ORACLE
Financial Services

Next-Gen Customer Screening & Transaction Filtering

Entity resolution, enhanced investigative context, network analysis/scoring, building identity, uncovering risk, and improving operational processes are among the many uses of advanced analytics and data quality management in enhancing sanctions screening and transaction filtering processes

By: Matthew Long, Director, Financial Crime & Compliance Solution Consulting,
Oracle Financial Services

As current screening and filtering programs struggle to respond to the complexity of the modern trading and sanctions environment, organizations are increasingly turning to advanced analytics, graph pattern matching in particular, and more robust data quality management solutions to help achieve greater customer and transaction insights as well as operational efficiency.

The problems and potential risks associated with the ever-changing and hugely complex international sanctions regime represent a dynamic financial crime and compliance (FCC) challenge. Historically, economic "sanctions" targeted activities such as trade, financing, and banking, but increasingly the use of sectoral sanctions has become more complex and nuanced. For example, United States (US) sanctions include secondary sanctions in the Russia/Ukraine context and the possibility to impose sanctions on foreign financial institutions that fulfill one of the below:

1. engage in certain significant transactions involving defense-related activities by sanctioned persons
2. engage in significant transactions involving investment in special Russian crude oil projects
3. facilitate a significant financial transaction on behalf of any Russian person on the Specially Designated Nationals and Blocked Persons (SDN) List under a Ukraine/Russia program.

Similarly, the US introduced Executive Order 13846[1] to re-impose mostly secondary sanctions targeting Iran. In response to the US decision, the European Union (EU) issued an updated Blocking Regulation in the same month [2]—aiming to counter the effects of these re-imposed US sanctions on EU companies. As a result, both jurisdictions have signaled much tougher enforcement, which could put EU entities in a challenging position.

Further complexity arises with regard to the "50% rule" imposed in EU and US sanctions policies. The rule places an increased burden on organizations that deal with entities, which, while not directly associated with them, are linked to sanctioned entities—putting the organization at risk of enforcement. This development pushes sanctions and screening programs to include subsidiaries and any company where a sanctioned individual may have more than a 50% ownership stake—often a challenging operational and technological ask.

As the complexity increases, so does the cost of compliance and the cost of getting it wrong. To help address this environment, organizations are looking to advanced analytics and data quality management capabilities to help ensure they not only remain compliant, but keep their compliance costs under control.

"The pace and complexity of geopolitical change, a constant fluctuation of sanction regimes between tightening and lifting, combined with heightened regulatory scrutiny, fragmented customer and payment data, outdated technology, and high numbers of false positive alerts is creating multiple challenges for organizations and their underpinning screening and filtering programs."

Matthew Long, Director, Financial Crime & Compliance Solution Consulting, Oracle Financial Services

CURRENT PROGRAM AND SYSTEM LIMITATIONS

Customer screening and transaction filtering programs and processes 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, correspondent bank, and message type.

[1] Reimposing Certain Sanctions with Respect to Iran, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/08062018_iran_eo.pdf.
[2] Updated Blocking Statute in Support of Iran Nuclear Deal, http://ec.europa.eu/dgs/fpi/what-we-do/blocking_statute_en.htm.

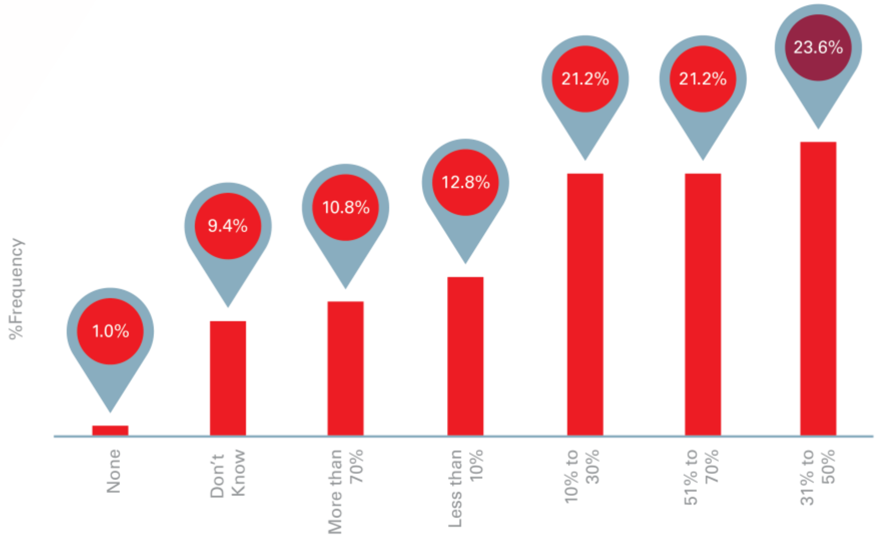
However, most current screening solutions rely on rules-based name matching criteria to identify potential matches, along with secondary identifiers (e.g., date of birth or location) to reduce false positives. An analyst will manually investigate and review the event/alert to create and check the context, 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, time consuming (see Figure 1), and frustrating for the customer when his or her assets/payments are being held or delayed.

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

Even when a degree of automated decision-making is in place, complications can arise due to a combination of poor or unconnected data, creating an inaccurate view of a customer, the purpose of the transaction, or a lack of context in which none of the interactions between businesses or individual relationships is effectively captured.

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 organization 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.

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.)



Source: “Transforming Financial Crime Investigations through Automation,” PwC, 2016, https://www.pwc.com/us/en/industries/financial-services/financial-crimes/library/investigation-automation.html.

Figure 1.

“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.”

Source: “Transforming Financial Crime Investigations through Automation,” PwC, 2016

ENTITY RESOLUTION, ADDING INVESTIGATIVE CONTEXT, BUILDING IDENTITY, IMPROVING OPERATIONAL PROCESSES

Recognizing the current external issues detailed in the introduction to this paper, along with the internal process and system inefficiencies and limitations noted previously, organizations are seeking ways to augment the initial trigger event (e.g., the potential watch list name match) with relevant investigative information available through the application of graph analysis, including the data gathering and assessment steps usually completed by an analyst.

That, together with the appropriate application of process automation/event scoring and machine learning, can drive actions, such as:

- updating the initial screening event rating
- supporting the investigator by completing the historically manual link analysis process through use of graph pattern matching on all known relationships and prior history
- updating the overall customer risk score in an organization’s Know Your Customer (KYC)/Customer Due Diligence (CDD) engines
- generating a direct process step, such as moving the customer to the appropriate Enhanced Due Diligence (EDD)/PEP queue to accelerate the final business decision

Similarly, with an advanced-analytics-empowered process, the system can learn from analysts’ previous decisions and/or the organization’s risk appetite and policy 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 risk data set are most important to the organization 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 organization would be able to use all of the data available to it internally (e.g., transaction and customer records, prior suspicions), automatically augmented with external data, such as web searches; input from negative news engines; external watch lists/data, such as that provided by Companies House in the UK; beneficial ownership registries; and publicly-sourced data, such as the Panama Papers, to obtain a much richer and comprehensive picture of who John Doe actually is and the risks he and the broader network that he’s a part of pose, and what the next steps should be (Figure 2).

“With a graph technology, the basic premise is that you store, manage, and query data in the form of a graph. Entities become vertices and relationships become edges.

By analyzing these fine-grained relationships, you can use graph analysis to detect anomalies with queries and algorithms.

The major benefit of graph databases is that they’re naturally indexed by relationships, which provides faster access to data. You can also add data without doing a lot of modelling in advance.

These features make graph technology particularly useful for anomaly detection.”

Source: 5 Innovative Ways to Use Graph Analytics
https://blogs.oracle.com/bigdata/fraud-detection-use-cases-graph-technology

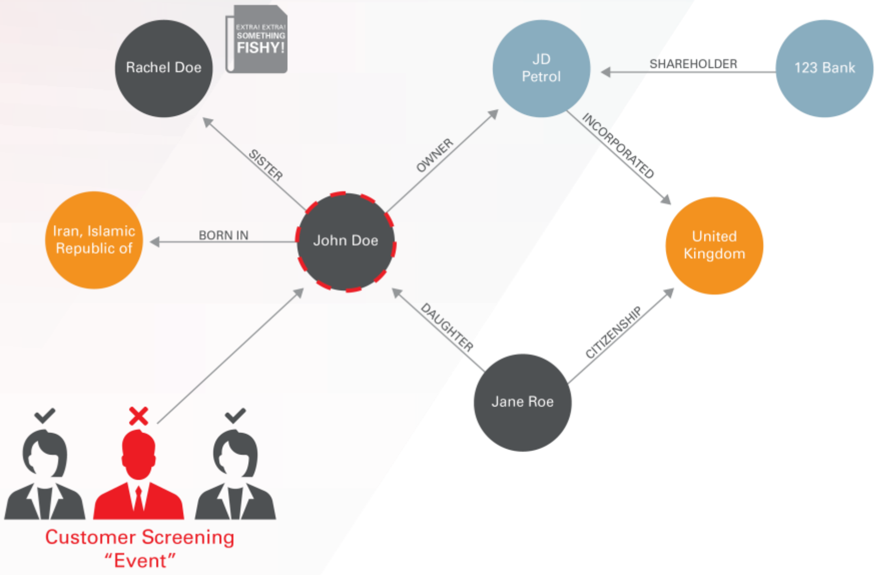


Figure 2.

As part of building the graph and ensuring a holistic and efficient investigation process, entity resolution along with data accuracy and quality, is essential. Entity resolution, as a topic, is tackled in a separate whitepaper, however, the following simple example (Figure 3) shows factors that would help support the resolution of two apparently separate entities into a single record (in this case, "John Doe") through the application of fuzzy logic on certain data points and a sufficient degree of confidence that the names, email addresses and accounts that interact with the same counter parties point to this being the same person and can, therefore, be treated as one record to process / investigate.

Entity resolution… "*helps organizations create a unified record for individuals and other entities by combining data and information from multiple sources and resolving the different spellings, text styles, photos, and addresses".*

"The Business Value of Entity Resolution Solutions for Financial Crimes and Compliance Operations," IDC September 2017

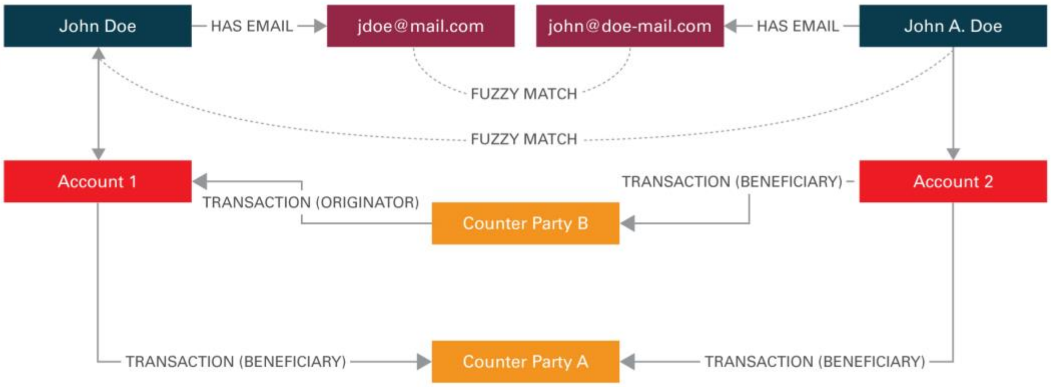


Figure 3.

During manual investigations and/or using current technologies, identifying and assessing these potential linkages and then consolidating them into a single record can be timely and challenging, particularly given the increasing volume and variety of data available about customers and their relationships.

Entity resolution provides organizations with an efficient and cost-effective means of ensuring financial crime compliance and process efficiency. Without the ability to process and analyze large volumes of customer data, organizations would have to continue employing ever increasing numbers of staff to manually collect, manage, and use the data within their compliance processes.

UNCOVERRING HIDDEN RISK

Once the entity has been resolved, the graph can be used to further highlight areas of risk for the system/analyst to take into account by generating and visualizing the network of relationships and entities linked to the John Doe example. 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 4.)

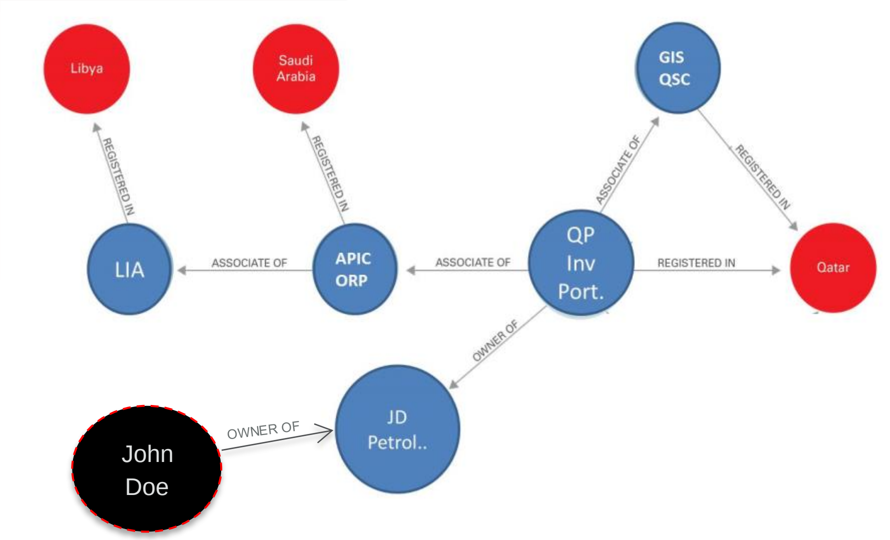


Figure 4.

Through implementing or improving on existing entity resolution capabilities, organizations can help reduce the risk of non-compliance with regulations and drive down manual resourcing costs through improving investigative/analyst efficiency.

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."*
>
> — The Financial Action Task Force on Money Laundering (FATF) – Egmont Group, 2018[3]

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 shell companies. However, as seen in highly publicized schemes that include foreign property investment[4], 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.

DATA PREPARATION IS CRITICAL

Data used in screening principally contains names, addresses, countries, and (in the case of individuals) dates of birth. For corporations or other entities, it also includes company registration and other details, plus data on key executives, stakeholders, and beneficial owners. This data is likely to contain anomalies that will reduce the accuracy of the screening process, but it is also likely that the data being used in the screening will also have anomalies or imperfections that will impact screening results.

In addition, many organizations with a global footprint hold their data in international language scripts. This presents a problem when these organizations screen against sanctions and commercial watch lists, the majority of which are in Latin script and typically include limited translations of name data into Latin phonetic equivalents.

[3] FATF – Egmont Group (2018), Concealment of Beneficial Ownership , FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/concealment-beneficial-ownership.html.
[4] "Shell Company Frontmen Face Prison Sentences in Crackdown on Dirty Money in U.K. Property Market," *The Independent*, March 22, 2018, https://www.independent.co.uk/news/business/news/shell-companies-money-laundering-crackdown-prison-uk-property-market-a8269281.html.

Increasingly, to effectively use content provided by both commercial and open-source list providers, organizations need to prepare data in a manner that goes beyond simple name cleansing. They need to include attributes such as nationality, country of residence, membership in certain regimes or political parties, close associates (otherwise known as "secondary identifiers"), and writing system used.

Extensive profiling and auditing of the data ahead of screening is, therefore, crucial. Techniques such as profiling, auditing, transforming, and analyzing text can be used to validate data against source systems. Often this will allow for removal of white spaces or questionable characters or split a single name field containing multiple attributes into a number of discrete fields, enabling data to be optimized to match rules.

One of the most effective (but often overlooked) methods of reducing false positives and regulatory risk is to ensure accurate preparation of data sources ahead of screening.

This is because the accuracy of underlying data directly influences the results of any screening solution. Following are examples of how results can be skewed when poorly prepared data enters the screening system:

- Excessive numbers of false positives often occur when match rules cannot adequately process poor quality data. Invalid, incomplete, or inconsistent client data undermines most screening systems, resulting in mountains of repetitive false positives and screening criteria set so loose that the results are meaningless.
- Excessive numbers of false negatives can result from screening when inaccurate or poorly structured data enters the system. Data pollution is a fact of life in most organizations, yet it is intensely problematic for typical screening systems. For example, an entity name stored as "AIR-CON INC. T/A PRIME AIR-CONDITIONING SOLUTIONS" will not reliably trigger a match against "Air-Con Inc" in systems that are incapable of accurately parsing data and executing powerful fuzzy matching algorithms.

Once data preparation is complete, a careful balance needs to be struck in defining and applying the match rules for each risk profile being screened. Simply narrowing the screening criteria reduces the number of false positives; however, this increases the risk of a genuine threat evading detection. Therefore, quick and simple fine-tuning of highly granular match rules is needed to achieve an effective balance between minimizing both potential risk and the compliance team's workload.

Accurate screening also relies on non-exact complex fuzzy matching. This is because criminal elements targeting organizations often transpose names, dates of birth, and other personal information to attempt to conceal their true identity.

Effective screening will differentiate between individuals and entities with common names, but will have discrete match rules available that can be activated. With the correct definition and application of rules to customer and list data sources, along with the use of secondary identifiers as part of the screening process, false positives can be reduced to a minimum without increasing risk.

CONCLUSION

The use of data quality management and advanced analytics enables organizations to accelerate the evolution of their screening processes and complex manual data gathering and investigation to more contextualized "identity matching" with a leaner and more intelligence-led process.

False Positive: *A match produced by the system that, following subsequent investigation, turns out to be wrong.*

False Negative: *A genuine risk is missed by the system and is not flagged for attention. This can be seen as a weakness in the matching solution, but in practice, is often caused by poor quality of source data.*

Organizations 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, organizations 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.

Effective data preparation, whatever writing system is used to capture the original source data, is paramount in both minimizing the number of false positives and reducing the risk of false negatives. Techniques such as risk scoring and the use of secondary identifiers can also simplify identification of those individuals and entities contained within a PEP database that present the greatest threat to an organization – enabling it to take rapid action to eliminate unnecessary sources of risk.

This approach empowers organizations 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.

More information on customer screening techniques and data issues and improvements can be found at http://www.oracle.com/us/industries/financial-services/ofs-customer-screening-guide-3590304.pdf.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracleFS facebook.com/oracleFS twitter.com/oracleFS

ORACLE

Integrated Cloud Applications & Platform Services