protiviti®
Global Business Consulting

SANCTIONS SERIES

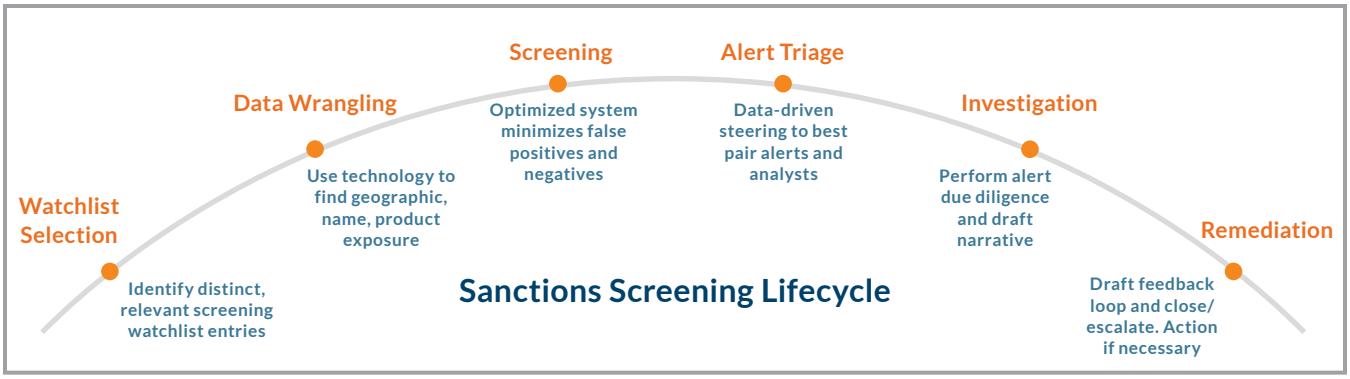
Advanced Analytics in Sanctions Compliance

by Thomas Dessalet and Edwin Oloo

The adoption of advanced analytical tools and emerging technologies such as artificial intelligence and machine learning (AI/ML) has continued to gain enterprise adoption across compliance solutions within the financial services industry. While the advantages of these techniques are widely accepted and continue to be leveraged and monetized in the domains of transaction monitoring, customer segmentation and risk rating, their adoption in sanctions programs lags in relative comparison. Despite robust progress in compliance model development, regulatory bodies, internal and external auditors, and compliance stakeholders often do not enthusiastically embrace approaches which augment human judgment with emerging technology. However, that does not disqualify the use of other analytical tools in the pursuit of a leading, efficient and risk-based sanctions program.

There are ample opportunities to leverage an analytics-focused, data-driven approach to enhance sanctions screening compliance programs during all phases of the program workflow. The illustration below depicts this approach and is followed by a discussion on how technology, including AI, and analytics can drive advances in these programs.

There are ample opportunities to leverage an analytics-focused, data-driven approach to enhance sanctions screening compliance programs during all phases of the program workflow.



Watchlist Selection: Overlap Reduction

The use of multiple screening lists with significant overlap of entities may add to the complexity and costs of system maintenance and testing, while also increasing analysts' efforts to resolve unnecessarily duplicative alerts. Analytics will assist with the consolidation of lists and the identification and removal of overlap among watchlist parties.

List overlap identification can be performed in Python (and/or other open-source technology/ tools) to identify distinct list entries. If naming conventions differ among lists due to regional, linguistic or alphabetic differences, open-source fuzzy logic algorithms and constructs such as RapidFuzz, FuzzyWuzzy or Jaro-Winkler can be applied to quantify levels of similarity between text strings. These algorithms serve to measure the "distance" between two text strings. In other words, edit-distance algorithms can be utilized to quantify the sameness of the character strings in question, with tolerances identified by the user. The result is a streamlined list of unique entries, reducing double-counting and eliminating the artificial inflation of sanction alert volumes.

Data Wrangling: Named-Entity Recognition for Critical Element Identification

Most sanctions screening programs identify potential matches solely through comparison of watchlist entities to text strings in fields commonly identified as compliance-critical data elements. Named-entity recognition (NER), a type of natural language processing (NLP), is an analytical approach to text mining of large, unstructured or otherwise unformatted data. Nimble in nature, NER tools identify tokens, or critical named-entity strings, within fields explicitly mapped to contain a name, as well as within free-format text fields such as payment notes and/or in analyst comments on onboarding forms.

The critical fields required for sanctions screening show up in various points along an institution's compliance operations lifecycle. For example:

- In order to support a robust customer identification program (CIP), onboarding documentation should include name, address(es), date of birth, SSN/TIN, etc., which are usually entered in clearly defined form fields.

- Ongoing customer due diligence (CDD) often entails re-screening of this same account data at a later time on a risk-based frequency.

NER can identify potential matches against watchlist entities based on the aforementioned fields.

We can draw another illustrative example from the payments arena. Payments subject to sanctions screening require similar critical fields for counterparties, including financial institution information. For example, 31 CFR 103.33(g) of the Bank Secrecy Act, known as the "Travel Rule," identifies the minimum required fields to be populated for funds transfers greater than $3,000 USD (or equivalent). Because many data elements critical to sanctions screening are required by such regulations, NER can be used on free-format fields such as those in SWIFT wire messages or peer-to-peer payment notes on platforms such as Venmo or Zelle.

Risk mitigation through robust CIP, CDD, payment screening and Travel Rule controls is considered the bare minimum action and often relies on screening against a pre-determined mapping of fields. A common gap in screening coverage is not that critical fields are missing from data — it is that the critical fields appear outside the mapped locations the system is programmed to screen. Through techniques such as NER, institutions create coverage against the risk from these gaps.

A common gap in screening coverage is not that critical fields are missing from data — it is that the critical fields appear outside the mapped locations the system is programmed to screen.

Data Wrangling: Geolocation Use Cases

1. Vessel tracking

It is not only individuals and institutions that are sanctioned. Institutions offering trade finance services have a vested interest in keeping sanctioned vessels away from their financed or insured fleets. The use of automatic identification systems (AIS) is mandatory for most vessels of cargo-carrying size[1] and the corresponding AIS latitude and longitude pings are available from subscription data sources for analysts interested in monitoring fleet movements. Armed with distinct vessel identifiers governed by the International Maritime Organization (IMO) and pairwise time-location datapoints, model users can predict future paths and timing of trade finance cargo with regard to risky locales and/or other vessels of interest.

[1] *Vessel Ownership, Trade Finance and Regulatory Compliance*, S&P Global Market Intelligence, April 2023: https://tradefinanceglobal.com/wp-content/uploads/2023/04/Vessel-OwnershipTrade-Finance-and-Regulatory-Compliance.pdf.

Analysts can establish controls for tracking the location of real-time movements against specific regulatory sanction lists or organization bad-guy vessel lists to detect (or proactively minimize) proximity to higher-risk encounters at sea. Risk rating of vessels for monitoring purposes may include factors such as:

- Prior suspected ship-to-ship transfers
- Transshipment of goods to mask origination location or obfuscation of cargo details
- Lack of clear identification of vessel ownership
- Geographic/jurisdictional ties based on ship registry
- Prior high-risk vessel activity locations — with significant attention focused on ports in sanctioned countries

Tracking models are created to identify proximity of trade financed vessels to sanctioned vessels, measure vessel time in port, or highlight any offshore anchorages (which are susceptible to the illicit ship-to-ship transfer of sanctioned goods). Vessel location data, including latitude, longitude, timestamps and directionality, combined with bill of lading information, support the use of a graphical interface like Tableau, QlikView or PowerBI for visual reporting of potential sanctioned activity in near real-time. Furthermore, use of advanced analytics and ML techniques such as social network analysis (SNA), graph analysis and matrix completion, among others, can be leveraged to detect trafficking, missing or falsified data. Additional benefits to vessel tracking include the ability to predict trade finance-related operational delays in and around ports.

2. Payments

Analysts can establish controls for tracking the location of real-time movements against specific regulatory sanction lists or organization bad-guy vessel lists to detect proximity to higher-risk encounters at sea.

With the omnipresence of peer-to-peer instant payment services and virtual currencies, sanctions risk mitigation is paramount. The ability of institutions to identify the geographic locations of payment counterparties — whether through IP address tracking or geolocation software — is the backbone of such compliance. In late 2022, the Office of Foreign Assets Control (OFAC) issued guidance[2] reinforcing the risk-based need for instant payment providers to utilize adequate technology to remain in control of both domestic instant payments to potentially sanctioned individuals and cross-border instant payments to sanctioned individuals or jurisdictions.

[2] "Sanctions Compliance Guidance for Instant Payment Systems," September 2022: https://ofac.treasury.gov/media/928316/download?inline.

Compliance stakeholders should consult with their respective IT resources to identify the capabilities already leveraged in other departments — for example, IP address identification leveraged for cybersecurity in online banking — to mitigate sanctions risk. In addition to identifying the location of IP addresses, other geolocation techniques include but are not limited to GPS, Wi-Fi positioning, cell tower triangulation, radio frequency identification (RFID), Bluetooth beacon technology and mobile network data.

3. Combating evasion

In order to capture and stem sanctions exposure, the identification and accuracy of geographic location data is of utmost importance. Sanctions evasion takes many forms and can be seen as either intentional from the users or negligent on the institution's behalf. Neither is acceptable. The challenges to corral, clean and utilize geolocation data for combating the evasion of sanctioned activity involve both the products and methods of transactions.

In order to capture and stem sanctions exposure, the identification and accuracy of geographic location data is of utmost importance.

The exchange of virtual currencies poses heightened sanctions risk due to the degree of anonymity of the counterparties, coupled with the ease of disguising the end users' locations. For other payments, the use of virtual private networks (VPN), proxy servers and other location-spoofing techniques are hurdles which must be cleared with advanced location identification techniques. Due to this widespread prevalence, OFAC advocated for the use of advanced geolocation technology against VPNs and proxy servers in official guidance directed at identifying the ultimate IP address/location of persons in comprehensively sanctioned jurisdictions.[3]

Sourced solutions exist that can alleviate the burdens of location detection and may leverage the following:

- **Wi-Fi positioning:** Leverages the location information from nearby connected devices, routers, mobile hotspots, etc.
- **Mobile GPS:** Location pings can geolocate users performing transaction activities from mobile devices not connected via Wi-Fi.
- **Cell tower triangulation:** The use of multiple telecommunications towers can pinpoint the location of a pinged mobile device based on signal strength and response time.

[3] *Sanctions Compliance Guidance for the Virtual Currency Industry*, Office of Foreign Assets Control, October 2021: https://ofac.treasury.gov/media/913571/download?inline.

Proprietary solutions exist for geolocation using some mix of one or more of the above (though data availability and acquisition remain the most significant challenges for identification of referential geolocation data). The savings from the costs of geolocation tools can be recouped in the form of tangible benefits such as reduced penalties for lack of compliance, as well as additional intangible enterprise benefits such as mitigating negative reputational/headline risks. As with most compliance costs, the downside risk in the form of reduced penalties from sanctioned activity greatly outweighs the technological and operational expenditure. The ability to streamline operations in a quick and lean manner using instantaneous geolocation also reduces the costs, both time and monetary, of manual identification of payer location within permissible areas.

Screening: Optimized Good-Guy Lists for False Positive Reduction

Data analytics can support the use of good-guy lists with a risk-based approach to transactional and referential data analysis. By using the historical activity of an entity, such as a lengthy history of prior false positive alerts, institutions can rationalize with confidence the "why?" of false positives. This may be as simple as determining that in a system which only uses name fields for matching an individual who frequently triggers alerts, the person has a different date of birth or SSN than the sanctioned individual. Based on the results of this triage, the alerting party is assigned to the system's good-guy list and corresponding narratives are pre-prepared with the documented support for a quick closure based on the mitigating factors.

Maintenance of good-guy list names should include periodic review to confirm that inclusion of names on the list is still appropriate. Supporting data to reaffirm good-guy listing during this review should include the most recent output/results generated from running the current up-to-date good-guy list against in-scope watchlists.

Alert Triage, Investigation and Remediation: Workflow Simplification

With the current availability of open-source analytics tools, institutions have the ability to challenge the operational efficiency of out-of-the-box vendor workflows. By assigning a risk-rating to sanctions screening hits or otherwise triaging alerts into useful groupings, compliance management can ensure the most efficient combination of alert and analyst efforts. For some institutions, this means pairing the most experienced analysts with the highest risk alerts. Depending on factors such as customer base or geographic exposure, this also may mean putting specific language speakers in charge of reviewing screening hits in a native or fluent tongue. Workflow efficiency is accomplished through the identification of, creation of a scorecard for, and assigning weight to factors such as name-match scoring, nature of the transaction, product/service line, and geographies or currencies involved, among others.

Some questions to consider when performing scorecard analysis:

1. **Are there prior alerts for this customer/name? If so, how were they dispositioned?**

   Prior positive matches may drive a higher risk rating and require more scrutiny. Similarly, many prior false positives for the same alert content usually indicate a lower level of effort may be needed to disposition — and an analytical model which may require further tuning/honing.

2. **Does the type of alert make sense?**

   For example, if an entity hits against a watchlist entry for a person, or vice versa, this is usually indicative of a low-quality alert, which implies a low level of effort to disposition.

3. **What geographies are involved in this alert?**

   Payments involving higher-risk jurisdictions or consisting of more complex payment flows through multiple countries require a higher level of effort.

4. **What was the system-generated match score for this alert?**

   An alert with a score indicating proximity to an exact match is likely to require escalation anyway, so putting it in the most experienced hands will provide the most thorough and efficient work product.

5. **In what language is the watchlist-matched entity?**

   A benefit of putting certain language or alphabet-based hits in the hands of native language speakers is cultivating a more nuanced understanding of any local language documentation, negative news, etc., as well as a familiarity with characters which may become ambiguous after translation.

Where Do We Go From Here?

Supporting a robust and risk-based sanctions program with the use of emerging technology and further leveraging advanced analytics require an ever-evolving effort. Analytics and technology must be deployed as proactively as possible in order to stay on the forefront. Simply put, considering the ever-morphing regulatory landscape and level of scrutiny, an institution's increasingly complex products, services and customer relationships require building out stronger sanctions detection competencies in order to combat advancing technology used for obfuscation, non-compliance and evasion.

Analytics and technology must be deployed as proactively as possible in order to stay on the forefront.

Investment in the right tools, personnel and upskilling will help streamline sanctions workflows, optimize sanctions detection systems, augment risk insight generation, and soundly compile the requisite data for end-to-end sanctions compliance. As such, it is incumbent upon compliance stakeholders to seek out such opportunities for technological enhancement, no matter the size, geography/jurisdiction or business of the institution.

About the Authors

Edwin Oloo is an associate director in Protiviti's Risk and Compliance practice, specializing in regulatory compliance and advanced data analytics. He has over 10 years of experience building multivariable statistical and machine learning models in the areas of financial crime compliance, anti-money laundering, counter-terrorist financing, eDiscovery, customer risk-rating analysis, risk assessment, fraud, alert risk-scoring, forensics investigations and process automation. He is adept with data privacy laws and building machine learning applications adhering to GDPR requirements. Oloo delivers consulting and advisory services through a quantitative perspective, implementing project management best practices and advanced technical insights while identifying opportunities to integrate data-science solutions.

Thomas Dessalet is a senior manager in Protiviti's Risk and Compliance practice focused on providing advanced data science and modeling solutions. Based in Philadelphia, he has more than 10 years of experience with model development, risk management and data analytics covering anti-money laundering, financial crimes compliance, sanctions detection, risk rating, credit and AI/ML models. Prior to re-joining Protiviti, he served as the head of compliance model development at Oppenheimer & Co., responsible for end-to-end oversight of transaction monitoring, KYC customer risk rating and sanctions screening models. Dessalet is a contributor to and recurring panelist in Protiviti's Financial Crimes Compliance Roundtable series, specializing in technology and industry trends.

About Protiviti's Financial Crime practice

Protiviti's Financial Crime practice specializes in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of anti-money laundering/combating the financing of terrorism and sanctions risk assessment, control enhancements, and change capability to deliver effective operational risk and compliance frameworks. Our team of specialists assists organizations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.