The Future of Transaction Monitoring for AML

A series of trends is in motion that points to a different future for AML (anti-money-laundering) systems within banks.
Introduction

Current AML systems are no longer fit for purpose. This is a serious problem for banks, but just as importantly for their regulators, whose credibility is at stake.

Better transaction monitoring tools exist, the latest of which incorporate machine-learning algorithms. These perform far better than conventional, rules-based systems. But banks have been cautious about adopting them, largely due to concerns about the difficulty of explaining to financial regulators how they work.

There are signs that this situation is starting to change, thanks to growing pressure to consider machine-learning-based systems from forward-looking regulators in major jurisdictions.

This white paper explains why relying on rules-based AML detection systems is not sustainable and examines why banks are often reluctant to adopt solutions based on machine learning. It outlines how financial regulators around the world are beginning to recognize the potential of machine-learning models and introduces NetGuardians’ innovative AML solution.

This solution builds on NetGuardians’ success in applying statistical modeling and machine-learning techniques to transaction monitoring for fraud. It fully explains every AI-generated alert, allowing banks to make the transition to machine-learning-based systems confidently and at a pace of their choosing.
It is an open secret that money laundering is not being effectively addressed within banks and financial institutions. According to the United Nations, less than 1 percent of illicit funds in circulation (around $4 trillion) are being intercepted by law enforcement. The industry’s failure to address money laundering properly is a direct result of the ineffective and unsustainable detection methods the industry currently relies on.

Many suspected money laundering cases flagged to compliance officers by banks’ existing rules-based transaction-monitoring tools are likely to be false positives. These systems use static, predefined conditions to identify suspicious transactions, but achieve low accuracy because their frameworks of rules cannot be fine-tuned with sufficient flexibility to catch money laundering without incurring large numbers of false positives.

A review of one US universal bank’s risk rating model for retail customers, cited by McKinsey, found that of every 100 high-risk customers that the model identified, 72 were in fact medium or low-risk. Meanwhile 57 of every 100 customers classified by the model as medium or low-risk were actually high-risk. “To put this into perspective, a credit risk model with this kind of performance would never be allowed into production,” the consultancy commented.

Relying on these ineffective detection systems burdens banks with huge costs in staffing and wasted time. McKinsey reports that “as much as 85 percent of [banks’] financial crime compliance (FCC) and anti-money-laundering (AML) activities remain administrative or non-analytical in character [such as the manual collection of data from some systems to import into others].” Current systems are arguably not fit for purpose. They are ill-suited to an environment where budgets are getting tighter and digitalization means that client relationships have become more transactional, and banks know less about their clients.

Faced with such high volumes of false-positive alerts, compliance teams are overwhelmed. As a result, most AML alerts are never investigated. McKinsey reports: “For most banks, more than 90 percent of transaction-monitoring alerts turn out to be false positives. Of those alerts that do result in a suspicious activity report filing, 80 to 90 percent are not acted upon.”

But even if existing systems were effective, the spread of instant electronic payments means they would come under impossible strain. The historic approach of alerting potentially suspect transactions after they have been made no longer works in an era of instant payments – an essential feature of digital banking propositions. Without effective safeguards, instant payments can enable industrial-scale money laundering to take place without banks necessarily being aware, despite their legal obligations to prevent it. Banks know they must address this risk.

The status quo therefore poses a serious reputational risk to banks. But just as importantly, it is a serious headache for the regulators tasked with supervising them and ensuring they operate effective AML systems. NetGuardians believes it is this factor – the threat that ineffective AML systems pose to the credibility of financial regulators globally – that will ultimately drive uptake of new technologies that can improve oversight and increase detection and recovery rates. We see increasing signs that this is already happening.
Transaction monitoring systems based on machine learning have been successfully implemented and shown to offer compelling advantages over existing AML tools. They result in greater accuracy and fewer false positives, leading to more efficient use of compliance resources.

But for all their superiority, banks have historically been reluctant to adopt machine-learning-based systems. Marc Kilcher, Director in the Risk, Regulation and Compliance team at KPMG Geneva, believes this partly reflects a generational issue in banks’ compliance teams. “Now that compliance is everywhere, impacting all processes in this industry, banks need to move to more operational, efficient and ‘tech-enabled’ compliance. Not all decisionmakers in the compliance community are interested in tech topics, although given the volume of data they must deal with today, new systems would provide a very useful support for compliance activities,” he says.

Banks’ hesitancy in implementing machine learning also stems from concerns about the difficulty of explaining to financial regulators how these systems work. This “explainability problem” represents the most important practical challenge to the wider uptake of superior technologies such as machine-learning models in AML and transaction monitoring.

The Financial Action Task Force report, Opportunities and Challenges of New Technologies for AML/CFT, notes: “Difficulties with the explainability and interpretability of digital solutions are another key challenge for both industry and regulators that in part stems from the limited availability of relevant expertise and a lack of awareness of innovative technologies’ potential among AML/CFT professionals, both in industry and government.”
However, there are signs that change is starting to take hold. Some forward-looking financial regulators, including those in France, Germany, Singapore, the UK and US, are showing greater interest in new solutions to the problem of transaction monitoring, including machine-learning techniques.

For several years, the Monetary Authority of Singapore has been encouraging financial institutions to make use of advanced technology solutions to “enhance the effectiveness and efficiency of their AML/CFT controls,” says Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime), Monetary Authority of Singapore. “Harnessing new technologies can lead to a significant improvement in AML/CFT outcomes,” she says.

The US Financial Crimes Enforcement Network (FinCEN) has publicly recognized the potential of AI applications to “better manage money laundering and terrorist financing risks while reducing the cost of compliance.” Similarly, the Financial Action Task Force says: “The increased use of digital solutions for AML/CFT based on artificial intelligence (AI) and its different subsets (machine learning, natural language processing) can potentially help to better identify risks and respond to, communicate, and monitor suspicious activity. At public-sector level, improved live (real-time) monitoring and information exchange with counterparts enable more informed oversight of regulated entities, helping to improve supervision. At private-sector level, technology can improve risk assessments, onboarding practices, relationships with competent authorities, auditability, accountability and overall good governance while cost saving.”

It is clear that banking is in the early stages of a long-term transition from the current rules-based transaction monitoring systems to real-time monitoring using machine-learning models. Marc Kilcher of KPMG suggests this is in part due to the arrival of younger compliance staff at some banks and “the number, variety and complexity of regulatory requirements”. Even so, for this transition to progress, it is essential that AML systems that employ machine-learning algorithms are developed with explainability as a key priority from the outset.

NETGUARDIANS HAS DEVELOPED AN AML MONITORING SOLUTION BASED ON ITS SUCCESS IN APPLYING BEHAVIORAL MONITORING TECHNIQUES TO TRANSACTION MONITORING FOR FRAUD

NetGuardians developed its AML monitoring solution, based on its success over 10 years in applying behavioral monitoring techniques to transaction monitoring for fraud. The NetGuardians transaction monitoring system uses statistical models to achieve highly accurate identification of potentially suspicious behavior, reduce false positives by 85 percent compared with existing rules-based solutions, and cut operating costs by up to 75 percent.

To enhance the effectiveness of its statistical approach to transaction monitoring, NetGuardians has also developed machine-learning algorithms. But even without using machine learning, it has demonstrated that its statistical models are much more effective against fraud than rules-based systems. We believe the same advantages will apply to AML monitoring.

NetGuardians’ approach to AML is to build on the common characteristics of transaction monitoring for fraud prevention and AML by transferring expertise from the fraud domain across to AML. This reflects a trend we see among some banks for breaking down silos and enabling a degree of convergence between fraud prevention, which typically sits with the risk team, and AML, which is part of the legal and compliance function. These teams do not normally share information or systems and will usually have separate reporting lines. But there are signs that banks are recognizing the common characteristics of transaction monitoring for fraud and
AML and are looking at ways to create synergies between these siloed teams.

The behavioral models that NetGuardians uses can improve on current rules-based systems for AML and will make it easy to incorporate machine-learning models when banks are ready to go that far. Implementing NetGuardians’ solution will not force banks immediately to abandon the approach their current systems use. Instead, it will enable them to make the transition to new techniques for transaction monitoring at the pace they choose.

At the most basic level, NetGuardians’ rules and behavioral modeling can allow banks to adopt a more effective approach to transaction monitoring than they currently have, without having to move directly and immediately to wholesale use of machine learning. If they decide in future to adopt machine learning, the NetGuardians platform gives them the tools and pre-built models to do so, as and when they are ready. These models use machine learning as a first-line transaction-monitoring tool, not simply as an overlay applied to analyze the outputs from their existing monitoring systems. Banks are therefore able to evolve the techniques they use gradually, using new tools and techniques, to achieve much more effective transaction-monitoring outcomes.

NetGuardians solves the explainability problem that machine-learning algorithms bring by providing a comprehensive dashboard, including graphs, data visualization and evidence cards which explain how the models are triggered by particular customer behaviors and/or the attributes of their transactions.
NetGuardians’ AML Monitoring System

**Evidence Cards**
Evidence cards use clear, natural language to highlight areas for further investigation so the user can easily understand the context of each alert.

**Case Manager**
Graphic dashboards have been designed to be intuitive and interactive, putting all relevant data relating to each case in one place.

**Rule Editor**
Users can create, edit and manage detection scenarios within the modelling studio.
Community Scoring & Intelligence Service

In the future, we see a big opportunity to use our Community Scoring & Intelligence Service to improve banks’ defenses against money laundering. The service gathers a wider pool of anonymized external data from peers and third parties, increasing the scope and volume of data that can be applied. This can be used not only as training data to improve effectiveness of the machine-learning algorithms, but also to uncover wider mule networks and even protect against predicate fraud. This allows individual banks, which inevitably have a partial and limited view of the money-laundering problem, to benefit from the experience of their peers, leading to better outcomes for all.

CS&I collects, collates and categorizes validated data from peer institutions and third-party providers, transforming it into actionable intelligence for banks. This can be used to visualize the wider context via interactive dashboards. Investigations become more effective through this expansive external context, improving both understanding and the resulting decisions. Ultimately, this shared external intelligence may be directly deployed in detection models, driving improved effectiveness.

This innovation is in step with the COSMIC platform initiative, which the Monetary Authority of Singapore plans to launch in the first half of 2023. COSMIC will create a secure and fully regulated digital platform that will allow financial institutions to share information on customers and transactions to strengthen defenses against money laundering and terrorist financing activities.

"In the future, we see a big opportunity to use our Community Scoring & Intelligence Service to improve banks’ defenses against money laundering."
Conclusion

NetGuardians believes that we are in the early stages of a trend that will see banks ultimately converge on a better, more efficient, machine-learning-based solution for AML transaction monitoring some years from now. NetGuardians’ solution will provide a highly effective tool to counteract money laundering and enable banks to make the transition to machine-learning-based systems at a pace that suits them.

Marc Kilcher of KPMG concludes: “Nowadays clients understand that AML is part of their bank’s onboarding and monitoring processes. What they do not understand is the delay they experience when opening a new account or the repeated questions about the same types of transactions. Efficiency and effectiveness in compliance is now part of customer service. I believe banks that continue to struggle with their processes to mitigate potential AML risks will lose more and more customers. And if you add to that the fact that regulatory penalties will also increase, attracting negative media coverage, the costs of delaying the tech transformation of compliance are becoming a real strategic issue.

“Moving to more modern systems can provide a huge gain in detection rates and operational efficiency, and so enhance overall customer service. But it cannot remove all AML risks. False positives will always occur – they are part of the compliance team’s job – but the ratio of false vs true needs to be much lower.”
About NetGuardians

NetGuardians is an award-winning Swiss FinTech helping financial institutions in over 30 countries to fight fraud. More than 80 banks and wealth managers, including 40 percent of all Swiss cantonal banks and three of the top 10 private banks as ranked by Euromoney, rely on NetGuardians’ 3D artificial intelligence (3D AI) solution to prevent fraudulent payments in real time. Banks using NetGuardians’ software have achieved an 85 percent reduction in customer friction, enjoy more than 75 percent lower operating costs and have detected new fraud cases.

NetGuardians is the fraud-prevention partner of major banking software companies including Finastra, Avaloq, Mambu and Finacle. NetGuardians was listed as a representative vendor in Gartner’s 2020 Market Guide for Online Fraud Detection and as a Global Leader in the 2021 Aite report on Fraud and AML Machine Learning Platforms. Headquartered in Switzerland, NetGuardians has offices in Singapore, Kenya, and Poland.