IdentityMind GLOBAL

IdentityMind

SANCTIONS SCREENING

WHITE PAPER

PRECISION
SANCTIONS SCREENING

www.IdentityMindGlobal.com

Introduction

Sanctions screening is a compliance requirement for institutions to:

1) Assess whether they are forbidden from working with potential clients and partners (e.g. Office Foreign Asset Control – OFAC – in the U.S.), and
2) Assess higher risk clients that require enhanced due diligence and reporting (e.g. Politically Exposed Persons - PEP - Internationally or Domestically).

Regulated institutions must compare clients' data (potential and existing) against lists of people, countries, and business entities typically provided by domestic and international regulatory bodies to confirm whether a client's data is on one of these lists.

Operational Challenges

Sanctions screening creates a significant operational burden. Institutions are required to screen every client against various Sanctions Lists, periodically retest all clients, and more importantly, investigate each hit or match. **We have seen as many as 10% of total transactions flagged for evaluation as a potential sanctions match.**

In our experience, clients deal with very high rates of false positives, usually above 90%. Putting these numbers in perspective, with a 10% flag rate, a financial institution reviewing 10,000 clients' applications per month would have (on average) 1,000 matches against various sanction lists, and in all likelihood, maybe 1 real match. Assuming an average analyst reviews 20-40 matches per day, this would require the institution to have 1.5 analysts per month dedicated exclusively to sanctions screening, and nearly all of this effort would be "wasted" time. Unfortunately, as many of these institutions would admit, it's a cost of doing business. In the end, sanctions screening is much less expensive than dealing with actual monetary sanctions, or even criminal charges.

This illustrates two fundamental problems that exist with this process:

1. High rates of false positives

The large majority of matching algorithms are based on some form of fuzzy logic, with a threshold level setting to tune the matching. Most matching relies on names. This approach by itself will never work efficiently, irrespective of algorithm tuning, because it is designed to match more often than not, which causes the false positive problem. Most organizations are left to manage a big queue for manual investigation and decisioning. A large part of the operational hassle is how to weed out false positives in an automated manner.`

2. Time required to investigate a match

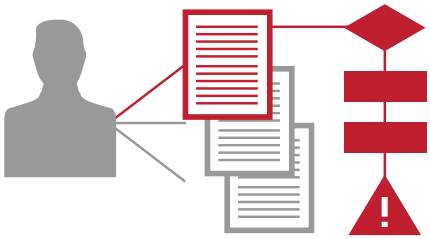
In general, there are two types of sanctions screening providers: those who provide screening integrated with KYC services, and those who provide a stand-alone service not integrated with either KYC or transaction monitoring. The former usually suffers from poor matching tuning algorithms and lack of automated false positive reduction; the latter suffer from a lack of contextual information outside the transaction, which leaves compliance investigators dealing with disparate systems, and non-real time operations. In either case, analysts spend too much time trying to discern whether the match they are dealing with is real, when it usually is not. The added peril is that with so many false positives, the analyst is actually more likely to miss genuine matches. In our interviews with clients, most complained about the lack of sufficient information available within the alert itself, and the inability to quickly decide the authenticity of a match.

IdentityMind Sanctions Screening

The key part of any solution is to make sure there are no false negatives - where entities should be flagged, but are not. Obviously, an optimal system will match ONLY when it needs to match. As mentioned before, the wider the net, the higher the likelihood for false positives. **The most fundamental part of a solution is to achieve an operational balance that enables strong detection, while minimizing false positives.**

Matching

The key matching features of IdentityMind's sanctions screening service incorporate public sanctions lists, proprietary lists such as PEP, eDNA™ - our own proprietary database, and the Weave™ database, along with the relevant matching algorithms and techniques.



Sanctions Lists

Most sanctions lists are publically available (e.g. OFAC SDN, OSFI). Others, like the PEP list are also required, but left for providers to develop. There are guidelines as to how these lists should be created and updated; PEP in particular is a bit tricky, as it requires highlighting business associations which are difficult to establish and update. At IdentityMind, we've created and maintain our own PEP list using open-source intelligence.

IdentityMind GLOBAL

IDENTITYMIND SANCTIONS SCREENING

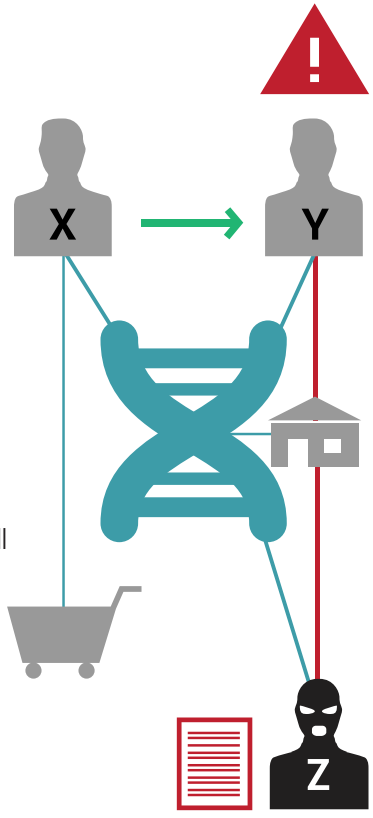
IdentityMind's sanctions screening enables users to choose among the most important public data sources including:

- Arms Export Control Act (AECA) Debarred List
- Bureau of Industry and Security
  - — Denied Persons List
  - — Entity List
  - — Unverified List
- Chiefs of State and Cabinet Members of Foreign Governments
- Consolidated List of Persons, Groups, and Entities Subject to E.U. Financial Sanctions (EU Freeze List)
- Consolidated UNSC Sanctions Lists
- Department of State Designated Terrorist Organizations
- Department of State Terrorist Exclusion List (TEL)
- FBI Most Wanted Terrorists
- Foreign Consular Offices in the US
- Immigration and Customs Enforcement Most Wanted Fugitives
- Interpol Recently Wanted
- Japan Foreign End Users of Concern
- Naval Criminal Investigative Service — Wanted Fugitives
- Nonproliferation Sanctions
- Non-SDN Iranian Sanctions Act List (NS-ISA)
- Office of the Superintendent of Financial Institutions' Anti Terrorism Financing List
- Office of Foreign Assets Control
  - — Foreign Sanctions Evaders List (OFAC FSE)
  - — Specially Designated Nationals List (OFAC SDN)
- Palestinian Legislative Council (PLC) List
- Royal Canadian Mounted Police
  - — Wanted
- Sectoral Sanctions Identifications (SSI) List
- The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
- U.S. Drug Enforcement Administration
  - — Major International Fugitives
- U.S. Marshals Service
  - — Major Fugitives Cases
  - — Top 15 Most Wanted
  - — Most Wanted
- U.S. Secret Service
  - — Most Wanted
- US Department of State Diplomatic List
- Our own Political Exposed Persons (PEP) list.

All lists are updated continuously, and additional public lists are added as necessary. IdentityMind has a team of analysts ensuring all lists are up-to-date.

The eDNA™ Proprietary Database

The eDNA™ database is unique to IdentityMind. eDNA™ contains descriptions of users, businesses, and their relationships to other users and businesses, built over time from digital transactions across the financial ecosystem. These entities (users and businesses) achieve reputations representative of their aggregated behavior through authoritative sources, heuristics, and the lenses of the clients that recorded and evaluated their transactions.



Users and business entities are described based on a set of collected attributes using cryptographic representations of physical addresses, emails, phone numbers, payment instruments, date of birth, devices, articles of incorporation address, principals, ultimate beneficiaries, and more.

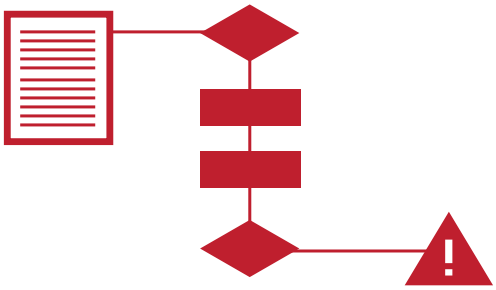
The eDNA™ database is then used to extend the matching of sanctions to all recorded users and businesses.

For example, if User X is transferring money to User Y, a normal sanctions screening procedure would check User X and User Y. With eDNA,™ if User Y's address is associated with User Z, who is a principal of a company on the OFAC list, eDNA™ will alert you to the match within our network of connections.

WEAVE™: The Next Generation of Sanctions Screening

IdentityMind has secured exclusive access to an extensive database of threat finance organizations and actors, including terror financiers, state sanctions evaders, arms proliferators, and narcotraffickers. These organizations and actors are effectively blacklisted under the scope of OFAC, but do not currently exist in any commercially available lists. This database expands OFAC designations by upwards of 55%, with tiered risk thresholds. The WEAVE™ database is the product of a highly skilled data discovery firm who utilizes open source intelligence techniques to exploit global public record systems. This data is permissible in court, able to be shared across legal jurisdictions, and is easy to parallel construct on the client side. Weave is currently under deployment with an expected delivery date of Q1 2016.

Algorithms



IdentityMind matching algorithms currently include exact matching, fuzzy matching, nicknames, aliases, and shortened names.

Additional algorithms for string distance analysis, transliteration and phonetic matching are in the roadmap with an expected delivery date of Q1 2016.

Reducing False Positives

IdentityMind provides several automated mechanisms to disambiguate a match and reduce the operational burden it can create.

1. **Comparing to list data attributes.** Our system compares against address, city, country, social security number, and date of birth when there is additional data in the list.
2. **Comparing to eDNA™.** IdentityMind compares against known relationships within the eDNA™ database to reduce the likelihood of false positives based on matching data associations.
3. **Rule system.** Clients can develop their own rules for filtering results by developing rules that can automatically rule out matches.
4. **Risk integrated rules.** Clients can combine additional risk conditions with analysis to highlight or downplay the matching attributes.
5. **Specific lists.** Our system allows users to be screened against specific lists based on location, risk profile, or other factors. These lists are configurable for each client.

Expediting the investigative process

1. Matching is part of the KYC and transaction process. The results of the matching process are presented with all the transactions performed by the user- be it the onboarding application, past transactions, analysis, or other. Context and visibility into past actions speeds the analysis process.

2. Learning from history. Clients can inform the system such that matched attributes previously evaluated and accepted during the review process are leveraged automatically.

3. Matches provide as much information as contained in the list itself, or in additional proprietary annotations. This enables faster confirmation that the individual is, or is not on the list.

4. Our intuitive user interface enables analysts to quickly research the match through all IdentityMind data and technology partners in the context of the analysis. Our full case management support ensures all investigation notes can be recorded and are easily accessible.

Additional Features

Continuous Monitoring

To comply with regulations, clients are required to perform sanctions screening on a periodic basis - guidelines state every 90 days. Our system can be configured to automatically check clients against sanctions screening and would only report if a new match occurs - one that was not previously investigated and ruled out as a false positive.

Case Management

The IdentityMind platform offers a sophisticated case management system to track analysts' investigation. Our case management system records and reports all activities, including results of the KYC Process, historical transactions, third party data, notes and evidence files, to enable business logic and integrated reporting for auditors and regulators. The case management system is also integrated with Suspicious Activity Report filing, providing full lifecycle capabilities to financial crime analysts and compliance operations.

IdentityMind GLOBAL

IDENTITYMIND SANCTIONS SCREENING

Case Study: KYC eBanking

A top 50 U.S. financial institution providing aggregated bill pay, and taking on approximately 10,000 new accounts per month, was receiving problematic results with a third party sanctions screening provider. This vendor produced a match rate of 2.3% against their sanctions lists, resulting in a false positive rate of 99% and wasted manual efforts- estimated at 20-30 minutes per match (adding up to a cumulative average of 30-40 hours per month).

The Case

Previous Vendor

Their vendor matched against name, but ignored address, date of birth, country, and other vital parameters, and offered no visibility into any information, including the name of the matched list. There were no options for the client to reduce the number of lists the information was evaluated against, and the vendor's fuzzy matching algorithms were "too fuzzy," resulting in high rates of false positives.

IdentityMind™

IdentityMind™ sanction screening produced a match rate of 0.1%, reducing false positives by 95% and minimizing manual review efforts to approximately 5 hours per month. The key factor was matching IdentityMind's eDNA™ against the lists, as opposed to single parameters.

Match Rate with Sanctions List

2.3%

0.1%

False Positives

99.9%

95% Reduction

Time Spent on Manual Review

30-40 hours per month

5 hours per month

Share

www.IdentityMindGlobal.com

Our system matches against a combination of name, address, date of birth, country, and other parameters, reducing the need for fuzzy algorithms that produce too much "noise." IdentityMind only matches against required lists, further reducing false positives, and following a match, clients are provided with contextual information to quickly assess whether they are prohibited from working with the individual or entity, and especially, PEP. IdentityMind further provides data on the context of the identity's reputation and past associations, giving our clients a unique dimension to expedite assessment.

Conclusions

The IdentityMind platform provides a comprehensive solution to address regulatory requirements associated with sanctions screening, but importantly, we've also reduced the operational burden created by it. IdentityMind expands current matching techniques by adding our own eDNA™ proprietary database of proven associations between users and businesses, and deep OFAC associations with the Weave™ database. We've applied sophisticated techniques for disambiguation and reduction of false positives, including integrating historical, risk, and entity link analysis. Furthermore, our platform provides the operational tools to expedite the review process, and the ability to record and report for regulators.

The net result is fewer and more accurate matches. The IdentityMind platform enables clients to go beyond the existing sanctions lists, and provide far greater protection against potential nefarious users and businesses trying to hide between webs and layers of connections and relationships.

Streamline your sanctions screening program,
and reduce false positives.
Contact us today at evangelist@identitymind.com.