Algorithmic AML:

Making Visible What is Frequently Invisible. Tackling the 1% Problem.

A CLEARPRISM WHITE PAPER

CLEARPRISM

Powered by: CapImpact

Focused on execution, powered by analytics.

Proven algorithmic methods, experience and tools that eliminate guesswork and risk.

877-717-7476 | clearprism.com

Ouch

3-5% of global GDP is laundered through the global financial system. That's a range of $800 billion to more than $2 trillion a year. According to the United Nations Office on Drugs and Crime, despite the nearly $2.4 trillion in illicit funds laundered each year, less than 1% of that money is detected.

Financial institutions are required by regulators to combat money laundering. They have invested billions of dollars to do so. Despite this, these institutions still face significant penalties for non-compliance. Penalties over the past five years have totaled more than $300 billion dollars and is expected to increase to well over $400 billion over the next few years.

In September 2020, the International Consortium of Investigative Journalists (ICIJ) released more than 2,100 suspicious activity reports – known as SARS reports – filed by banks and other financial firms with the U.S. Department of Treasury's Financial Crimes Enforcement Network, or FinCEN. SARs reflect specific concerns of regulatory agencies delivered to banks and other financial institutions based on fraud patterns identified or they intend to monitor. They are not necessarily evidence of criminal conduct or other wrongdoing. They are, however, triggers or "Flags" of concern. And consequently, serve as an "early warning signal" of what banks and others should pay attention, but these are the "leading indicators" of what regulators are and will be paying attention to.

Less than 1% of the $2.4 trillion dollars in laundered money per year is detected.

Banks have spent billions on transaction monitoring systems that scrub their accounts for possible money laundering schemes. Detection rules are action-based and target suspicious transaction behaviors, such as excessive cash deposits, structured transactions intended to avoid government record-keeping thresholds, and rapid money movement through one bank to another.

Customers who violate the detection rules trigger a system-generated alert, which is reviewed by an internal investigator. Despite decades and billions of dollars in industry investment, over 95 percent of system-generated alerts are closed as "false positives" in the first phase of review, with approximately 98 percent of alerts never culminating in a suspicious activity report (SAR).

80% of SARS are false positives. And every SAR reported requires investigations. No matter an imperative is to reduce false positives.

False positives cost the financial industry billions of dollars in wasted investigation time each year but more importantly, expose banks to steep fines and reputational damage for failing to identify bad actors involved in organized crime, sanctions evasion, or terrorism. Banks can reduce risk by reassessing their detection strategies, which presently lack the focus or sophistication to identify illicit source behavior.

Whether or not banks are motivated to actually counter illicit funds flowing through their accounts is a topic for others to wrestle through. The recently released FinCEN files suggest perhaps not. It suggests that there is lots of "box-checking but little practical progress" with many focused on "technical compliance" rather than whether systems "are really making a difference." (source: https://www.icij.org/investigations/fincen-files/global-banks-defy-u-s-crackdowns-by-serving-oligarchs-criminals-and-terrorists/)

People will dispute on whether or not banks should be more aggressive to counter money laundering and/or whether or not they will be. What is not in dispute, however, is that significant monies are spent by banks as a result of anti-money laundering (AML) activities and requirements. And where monies are spent, new capabilities will be developed. More than 335 start-ups globally have entered the AML space within the past 3 years. The draw? The growth of spend anticipated to counter illicit fund movement and fraud.

And here it gets interesting. Because, as the old saying goes, the more things change, the more things stay the same. Unless it doesn't. And of all the energies and monies, start-ups and SARS being created, the domain of AML reflects both sides of this saying: there is much staying the same, yet some incredibly interesting new capabilities being developed that could (finally) start to tip how AML is conducted, fraud patterns identified and both penalties and investigatory costs reduced.

Let's explore how.

Making it Pragmatic

There are two fundamental problems to overcome to strengthen one's AML / Fraud process.

1. The False Negative Problem – which focuses on the financial exposure of fraud. Penalties imposed on a bank reflects this exposure rate. This problem is also known as the "upstream" – or initial part – of the "Know your Customer" (KYC) process. New customers need to be vetted, scored according to risk profiles aligned with the institutional criteria of who makes up an "acceptable" customer.

2. The False Positives Problem – which requires being current with regulators and the notices or "flags" they provide based on insights they've seen and concerns they have. Alignment with such SARS reports involves significant monies spent by banks as they investigate potential discrepancies. Due to the sophistication of contra-partiers, 95% of system generated alerts are false positives. False positives cost billions of dollars in wasted investigation time each year and expose banks to steep fines and reputational damage for failing to identify bad actors.

Both the False Negative and False Positive problems are costly. In the former case, it stems from penalties, in the latter case, from the costs of both investigations and reputational damage.

Bad guys are clever guys. They adapt to new capabilities and respond to SARS reports. The former stems from the never-ending introduction of new technical capabilities (e.g., witness the hundreds of new startups alone in the space). The latter indicate where they should focus since such reports are how the regulators tell the banks what is important to them and consequently where banks should allocate their resources to align with regulatory focus.

The implication of both? An ongoing game of cat-and-mouse juggling new capabilities to use and the "white space" of regulatory focus leaving plenty of "dark space" to continue to commit fraud.

Making Visible what is far too often invisible: From Rules-Based Methods to Algorithmic Insight

There are two different approaches to tackle fraud; one has been the mainstay of the industry to date, the second reflects new capabilities based on pragmatic lessons from machine learning, algorithms and math.

The Mainstay: Rules-based approach

A rules-based approach – whereby the system flags cash transactions over a certain currency amount, blocks transactions to certain countries, uses customer data to select accounts for additional monitoring, and categorizes merchant accounts based on prior transactions.

It is the foundation of many (the majority?) of current products and approaches used. As new flags are identified, rules are constructed to monitor similar transactions. Rules get updated into an ever-increasing set of rules to monitor.

Rules-based approaches have an inherent limitation. Bad guys change behaviors frequently requiring catch-up and the addition of new rules. The volume, velocity and variety of new bad behaviors overwhelms rule-based approaches. Either there is a constant "you can't see what you don't catch" problem and so only create rules of bad behaviors that are found or the rule set becomes brittle because each one needs to be coordinated with other rules creating a "log jam" of code which makes fraud monitoring heavy (e.g., expensive) and hard to maintain. Combine with this the comment earlier that only 1% of bad behaviors tends to be found, and you get a quick sense of the imperative of new capabilities.

Algorithmic approaches.

Algorithms with machine-learning capabilities have three characteristics which significantly helps to reduce both false positives and false negatives. (Note: a recent engagement completed with PwC on one of their banking clients attested that our Minerva-AML approach was 3x more effective in finding fraud patterns than rules-based approaches. We'll further explain how later.). Rather than mapping transactional data to known flags (e.g., bad behaviors), algorithmic approaches seek to "stitch together" patterns of behaviors, some seen before and some inferred from anomalous behaviors.

Our algorithmic approach differs from rules-based approaches in three ways.

First, it is based on rich fraud taxonomies. This solves the "10,000 acre forest problem." Here's the problem. Finding a needle in a large forest (e.g., fraud in a set of millions of financial transactions) is difficult. You need to cover lots to ground to do so. Common sense tells you that there is no need to walk every inch of the forest. The needle, and fraud, isn't everywhere, but in particular parts of the forest, or in a subset of the tens of millions of transactions. Narrowing the ground to cover, from 10,000 to, say, 1,000 or fewer acres will a) increase the odds of finding what you want and b) accelerating doing so.

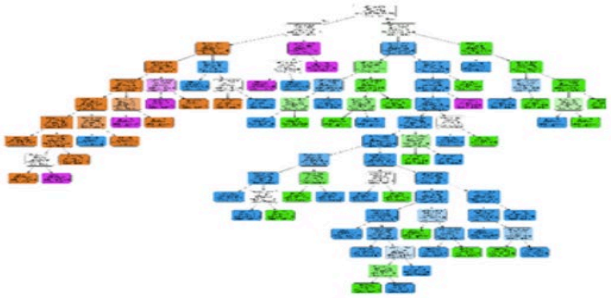
AML involves an ongoing game of cat-and-mouse juggling new capabilities to use and the "white space" of regulatory focus leaving plenty of "dark space" to continue to commit fraud... Requiring algorithmic rather than rule-based approaches to "make visible" what often remains invisible.

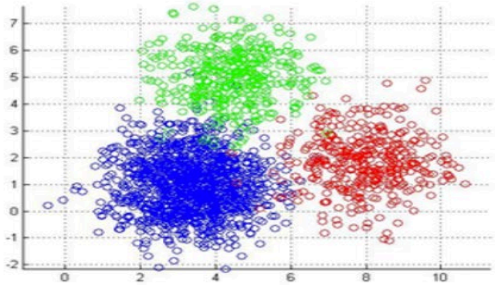
Rules-based approaches cover all 10,000 acres, the more the rules, the more the ground they cover. Algorithmic approaches do it differently. Narrowing this search space rests on the taxonomies and learning modules run across them. This involves two steps:

Step 1, prepare the data to be explored – the 1,000 acre search space. Often, significant data is missing from transactional records such as beneficiary flags, country office, region, perhaps the instrument name, and so on. The taxonomy helps to fill in blanks, inferentially again based on the underlying patterns that make up the taxonomies.

Step 2, and again based on the taxonomy, it's important to "force a segmentation" of the data. This segmentation becomes the "common sense" search space – the 1,000 rather than the 10,000 acre forest to explore.

The following depicts the nature of transactional data often received that needs to be prepared, powered by the fraud taxonomies.



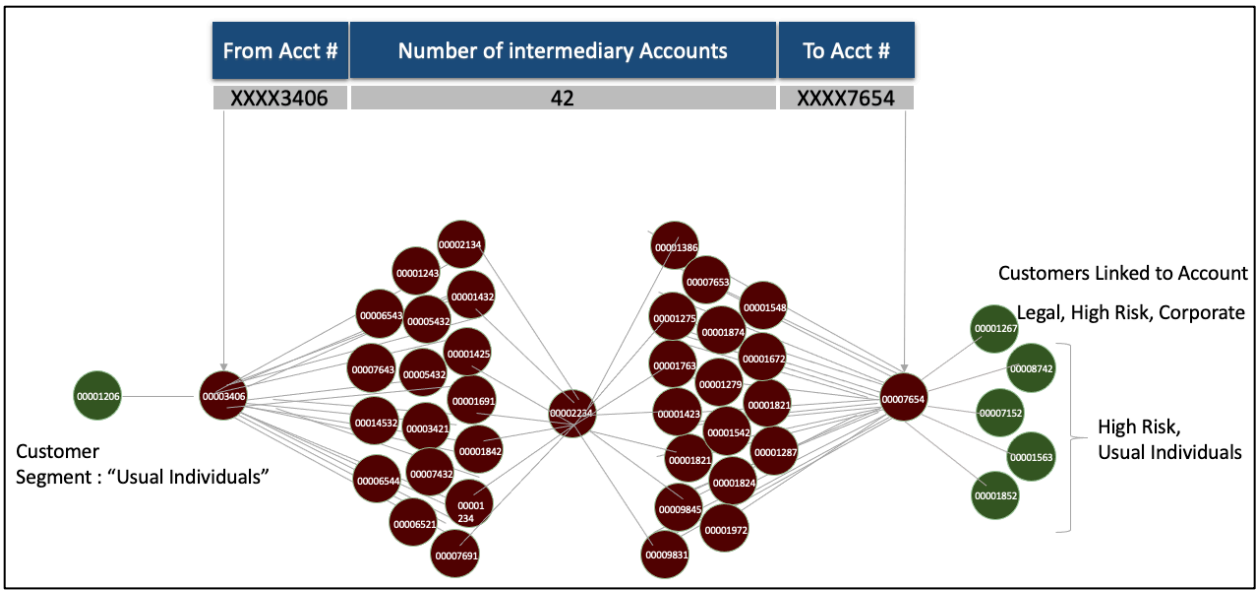


Second, the learning engine is strengthened through insight into the current set of SARs flags, their stability over time and over efficacy at targeting known frauds. This step involves building classification models identifying combinations of alerts which translate into "true," known or knowable SARs. It is insight into the combination of, and the sensitivity of relevance among them, rather than a listing of them that matters. How? By isolating "faint signals" of which types of SARs influence others and thereby serve as "pointers" to derivative / new fraud patterns.

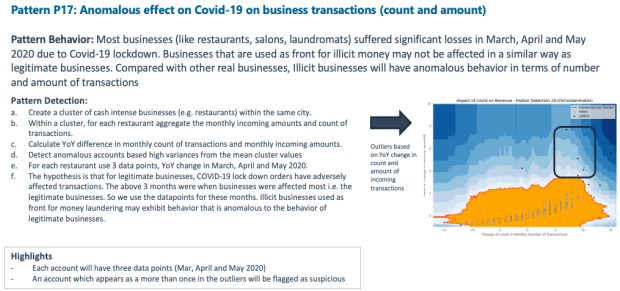
Third, network insights. One reason identifying fraud is that no single financial transaction may be problematic and hence not identified. It is the combination of many of them over periods of them that gets interesting. There are two blunt implications of this clever way to "remain under the radar." One, statistical analysis across transactions are limited – since, again, any particular transaction may be legal. Two, relationship analysis needs to be performed to understand a) if and how any particular transactions may be connected with each other and b) the number of hops between two accounts (the origin and disbursement accounts) and (here it gets particularly interesting) the number of intermediaries between the accounts.

The only way "into" this problem is to use link, or network, analysis, transposing the data into a graph database to derive such insights.

The figures below visually depict how intermediaries can be linked together resulting in patterns previously invisible to become visible.



Non-Linear pattern based on number of intermediaries – tracing a transaction (Graph edge) through number of accounts (nodes)



Pattern P17: Anomalous effect on Covid-19 on business transactions (count and amount)

Pattern Behavior: Most businesses (like restaurants, salons, laundromats) suffered significant losses in March, April and May 2020 due to Covid-19 lockdown. Businesses that are used as front for illicit money may not be affected in a similar way as legitimate businesses. Compared with other real businesses, Illicit businesses will have anomalous behavior in terms of number and amount of transactions

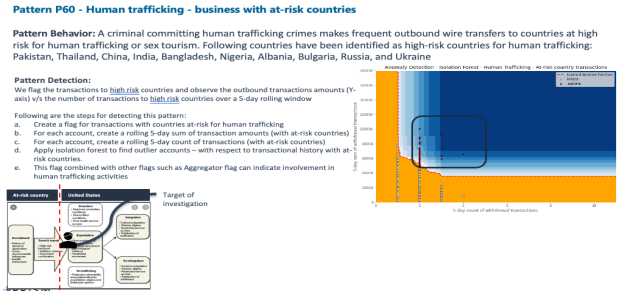
Pattern Detection:

a. Create a cluster of cash intense businesses (e.g. restaurants) within the same city.
b. Within a cluster, for each restaurant aggregate the monthly incoming amounts and count of transactions.
c. Calculate YoY difference in monthly count of transactions and monthly incoming amounts.
d. Detect anomalous accounts based high variances from the mean cluster values
e. For each restaurant use 3 data points, YoY change in March, April and May 2020.
f. The hypothesis is that for legitimate businesses, COVID-19 lock down orders have adversely affected transactions. The above 3 months were when businesses were affected most i.e. the legitimate businesses. So we use the datapoints for these months. Illicit businesses used as front for money laundering may exhibit behavior that is anomalous to the behavior of legitimate businesses.

Outliers based on YoY change in count and amount of incoming transactions

Highlights

- Each account will have three data points (Mar, April and May 2020)
- An account which appears as a more than once in the outliers will be flagged as suspicious



Pattern P60 - Human trafficking - business with at-risk countries

Pattern Behavior: A criminal committing human trafficking crimes makes frequent outbound wire transfers to countries at high risk for human trafficking or sex tourism. Following countries have been identified as high-risk countries for human trafficking: Pakistan, Thailand, China, India, Bangladesh, Nigeria, Albania, Bulgaria, Russia, and Ukraine

Pattern Detection:

We flag the transactions to high risk countries and observe the outbound transactions amounts (Y-axis) v/s the number of transactions to high risk countries over a 5-day rolling window

Following are the steps for detecting this pattern:

a. Create a flag for transactions with countries at-risk for human trafficking
b. For each account, create a rolling 5-day sum of transaction amounts (with at-risk countries)
c. For each account, create a rolling 5-day count of transactions (with at-risk countries)
d. Apply Isolation forest to find outlier accounts – with respect to transactional history with at-risk countries.
e. This flag combined with other flags such as Aggregator flag can indicate involvement in human trafficking activities

Target of investigation

A Call to Action: moving fast with complementary approaches

It's important to note that the rules-based and algorithmic-approaches complement each other. Rules-based systems generate a set of flags to monitor. These become inputs into the learning modules for algorithmic insights. And the new fraud patterns identified by the algorithmic approach can be fed into the rules-engines to monitor fast-moving fraud patterns.

For the organization, this is key. How so? Because it means that the sunk costs of existing rules-based systems remain relevant. Algorithmic approaches to be "light-weight" in terms of investment; they can be thought of as "services on top of" or complementary to existing solutions. The second advantage of this is speed. As services, they can be deployed quickly – in days rather than weeks, thereby strengthening one's insights while reducing both false positives and false negatives and the penalties and investigation costs associated with them.

What's not to love?

About the Authors:

Prabhakar Jayade – Partner and Head of Risk & Regulatory Solutions, ClearPrism

Prabhakar has 30 years technology development experience, including senior partner roles at KPMG and Capgemini. For the past 10 years, his primary focus has been on AI, from which four patents applications were submitted in the areas of risk and predictive modeling. Prabhakar has a very granular and quantitative understanding of the variables (product x capabilities x processes) that make up key interdependencies for diverse industries. He also brings a strong technology and data science background with hands-on experience with latest techniques in AI/ML and use of natural language processing, big data and integration of unstructured data into mainstream computing. His current work is in the area of quantifying exposures across a wide range of risk-taxonomies including reputation, compliance, and operational exposure, as well as algorithmic fraud detection techniques.

Prabhakar can be reached at prabhakar.jayade@clearprism.com

Samir Kamat, Ph.D. – Partner and Head of Data Science, ClearPrism

With a focus on designing ML/AI/NLP algorithms and using data engineering to solve client problems and identify new investment opportunities, Samir joined the firm from KPMG, where he previously served as a an advisory practice partner managing the innovation portfolio and developing models and solutions for clients. Prior to that assignment, Samir was a vice president with Capgemini Financial Services, where he oversaw the company's business information management practice for the banking industry. His focus included advanced analytics, data wrangling and data visualization. Samir also served as vice president and head of the credit risk modeling for Wells Fargo Bank.

Samir can be reached at Samir.kamat@clearprism.com

Ralph Welborn, Ph.D. – Managing Partner and Co-Founder, ClearPrism

Previous roles included Head of Strategy & Transformation (IBM – Middle East / Africa), Senior Vice President Global Strategy, KPMG Consulting, CEO of Advanced Analytics Company. Author of three books on Business & Technology Transformation.

Ralph can be reached at ralph.welborn@clearprism.com