QuantaVerse

APPLYING ARTIFICIAL INTELLIGENCE TECHNOLOGY TO REDUCE AML RISK FOR GLOBAL FINANCIAL INSTITUTIONS

ENHANCING TRANSACTION MONITORING SYSTEMS WITH AI AND MACHINE LEARNING TO IMPROVE AML OUTCOMES

In recent years, financial institutions have navigated through a rising tide of regulatory obligations and compliance requirements related to anti-money laundering (AML), counter-terrorist financing (CTF), Bank Secrecy Act (BSA) and Know Your Customer (KYC). In response to increased scrutiny, and the risk of significant fines and enforcement actions, these covered institutions have spent billions of dollars in an effort to be compliant and thwart criminals from laundering their illicit proceeds through the global banking industry.

Maintaining both effective and efficient AML programs has proven elusive for financial institutions due to a reliance on legacy technology solutions and a seemingly ever-increasing investigator case workload. The new technologies of data science, including artificial intelligence (AI) and machine learning, however, hold the key to helping institutions reduce regulatory risk, and improve the AML investigation process.

An effective AI-based AML solution, designed to enhance financial institutions' existing compliance systems, can catch the false negatives that embody financial and reputational risk and increase investigative efficiency, driving out false positives. With trillions of dollars in laundered money still channeling through the global banking system, AI and machine learning offer the opportunity to move toward a new standard of AML.

The application of AI technology is a logical solution in solving the problem of AML risk for financial institutions. Modern AI systems have progressed to the point where large volumes of transactional and other sources of data can be culled, consolidated, analyzed and scored for risk so that investigators can make more accurate SAR-filing determinations. The time is now for financial institutions to confidently leverage the proven technology of AI in their AML ecosystems.

CURRENT APPROACH TO ANTI-MONEY LAUNDERING IS DUE FOR IMPROVEMENT

Today's financial institutions face an unprecedented array of technical challenges including cyber security defenses, customer service innovation, an explosion of data management challenges, and regulatory requirements and regulations related to financial crimes, including money laundering, terrorist financing, fraud, and corrupt practices. Under constant scrutiny from both federal and state regulators, financial institutions invest billions each year on technology and investigative personnel. Despite increases in compliance spending, the money laundering problem faced by financial institutions is not abating and the risk of penalties remains high. According to a WealthInsight report, global AML spending will exceed $8 billion in 2017. Additionally, banks around the globe have paid approximately $321 billion in fines since the 2007-2008 financial crisis as regulators stepped up enforcement, according to a report by the Boston Consulting Group.

The financial services industry relies heavily on legacy rules-based transaction monitoring systems (TMS) to detect and report on transaction detail that indicate suspicious activity. High-risk AML typologies targeted by TMS include:

- **Funnel account activity:** when an account receives a high volume of deposits or transfer activity and then rapidly transfers the funds to another account, often in another geographic area. These accounts are common with human trafficking organizations.

- **High velocity activity:** when an account exhibits an abnormal amount of activity over a short timeframe that is not consistent with similar customers or accounts. These accounts are common with various money laundering schemes for all types of criminal organizations.

- **Routing of transfers through multiple jurisdictions:** entities create business relationships or subsidiary companies in many countries allowing them to route money through multiple jurisdictions.

- Other money laundering indicators that TMS regularly monitor include activity outside of the customer's expected account profile; structured transactions; round-dollar transactions; pass through accounts; many to one transaction flows; one to many transaction flows; foreign fighter typology red flags; and tax amnesty and tax avoidance cues.

Transaction monitoring technology is essential for the maintenance of an effective AML program. However, transaction monitoring systems need assistance on two fronts:

1. *Catching transactions that represent serious risks for financial institutions.* If a financial crime does not violate a stated rule, the TMS will not flag it and a high volume of dirty transactions continue to go undiscovered. The United Nations Office on Drugs and Crime (UNODC) estimates that the amount of money laundered globally in one year is two to five percent of global GDP, or $800 billion to $2 trillion in U.S. dollars.

2. *Reducing the high rate of false positive alerts that TMS create.* With a rules-based TMS, the search for criminality will frequently catch the normal, licit transactions of legitimate clients. These "false positive" alerts trigger time-consuming and expensive human investigations. The industry estimates that approximately 95 percent of the alerts generated by TMS are false positives.

THE ALL TOO HUMAN ANTI MONEY LAUNDERING (AML) PROCESSES

On the front line in the fight against money laundering are human AML investigators. These men and women are tasked with identifying and stopping criminal and terrorist financing. They have the responsibility to review thousands of transactions flagged daily by TMS and determine if they are, indeed, suspicious.

A typical investigator at a financial institution works eight to 10 alert cases per day allocating, on average, 45 minutes to each. The work is complicated by having to check multiple, disparate bank systems such as customer information program (CIP) databases, KYC databases, cross-referencing the TMS for related flags and checking historical SAR databases as well as turning to external information sources such as online investigative services, government databases and Internet research sites. Complicating things further, when dealing with intermediaries and correspondent banks, customer information is often altogether unavailable.

Over time, it has become even harder to keep up. A 2013 report from Aite Group estimated that the number of AML alerts worked by financial institutions went from about 5.76 million in 2009 to an estimated 6.89 million in 2012. By 2016, the analyst firm estimated the number of investigations would have risen to about 10.36 million. And falling behind is not an option. The Financial Crimes Enforcement Network, or FinCEN, mandates that all U.S. financial institutions file a suspicious activity report (SAR) no later than 30 calendar days after the date of the initial detection of suspicious activity and no later than 120 days for continuing activity.

If being poorly equipped and pressured to work faster isn't enough to increase the likelihood of dangerous errors, investigators bring different levels of skill, training and biases to the job. Confirmation bias, for example, has been identified as point of failure occurring when an investigator inadvertently interprets data in a way that confirms his or her own pre-existing beliefs. Others include social bias, and pre- and post-decision biases that can impact the all too subjective nature of the investigative process.

ARTIFICIAL INTELLIGENCE: JUST LIKE HUMANS, BUT BETTER

Breakthroughs in the areas of data science, computational advancements and big data practices have accelerated the pace of technological innovation. This is particularly true of advancements in modern artificial intelligence. Possibly due to this rapid advancement, there is great variance in how the industry categorizes the continuously evolving AI category. For the purposes of this discussion, we offer the following definitions:

Artificial Intelligence

AI applications are developed to enhance human cognitive performance or completely replace people in the execution of non-routine tasks by enabling machines to emulate human intelligence processes including:

- Learning: acquiring information and the rules needed to use that information
- Reasoning: the ability to draw conclusions; and
- Self-correction: improving future outcomes based on feedback to past reasoning.

Essentially, instead of writing rules that require vast amounts of lines of codes to cover every potential criminal behavior, data science experts can develop an analytics engine by coding the ability for the machine to apply logic, and to learn from previous decisions.

Machine Learning

In this application of artificial intelligence, a model is established and the computer is empowered to adjust the model based on the data it encounters. Machine learning provides computers the ability to learn and change without being explicitly programmed.
For example, machine learning algorithms are used to distinguish objects in autonomous driving applications. In this instance, a machine learning algorithm is provided sample images of objects such as vehicles, pedestrians, or

animals. When the system is tested, incorrect guesses are removed from the algorithm and new images are added to improve the accuracy and to help the algorithm "learn."

On the AML front, the pattern detection capabilities of machine learning are well-suited to differentiate between legitimate and illicit transactions through a training set of data fed to the algorithm. For example, a scoring model can be established based on high-risk customers, entities and geographies. Important for the highly regulated financial services industry, machine learning can also report the logic it used to reach conclusions and document new learnings it adds to the consideration of cases in the future.

There are three ways that machine learning is classified:

1. Supervised learning: where the model is fed "labeled" data paired with a definition of that data. In the autonomous vehicle example, an image of a cat is provided with a specific "cat" tag attached. Equate this to showing a child an image on a flashcard while saying aloud what the image is called.
2. Unsupervised learning: where the model is provided "unlabeled" data and it is left to recognize patterns on its own.
3. Reinforcement learning: where the model is simply graded based on the outcomes it produces. This is the bleeding edge of machine learning that encompasses neural networks that emulate the way brain neurons are trained and deep learning which one InfoWorld post succinctly described as "many neural networks working together."

SHOWING YOUR WORK: THE DOCUMENTATION IMPERATIVE

The decision-related documentation and reporting that is required by AML investigators and regulators raises important considerations when AI strategies are considered. Machine learning can replicate the same level of abstraction when explaining and documenting a suspicious case as a human investigator might. Each AI decision is accompanied by a confidence level, evidence, rationale for a regulatory violation, anomalies discovered, and, if required, the system can cite cases from which it learned and based its conclusions.

Financial institutions have increasingly begun to incorporate these AI approaches into their regulatory and compliance frameworks. AI and machine learning have significant application in the identification and prevention of financial crimes such as money laundering and terrorist financing.

HOW AI TECHNOLOGY INTEGRATES INTO THE AML PROCESS

The application of AI for AML is a logical one. With an AI system, AML data points can be pulled and consolidated automatically, the transactions scored for risk and the anomalies documented for AML investigators that can now evolve from researchers desperately fighting against the clock to unearth relevant data into analysts presented with automated financial crime reports that allow them to be better informed and more accurate with their determinations.

An AI-based AML solution can analyze massive amounts of transactional and client information from a variety of sources such as TMS, KYC databases, Lines of Business (LOB) customer information, as well as investigative databases, public Internet sources and the deep web where criminals often interact and transact business. To conduct such an analysis, AI solutions utilize agents which are highly specialized algorithms responsible for collecting and interpreting data, modeling behaviors, detecting anomalies, inferring relationships, and identifying issues. These agents report issues to a machine learning engine by delivering both the alerts and all necessary supporting evidence.

The machine learning engine accepts all of the collected artifacts and develops an overall risk score. This score embodies the level of suspicion around transactions, transacting entities, and entity networks. These three areas represent the what, who, and why of financial activities, and provide a holistic view of transacting entities and their motives. The score also includes a measure of confidence about the decision. Confidence is calculated based on the number of alerts and anomalies detected, as well as similarity to past cases. This also allows the AI system to constantly evolve, learning from past decisions.

Specific AI and machine learning techniques that are employed to identify transactional anomalies worthy of further investigation include:

- Collaborative filtering: capable of finding transactions with missing, matching and/or odd information
- Feature matching: utilized to identify transactions below a specific monetary threshold
- Fuzzy logic: used to find data matches with slight changes to names or addresses
- Cluster analysis: can detect abnormalities in transactions benefiting a single person or entity
- Time series analysis: detects transactions benefiting a person or entity over an extended period
- Focused keyword searches: ability to dynamically monitor, screen and filter transactions based on keywords from high-risk AML, CTF and financial crimes typologies
- Ability to learn from an AI-identified suspicious activity to enhance transaction monitoring and KYC platforms

Let's consider how round-dollar transactions would be handled in an AI-enabled environment. Financial institutions are warned that these types of transactions are telltales of illicit drug payments, however, legitimate round-dollar transactions are also very common. An AI-enhanced system can instantaneously check the round-dollar transaction flags from the TMS against other indicators such as non-complementary lines of business, KYC data, history of transactions between entities and structuring behaviors to accurately eliminate round-dollar false positives.

COMPARING RULES-BASED TMS TO AI

While transaction monitoring technology continues to be the tool of choice for financial institutions, there are many inherent limitations. In a rules-based TMS environment, it is impractical for financial institutions to create all the rules required to effectively identify every suspicious activity. It would be an arduous and costly process to manually address the multitude of slight deviations in transaction behaviors with new lines of code on a continuous basis. Even if, somehow, all suspicious behaviors could be identified and TMS rules were updated, such a delay would allow bad actors execute money laundering schemes for months or even years before the system can be tuned to successfully flag the new criminal activity.

Additionally, rules-based solutions cannot distinguish between normal and illicit transactions that break the same rule. For example, although transaction monitoring systems are commonly programmed to flag all round dollar transactions, the majority of these types of transactions are not criminal in nature. What's more, criminals have evolved to mimic normal transactional behavior to prevent their illicit activities from being flagged by TMS. Smart money launderers know the rules commonly programmed into transaction monitoring systems and avoid them.

Rather than writing code to identify every potential financial crime, AI-based engines identify the patterns in transaction data and use that to identify when a transaction is behaving differently from the others it has encountered.

For example, North American Industry Classification System (NAICS) codes can help banks identify the type of business that they or their intermediaries are servicing and ensure that transactions from those businesses have valid economic perspective. It would be impossible to write TMS rules that make use of NAICS codes to account for every possible relationship between all businesses. However, when NAICS are provided to the system, an AI system learns common relationships, as well as transactional direction, frequency and amounts and based on that can identify anomalies.

AI IN ACTION FOR AML: PROTECTING AGAINST FALSE NEGATIVES

False negatives, which are instances of illicit transactions not flagged by the TMS, represent significant risk to financial organizations. It is estimated that 50 percent of financial crimes trafficked through the banking system pass through transaction monitoring systems unnoticed.

Unlike static rules-based TM engines, AI systems can detect patterns of behavior, analyze the intent of those patterns and expose anomalous activities.

For example, transactions that do not follow the usual frequency and directional patterns expected for a given type of account may not be flagged by a TMS, but would be identified with an effective AI solution. An AI solution can learn the baseline of normal reported payroll account activity and thus identify any irregularities in payroll transactions as potentially fictitious and worthy of further investigation.

While there is no economic purpose for a Yemen-based government fire protection agency to purchase fertilizer from a farm in the UK, that business relationship would not be flagged by a TMS. However, by comparing entities' NAICS codes, an AI solution could quickly determine that the two entities were not engaged in complementary lines of business triggering the system to further investigate those entities and their business transactions.

Its ability to efficiently evaluate large numbers of transactions means that an AI system can also be used to examine transactions that currently go unexamined as part of Above-the-Line/Below-the-Line practices.

AI IN ACTION FOR AML: IDENTIFYING AND REDUCING INTERMEDIARY RISK

The ability to send and receive payments internationally via correspondent banking is vital to the global economy. The World Bank estimates that global remittances will increase to more than $636 billion in 2017. However, high remittance volume can bring increased regulatory scrutiny, risk, and compliance costs that bite at the heels of financial institutions.

The result, unfortunately, is that institutions often abandon revenue sources by de-risking foreign correspondent relationships rather than deal with the inherent risk and problems of maintaining correspondent banking accounts. The financial institutions that choose not to de-risk will often file defensive SARs because the data is not available for them to establish the economic purpose and verify complementary lines of business for their correspondent banking customers. Effective entity resolution and entity relationship investigation are integral to curbing the de-risking cycle.

An important function of an AI solution is its ability to monitor customers' relationships to other customers and entities and learn from their associated behavior. An AI-based AML solution can automate the transactional analysis of these intermediary relationships to find anomalous behaviors and identify the end clients causing those anomalies. An AI-enhanced solution can account for seasonality, mergers and acquisitions, randomness and other legitimate variances to find the illegitimate anomalies that are presenting significant risks to financial institutions. An AI solution can also provide predictive insights into transactional behaviors, and automate the required regulatory analysis and reporting.

Correspondent banking relationships continue to grow so the AML risk to banks will remain. Deployment of AI-enhanced solutions can assist banks in better SAR reporting and ultimately prevent unnecessary de-risking of correspondent banking customers.

CONCLUSION

The proven field of AI and machine learning for AML is the only technology that can effectively improve financial crime investigations, scale to the volume and velocity of the modern financial system, and counter criminals' evolving approaches to money laundering.

For financial institutions, the time is now to deploy AI into their AML ecosystems. AI and machine learning hold the key to reducing risk related to financial crimes, addressing regulation, driving out operational cost through improved efficiency and, most importantly, effectively preventing criminals and terrorists from using the banking industry for their evil agendas.

ABOUT QUANTAVERSE, LLC.

QuantaVerse is the emerging leader in data science-powered risk reduction solutions, purpose-built for identifying financial crimes. Utilizing proprietary data science algorithms including artificial intelligence (AI), machine learning and big data technologies, QuantaVerse integrates and filters institutional data and related external data – including public Internet data, unstructured deep web data, as well as government and commercial datasets – to significantly improve AML, KYC and BSA compliance and prevent money laundering and the crimes it supports. For more information, contact QuantaVerse at (610) 465-7320 or visit www.QuantaVerse.net.

To learn how QuantaVerse data science powered solutions can benefit your financial institution, contact QuantaVerse at (610) 465-7320 or visit http://www.QuantaVerse.net for more information.

QuantaVerse