiding enforcement actions directly related to lack of controls. For example, a bank may not have implemented AML transaction monitoring scenarios covering cash deposits or offshore wires because it was unaware that this type of activity was permitted. By utilizing modern AML software, the AML SME can pull large amounts of data for analysis and identify the gaps quickly by creating a bar chart of transaction types and highlighting any gaps, as shown in the figure below.



Conclusion

AML enforcement actions against financial institutions often begin with an inadequate AML risk assessment, which in turn leads to the implementation of inadequate internal controls. To make matters worse, enforcement actions can be difficult to address if non-customizable AML technology is in place, preventing an AML program from quickly adjusting customer risk profiles and adapting to updated requirements. Such enforcement actions can result in significant financial penalties and remediation costs, which directly impact a bank's profitability. Furthermore, public knowledge of these enforcement actions can damage a bank's reputation, impeding its ability to attract and retain customers, partners, and employees.

In order to meet the current and future regulatory requirements and expectations, institutions should consider technology solutions that supplement and enhance their existing AML software platforms. It is also important to choose an AML software solution that can be quickly installed, customized, and updated to meet the rapidly changing regulatory environment.

It is well worth investing upfront in the proper AML software to minimize these risks. In the long run, efficient compliance with appropriate tools will help your institution avoid financial injury, reputational harm, and failure to meet internal goals.

About DataWalk

DataWalk provides a highly flexible next-generation software platform that utilizes both graph and AI/ML technologies, and can be used for AML/KYC monitoring and investigations. DataWalk can be quickly deployed, easily tuned for new scenarios, and utilized as a supplemental alerting system. For more information, visit datawalk.com.