Using Data Analytics to Identify AML Risk

Data is the lifeblood of financial institutions and other organizations. It is used to run processes, manage financials, predict risk, prove compliance, target customers and influence decisions. In anti-money laundering (AML) and compliance, the data required to identify and combat financial crime is complex. It is also difficult to gather because data is often stored across a patchwork of legacy systems, new systems and siloed business-specific applications. Data quality can vary greatly. Working with unreliable, incomplete or inconsistent data makes it difficult to identify bad actors who pose a financial and reputational threat, which undermines an institution’s ability to efficiently manage risk across the enterprise.

The more complex and geographically diverse a financial institution is, the greater the threat. Institutions with very large customer databases and transaction volumes that span numerous distribution channels and counterparties face the greatest number of challenges and the most risk.

The slinging arrows of risk

Traditional AML defenses that rely primarily on static rules to identify questionable individuals and activities are coming up short. Despite continued investment in AML technology and processes, institutions seem unable to keep pace with external threats from drug cartels, corrupt public officials, terrorist organizations and other bad actors that have developed increasingly sophisticated tactics to avoid detection. These savvy criminals know how to play the game. They will often cloak their malicious activities by keeping within the defined set of rules. One example of how criminals fly under the radar is through smurfing. By limiting transactions to under $10,000, they avoid triggering a currency transaction report.

Internal threats—whether unintentional human error or intentional fraud—must also be considered when managing enterprise risk. In addition to internal and external threats, emerging payment technologies and the digitalization of banking have introduced yet another set of risks to the AML landscape.

Cyber risk, social media monitoring and data management are all crucial considerations that have caught the attention of regulators, who have come to recognize that traditional, rules-based methodologies may not be optimal for certain typologies. Check-the-box compliance is not enough. Regulators expect banks to have defensive processes and systems in place to proactively seek out and catch perpetrators, whether external players or internal employees.

Big data, big challenges

Know your customer (KYC) regulatory requirements have compelled institutions to collect increasing amounts of data on customers and their transactions. Static, rules-based systems are not designed to handle huge stores of unstructured, internet-scale data. As a result, they produce an enormous volume of false positive alerts. More data only produces more false positives when screening for sanctioned entities or money laundering.

Managing the deluge of false positive alerts is a major pain point for many institutions. Not only is the process inefficient and operationally expensive, but it complicates an institution’s ability to quickly and accurately identify risk. The knee-jerk reaction of “throwing more bodies” at the problem is not the answer. Adding resources just drives up the cost of compliance and increases the risk of human error.

Driving change

The big data phenomena brought a proliferation of technology that can help meet the analytic and architecture challenges of AML, KYC and counter-terrorist financing. Data science, data analytics and other advanced technologies like artificial intelligence (AI) and machine learning offer a dynamic approach that is better suited to complex internet-scale data than static models. According to a report published by Celent, “AI-enabled solutions can not only...”
Automate significant parts of operations but also offer superior insights through advanced capabilities for analyzing structured and unstructured data."1

These dynamic models focus on patterns rather than individual data points or transactions. They detect anomalies, making it easier to identify behavior that truly accounts for malicious activities. Dynamic models enable institutions to keep pace with changing requirements while also resolving the costly problem of reducing false positives.

Integrating non-traditional data sources into a data management program will improve the effectiveness of detection and ongoing due diligence. Non-traditional internal and external data sources can include documents, newsfeeds, images, video, social media, clickstream data and machine log data. Driving the growth of these variable data sources are an increase in client interactions and the digitalization of business processes.

While these new data sources offer a wealth of information for AML and compliance purposes, traditional structured query language-based analytic techniques may not be well suited for these non-traditional data sources because their pre-set schemas vary and change often. For this reason, an alternative approach for analyzing data uses programming languages such as Java, Python and R. These coding languages are often chosen for big data and analytical tools for several different reasons. For example, Python has become a popular choice for applications because it relies on the most cutting-edge techniques, such as AI, machine learning and natural language processing.

The ability to integrate non-traditional internal and external data sources enables institutions to go beyond basic analytics to identify risk more quickly and efficiently. When transaction data is enriched with client/legal entity data (including names, addresses and other identifiers), and publicly available OFAC lists, banks can track transactions to determine if they were completed by known high-risk individuals or non-cooperative jurisdictions. Going one step further, enriching this data with verbal and written communications information can help cast a wider net when looking at potential indicators.

**Tip of the iceberg**

Fighting crime with big data and analytics still has a long way to go. Industry pioneers who wish to move beyond analytic technologies are looking toward cutting-edge solutions based on probability and inductive, heuristic logic that detects money laundering by replicating an analyst’s thought processes. This is the future state of advanced capabilities that institutions require to address comprehensive AML and compliance challenges in a dynamic environment. With the right investment in the right technology and data platforms, institutions can be confident that they have a clear view of risk across the enterprise. "

---


Carol Stabile, CAMS, chief sales and marketing officer, Safe Banking Systems, Mineola, NY, USA, carol.stabile@safe-banking.com