NICE
ACTIMIZE

Insights Article

Graph Analytics for AML

Author: Danny Butvinik

Graphs Analytics for AML

Nefarious industries rely on sophisticated money laundering schemes to operate. Money laundering, known as the process that transforms the proceeds of crime into clean legitimate assets, is a common phenomenon occurring all over the world. Illegally obtained money is typically 'cleaned' thanks to transfers that involve banks or legitimate businesses. It is among the hardest activities to detect in the world of financial crime. This is often linked to terrorism, drugs and arms trafficking, and exploitation of human beings. Funds move in plain sight through standard financial instruments, transactions, intermediaries, legal entities and institutions – avoiding detection by banks and law enforcement.

AML is generally viewed through the lens of regulatory compliance because the burden of forensic analysis falls primarily on financial institutions (FIs), which are responsible for meeting Know Your Customer (KYC) standards, monitoring transactions, shutting down or restricting accounts deemed suspect, and submitting timely Suspicious Activities Reports (SARs) to law enforcement agencies. The costs in regulatory fines and damaged reputation for FIs are all too real.

In the past decades, most of the suspicious activities were identified by considering anomalies in the regular transactions flows of a client: behavior patterns and trends were compared over time to spot unexpected turns.

Rule-based classification approaches are frequent. Other studies used Bayesian approaches either to assign a risk score to customer behavior, also taking into account the evolution of such behavior, or, more generally, to combine Bayesian rules with database information about past operation history outperforming other fuzzy techniques.

Machine learning algorithms were also applied with the same general purpose: ensemble classifiers, decision trees, neural networks, Bayesian networks and clustering algorithms to detect false invoicing of taxpayers. It was conceived by that time that clustering techniques are the best solution. By contrast, limitations of the machine learning approaches were heavily discussed – such as the problem of the identification of parameters that are data dependent, with sometimes limited adaptability and scalability, the risk of misclassification, the class unbalance problem, or the difficulties in the interpretation of the underlying behavioral patterns.

Recent studies have focused attention on relational data, in order to reveal new patterns and surpass some of the limits of the traditional approaches. There is a tradeoff between the need for financial institutions to rely on rules that can be easily applied and understood and the request for more sophisticated methodologies, which should be difficult to evade, not relying on pre-established and well-known rules that might be easily sidestepped.

Graph analytics has emerged at the forefront as an ideal technology to support AML analysis because money laundering involves cash flow relationships between entities (i.e. network structures). Graphs overcome the challenge of uncovering relationships in massive, complex and interconnected data, designed from the ground up.

A lot of anti-money laundering use cases require identifying suspicious connections whereas graph analytics is designed to analyze complex connections from big data at scale. Multiple graph types can be constructed. A graph can be formulated where a single account is represented as a vertex and a single transaction between two accounts is represented as an edge. Another approach is to represent a group of accounts as a vertex (e.g. such as those under a holding company, or such as those inferred to share an owner via clustering) and define an edge as the aggregate transaction volume with a neighboring node over a period of time.

There is a set of core problems in AML that impose challenges and require solutions which graph analytics has a capacity to address.

One example is **Identification of Politically Exposed Persons and sanctions screening:** FIs are tasked with screening their clients to identify their potential ties with politically exposed persons (PEPs) or individuals and organizations that are on sanctions lists (such as the lists published by the Office of Foreign Assets Control). These persons represent heightened money laundering risks. The relationships between a client and risky entities can be as simple as a client and a politically exposed person sharing the same address. In this case, detecting such a situation is easy. What if indeed the risky entity wants to engage in money laundering? Chances are that a lot of effort will go into hiding the relationships to escape enhanced due diligence. Graph analytics can identify such indirect relationships across multiple types of entities and relationships (addresses, co-owned companies, IP addresses, phone numbers, transactions, etc.).

Another example, **Entity Resolution** (ER) is a problem where each person or company in databases would be unique. Chances are though that it's not the case. Maybe the *David Johnson* that exists in the retail bank database has a different ID than the *David Johnson* of the consumer credit database or of the *David Johnson* in the company owners database, despite the fact that these 3 individuals are actually the same person. Avoiding this sort of duplication is a complex problem in an IT system with different silos. Graph analytics can detect common links across different entities to help identify potential duplicates. Maybe even though the 3 *David Johnson* have different IDs they all share the same date of birth, the same address and the same phone number. If so, chances are that they are indeed the same person.

Ultimate Beneficial Ownership (UBO) is additional interesting example where FIs are tasked with identifying UBOs. These are individuals that own a client, or on behalf of whom, a transaction is made. Sometimes that requires following a long chain of ownership relationships by taking into account relevant ownership thresholds. If a company is owned by a single shareholder, things are easy. It gets tricky when the number of ownership layers increases. Manually looking at the ownership structure of each company to identify its UBOs and repeating the process until there are no new UBOs is a time consuming and error-prone process. This type of analysis can be translated into a single graph query to automate the process. The result can also be visualized. Compliance analysts can look into the overall ownership graph to identify where a problematic UBO sits, for example.

Conclusion

The cases in which graph analytics can be beneficial in helping to detect money laundering efforts continues to grow. As criminals become more and more sophisticated in how they launder money, so too do the tools that help fight back against them. Money laundering efforts don't stand a chance when FIs are equipped with graph analytics.
