Whitepaper

Five Takeaways from Wolfsberg Group Guidance on Monitoring for Suspicious Activity

Contents

Introduction

The recent Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity presents a paradigm shift in anti-financial crime thinking.

Traditionally, banks have employed a transaction-focused approach to monitoring for financial crime risk. The Wolfsberg Group's guidance advocates for a broader alternative: monitoring for suspicious activity (MSA).

To implement this guidance, banks will need monitoring systems that complement their risk-based approach. In this article, we discuss the Wolfsberg Group's recommendations and how banks should use MSA technology to make productive changes to their programs, comply with regulations, and mitigate financial crime risk.

Monitoring Then	Monitoring Now
Narrow	Broad
Transaction-based	Customer-based
Theoretical Risk	Crystalized Risk
Parallel Processing	Sandbox Development
Transaction Monitoring Only	Monitoring for Suspicious Activity (MSA)

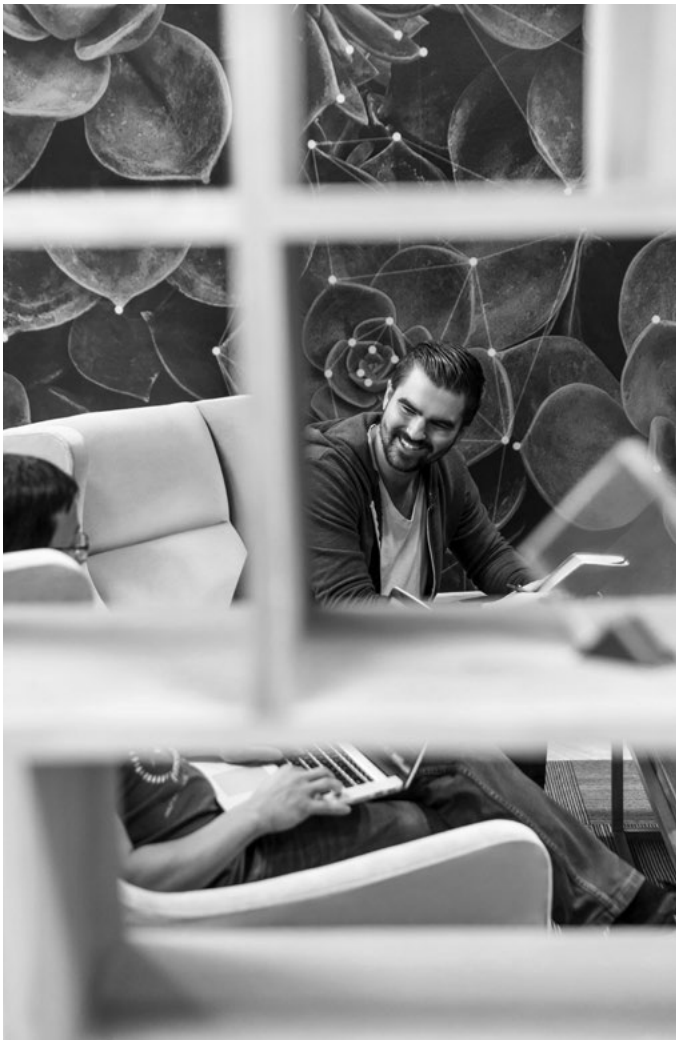
Prioritizing MSA System Effectiveness

The Wolfsberg Group paper advises banks to pursue net system effectiveness improvement over proving system equivalence, i.e., showing the same results.

This new approach encourages banks to “move away from legacy risk management approaches and towards higher-value, quality outputs.” It is a rejection of the “no SAR left behind” mentality and a call to focus on quality over quantity.

To move away from legacy risk management and get quality outputs, banks need MSA systems that effectively detect risk. These more modern systems feature machine learning, network analysis, and other cutting-edge risk detection methods. With effective MSA technology in place, banks can better comply with regulations, share valuable information with regulators, and mitigate financial crime risk.

If you’re thinking of introducing an MSA platform, proving perfect equivalence between the old platform and the new one may not be necessary. It’s more important to demonstrate that the net performance of the new platform outperforms the old one. Does it find more crime, faster, with less noise in the process?



Example:
Testing an MSA System

A bank runs a proof-of-value exercise, comparing its legacy monitoring system to a new MSA platform that uses AI anomaly detection and pattern recognition.

The legacy system finds three cases of suspicious behavior. The new system detects six total cases: two of the cases the legacy system found, plus four more.

According to the old way of thinking, the bank would deem the new system ineffective for missing one case. However, the new system has identified more risk (100% more, to be precise), making it much more effective than the old system. If a bank's baseline metric for effectiveness is the production of the exact same results, it will forego the opportunity to improve its financial crime controls and reduce risk. Measuring effectiveness based on how much risk an MSA system surfaces will yield better results in the long run.

Detecting Crystalized Risk

The Wolfsberg Group recommends prioritizing activities that monitor crystalized risk, rather than theoretical risk.

In this mode of thinking, if a bank can demonstrate that a given behavior isn't a reliable indicator of risk then it may redeploy its resources on more effective controls. This means that a risk-aware monitoring system empowers banks to run more efficient and effective MSA operations.

> Example: Monitoring Multiple Risk Factors

A rules-based system monitors for a certain type of behavior. For instance, it may flag transactions with round dollar amounts. In many situations (such as a peer-to-peer payment between friends), a round dollar amount signifies little to no risk. However, because the system has generated alerts, investigators must spend their valuable time reviewing them. An AI-powered MSA system can look at the bigger picture in a bank's data to better determine whether a transaction with a round dollar amount points to genuine financial crime risk. A bank using an AI-driven system can focus its efforts on feedback from crystalized risk whilst eliminating false positive alerts like these.

Taking a Sandbox Approach to MSA Technology

The Wolfsberg Group encourages banks to embrace sandbox development and reject parallel processing. Instead of running two systems at once, banks can prove a new system in a sandbox, sampling and testing before full implementation.

Parallel processing can be costly and time-consuming. This deters innovation. A sandbox approach to MSA technology empowers banks to develop and test new approaches in a cost-effective manner, transitioning with confidence to more effective financial crime risk management techniques.

Example: Evaluating a New System

A bank is considering the introduction of new technology to improve the effectiveness of its monitoring process. In scenario A, a full scope side-by-side comparison of the legacy platform and the new approach is deemed necessary. The cost to establish this process is prohibitive, so the bank maintains its compliant, but less effective, system.

In Scenario B, the bank plans a proof of value exercise to assess the uplift in effectiveness of the new system using a risk-based approach. The costs of this exercise, given the potential for further efficiencies, are acceptable to the bank. The evaluation demonstrates a measurable improvement in effectiveness, showing that the new system detects more financial crime risk, faster, with less noise.

Monitoring Both Customer and Transaction Data

The Wolfsberg Group urges banks to cast a wider net by Monitoring for Suspicious Activity (MSA), as opposed to transaction monitoring only:

> "Customer behavior and customer attributes, when combined with the consideration of transactions, can provide a broader insight into potentially suspicious activity."

In other words, monitoring both customer risk and transaction risk is more effective than focusing on transaction monitoring only. Technology that facilitates this comprehensive approach will help banks better comply with regulation and mitigate risk.

In the past, many banks have focused on transactions to assess customer behavior. Banks can only make an informed assessment of suspicion by considering the wider customer profile and broader customer behavior.

Example: Surfacing Suspicious Connections

A bank's customer sends $1,000 to 5 separate payees. Without any additional context, it's difficult to determine whether this behavior is truly of concern. However, with the additional information that all five of the payees were simultaneously created at an unusual time of day, the behavior immediately becomes suspicious. If a bank uses an MSA system that can effectively analyze both transaction and customer data, it will identify more of these connections and surface them for investigation.

HAWK

Using a Holistic MSA Technology Platform

The Wolfsberg Group suggests "developing and enhancing analytical capabilities to complement risk-based monitoring with targeted, timely data analysis."

This requires technology that can do more than just monitor transactions. Banks need the ability to evaluate customer risk in real time, detect connections to risky entities, and use contextual information to paint a more complete picture of financial crime risk.

By themselves, transactions can't tell the complete story. To assemble the full picture, you need an integrated approach that joins together customer and transaction data in a single digestible presentation.

Example: Identifying Connections to Risky Entities

A bank's MSA system raises an alert for a customer. The system's matching algorithm identifies a company shareholder with a similar name registered at the same address. It calculates a new risk rating for the customer based on the company's high-risk merchant category code and the risk level of its jurisdiction. The customer's profile was otherwise clean, so a transaction-focused approach would not have surfaced the risk inherent to the connection with the business entity. Because the bank's monitoring system has all the functionality necessary to identify these relationships, it effectively alerts the bank to more suspicious activity.

Banks can apply the following technologies on transaction and customer data to complement the holistic risk-based approach endorsed by the Wolfsberg Group:

Machine learning: Banks can use machine learning's predictive abilities to analyze vast amounts of transaction and customer data in real-time. This allows them to identify patterns and anomalies that may indicate financial crime.

Cluster analysis: Banks can use cluster analysis to group customers with similar behavioral patterns across multiple dimensions. This enables them to detect anomalies and deviations that indicate suspicious activity.

Entity resolution: Banks can use entity resolution to combine disparate data points across multiple accounts and transactions to create a unified view of entities. This empowers them to identify relationships, patterns, and anomalous behaviors that indicate suspicious activity.

Graph network analysis: Banks can use graph network analysis to map relationships between entities, transactions, and accounts. This helps them uncover hidden patterns, anomalies, and criminal networks.

Conclusion

Banks need effective technology to implement the Wolfsberg Group's guidance on monitoring for suspicious activity. An effective MSA platform features customer risk rating, entity risk detection, transaction monitoring, payment screening, customer screening, and transaction fraud prevention capabilities.

A holistic MSA platform empowers banks to detect and respond to crystalized risk in transaction and customer data. This technology complements banks' risk-based approach, helping them better comply with regulations and mitigate genuine financial crime risk.

HAWK

Hawk AI GmbH
Friedenstrasse 22B/i3
81671 Munich
Germany

Hawk AI USA Inc
230 Park Ave, Floors 3 & 4
New York, NY 10169
U.S.A.

Hawk AI APAC Pte Ltd
160 Robinson Road, #14-04
Singapore Business Federation Center
068914 Singapore

Follow us on LinkedIn >

info@hawk.ai >

www.hawk.ai >