Customer Screening

From “Name Matching” to Contextualized “Identity Matching” with Advanced Analytics

By: Matthew Long, Director, Financial Crime & Compliance Solution Consulting
The increasing understanding and industry/regulator acceptance of how advanced analytics could be applied and integrated with human inputs is driving new Financial Crime and Compliance program thinking and opportunities.

For example, research\(^1,2\) suggests that, as part of the ongoing evolution of the Anti-Money Laundering (AML) program, the industry will witness tighter integration of risk assessment, due diligence, monitoring, investigative, reporting, and governance processes. Advanced analytics, machine learning, and graph analytics, in particular, will play a critical role in breaking down the silos and providing a contextual basis for better determining risk, detecting suspicious activity, and improving process efficiencies.

According to research by the U.K. financial services regulator\(^3\), customer screening is an area where firms were universally positive about the potential impact of new and emerging technologies on their compliance efforts, including:

- Using better probabilistic matching and analytics technologies to improve the quality of the Politically Exposed Person (PEP)/sanctions screening activities and better identify potential individuals and entities with a higher degree of certainty
- Leveraging advanced matching technologies, such as analytics-driven “fuzzy matching” to reduce reliance on (sometimes outdated) vendor data

The U.K. regulator further noted that a key use case for technology in customer screening was around the use of analytics to reduce false positives. In fact, a number of respondents identified the processing of false positives as their largest unnecessary manual overhead in AML compliance generally.

**CURRENT PROGRAM AND SYSTEM LIMITATIONS**

Customer screening programs and processes within regulated firms take into account a variety of risk factors and data points, such as individual/organization name, address, date of birth/date of incorporation, country of residence/incorporation, product, industry type, company structure, and negative news/adverse media.

However, most current customer screening solutions rely on rules-based name matching criteria to identify potential matches, along with secondary identifiers (e.g., date of birth or location) to reduce false positives. An analyst will manually investigate and review the event/alert to create and check the context, identify any linkages of interest to other entities, and gather customer documents and other data, such as media searches, required to support a final decision. This is very often a significantly manual task for the investigator\(^4\). (See Figure 1.)

---


Most solutions do not automatically and proactively consolidate this wider contextual information and utilize the wider sets of relevant data available to the firm, such as information on the closest relatives or business partner information of the sanctioned individual/entity or PEP, to really understand who they are, the context in which they operate, and the risks they pose.

Even when a degree of automated decisioning has been based on the creation of data lakes, this approach can still cause issues and process inefficiencies. These complications arise due to a combination of poor or unconnected data creating an inaccurate view of a customer or a lack of context in which none of the interactions between businesses, or individual relationships, is effectively captured in the customer view.

As in all financial crime and compliance management (FCCM) solutions, poor data quality causes multiple issues (garbage in—garbage out rule). For example, there could be a customer firm called “Anti-Bribery & Corruption Inc.,” which would match against a list entry called “ABC” on the basis of an initials-only match. This type of example can generate numerous false positives or, worse, situations in which the analyst lacks further data points to determine with a degree of certainty as to whether this is a true or false match.

If a financial crime investigator spends just 10 minutes per day toggling in and out of software to retrieve data and if that task could be automated, they would save approximately 40 hours over the course of a year. For a 10-person team that equals 2.5 person-months saved simply by reduced toggling.


In thinking about a typical financial crime or compliance investigation, approximately what percent of time per month does an analyst spend on manual processes such as phone calls, emails and collection of data? (Respondents could choose only a single response.)

![Chart showing percentage of time spent on manual processes](source: “Transforming Financial Crime Investigations through Automation,” PwC, 2016.)

**ENTITY RESOLUTION, ADDING INVESTIGATIVE CONTEXT, BUILDING IDENTITY, IMPROVING RISK PROCESSES**

Recognizing these current issues, inefficiencies, and limitations, Oracle is empowering firms to augment the initial customer screening event (e.g., the potential watch list name match) by incorporating the context that is offered by the application of graph analysis.
That, together with the appropriate application of process automation/event scoring and machine learning can drive actions, such as:

- updating the initial customer-screening event rating
- updating the overall customer risk score in a firm’s Know Your Customer (KYC)/Customer Due Diligence (CDD) engines, or
- generating a direct process step, such as moving the customer to the appropriate enhanced due diligence (EDD)/PEP queue, together with a more accurate risk score and all of the known information gathered by the graph analysis to accelerate the final business decision.

Similarly, with an advanced-analytics-empowered process, the system can learn from analysts’ previous decisions and/or the firm’s risk appetite to proactively propose improvements to the screening rules and process to improve the relevance of events and the next steps in the process. For example, improving the targeting of which parts of the AML risk data set are most important to the firm at any point in time (e.g., source type, crime type, risk age, geography, product type) to enable the compliance function to continually optimize their use of the system.

In the following simple graph example, based on an initial customer screening trigger event on John Doe (watch list name match), the firm would be able to use all of the data available to it in the company, augmented with web searches or input from negative news engines, to obtain a much richer and comprehensive picture of who John Doe actually is, the risk he poses, and what the next steps should be. (See Figure 2.)

![Graph Example](image)

**UNCOVERING HIDDEN RISK**

Similarly, when looking at the wider network of relationships and entities linked to the John Doe example, the graph would further highlight areas of AML risk for the system/analyst to take into account. For example, the business owned by John Doe, is, in turn, owned by an overseas company with links to high risk/sanctioned countries. (See Figure 3.)
LINKING CRIMINALS, PEPS AND SANCTIONED INDIVIDUALS/ENTITIES TO SHELL COMPANIES

“Criminals employ a range of techniques and mechanisms to obscure their ownership and control of illicitly obtained assets. Identifying the true beneficial owner(s) or individual(s) exercising control represents a significant challenge for prosecutors, law enforcement agencies, and intelligence practitioners across the globe. Schemes designed to obscure beneficial ownership often employ a “hide-in-plain sight” strategy, leveraging global trade and commerce infrastructures to appear legitimate.

Analysis of 106 case studies demonstrates that legal persons, principally shell companies, are a key feature in schemes designed to disguise beneficial ownership, while front companies and bearer shares are less frequently exploited.” (FATF – Egmont Group, 2018)

Due to the anonymity of ownership they have historically offered, shell companies have been an attractive way for money launderers, fraudsters, and other financial criminals to hide their assets and avoid/evade taxes or to launder criminal funds.

The introduction of public beneficial ownership registers in some European countries has been a major step forward in preventing the abuse of companies. However, as seen in highly publicized schemes that include foreign property investment, some are still being used to launder corrupt wealth. As such, they represent an ongoing risk.

---


As seen in the Panama Papers and other similar investigations, shell companies are often formed using the address of the incorporating entity or service. Although, there is often a legitimate business reason for this, the common incorporation address is just one of many red flags or indicators for the graph analytics-enabled process to consider.

The utilization of advanced analytics can help to determine where these structures are potentially being deployed and identify links to higher-risk customers, such as PEPs or sanctioned individuals/entities.

CONCLUSION

The use of advanced analytics enables firms to accelerate the evolution of their customer screening processes from simple “name matching” followed by complex manual data gathering and investigation to more contextualized “identity matching” with a leaner and more intelligence-led process.

Firms can leverage graph analytics and machine-learning-enabled processes to take into account large numbers of data attributes and help them gain a holistic view to score the probability of a true identity match.

Given the nature of a graph database, firms can use machine learning search algorithms to query the linkages between entities faster and more efficiently than a traditional rules-based system analyzing a flat file.

Using machine learning, organizations can train screening systems to present next-step recommendations on the most likely decision the analyst/investigator will make for lower risk scenarios, while highlighting the most relevant information and the rationale behind the suggestion.

This approach empowers firms to more accurately deploy the risk-based approach demanded by the regulators and allows compliance teams to focus their time and investment on higher-risk, higher-probability and higher-complexity issues, which is where the human touch truly adds value.