ARTICLE

Name Screening in Financial Institutions:

Trends, Challenges and Opportunities

With increasing complexities in global business operations, the threat of Money Laundering (ML) and Terrorist Financing (TF) continues to grow significantly. Risk professionals and regulators across the globe have taken cognisance of these financial crime related risks and adopted various measures to enhance mitigating controls in the more challenging compliance environment.

Sanctions and name screening are key components of any Financial Crime Compliance (FCC) programme, the complexity of which is largely driven by its coverage and applicability. It is important to note that, globally, regulators view name and transaction screening with the highest level of scrutiny — investigating and penalising lapses identified in sanctions-related compliance breaches.

Fundamentally, financial institutions (FIs) are scrutinised with two aspects in consideration:
a. They are not engaging with sanctioned countries/ entities/individuals
b. They have an adequate framework and suitable operational mechanism to detect high risk individuals/ entities

FIs are, therefore, putting significant efforts in to developing and implementing a robust governance framework within their name screening programs. A key aspect remains to cover elements from a people, process and technology perspective to ensure adherence with compliance requirements. The fundamental challenge faced by FIs is the volume of alerts generated for such screening matches, with a false positive ratio of over 99%. This, along with other typical challenges, contributes significantly to the overall problem statement of effectively managing the screening program:

Key Trends and Challenges

1. Evolving scope & definition of screening

What started primarily as screening against specific UN sanctions lists has now widened significantly to incorporate l review of databases from multiple entities, regulators and regions. The concept has evolved considerably from simply managing "sanctioned" entities / regions / individuals to tracking "high risk" circumstances.

Hence, the term "Name screening" or "Identity & Transaction Screening" has effectively replaced "Sanctions Screening". Name screening incorporates screening against sanctions lists, politically exposed persons (PEPs), adverse media and local/internal blacklist databases. Further, it is now applicable not just to customers but also to employees, vendors and third parties.

This continuous evolution has resulted in organisations having to consider implications and complexities at multiple levels directly impacting day-to-day operations and overall due-diligence oriented processes applicable for all third parties.

2. Ineffective screening and monitoring programmes

Growing business volumes and geographical expansion are resulting in newer compliance considerations for FIs. This gives rise, for example, to a need to: a) review a wider range of business processes, b) manage multi-jurisdiction compliance requirements, and c) maintain consistency in the overall screening monitoring programme. Additionally, building effective controls to manage the risks of potentially dealing with blacklisted or high-risk customers such as PEPs is also a critical focus area within FIs.

In recent times, global FIs have invited considerable penalties on account of inefficiencies within their screening and monitoring programmes, despite allocating significant budgets – both in terms of technology and human capital allocation towards these programmes.

3. Inadequate governance and oversight

Governance and oversight is one of the foremost attributes of a name screening and monitoring programme within FIs. Regulators expect FIs to ensure that adequate governance and oversight mechanism is in place as a part of overall FCC programme. It is also important that the FIs understand and assess the risk model and Risk Based Approach (RBA) while developing governance and oversight structures to ensure they are aligned with RBA adopted by FIs.

Effective governance and oversight may help FIs in decision-making on what and how to screen without compromising on the expected results. A lack of comprehensive governance and oversight, however, may lead to an ineffective name screening and monitoring program. It should not be underestimated that designing, developing and implementing adequate risk-based governance and oversight structures complementing to RBA is difficult for FIs.

4. Inability to adopt an effective screening model

The effectiveness of a screening process largely depends on the nature of the model on which it is based, and the strength of algorithms used. FIs are moving from rudimentary name-based screening models to rule-based screening models that facilitate optimised results. While building these models, it is important for FIs to appreciate that a *'one-size-fits-all'* principle does not necessarily apply to this subject. The designing and building of a customised screening model depend on a multitude of factors such as the availability of requisite data attributes, quality of data available and finding a suitable matching logic/algorithm.

Building and implementing an effective rules-based screening model necessitates a detailed evaluation of risk factors, such as customer type, segment, products, geography, etc. vis-à-vis the screening model.

5. Data quality and list management issues

A key consideration in the name screening process is the potential consolidation of data points from multiple, disparate sources. Further, each of these varied data sources is likely to have a unique data structure and architecture. Factors such as data quality, consistency and accuracy are also pertinent in obtaining accurate results, particularly where legacy systems are involved.

FIs are gradually appreciating that a successful name screening programme warrants identification and remediation of data quality issues – from a retrospective and prospective standpoint – which, in itself, is a complex activity, involving significant effort.

Another key aspect of the screening process is the maintenance of the watchlists that are released by various sources such as government bodies, domestic/global law enforcement agencies and regulators. In addition, specific watchlists such as PEP lists and internal blacklists are also leveraged by FIs. One of the more dynamic upgrades to

the name screening process is the inclusion of a 'whitelist', which is a repository of the reviewed and verified customers maintained by the FIs in order to reduce the number of false positive alerts by applying filters to bypass screening hits.

An important point to note here is that these lists are amended on a regular basis by their respective issuing authorities, and most FIs are typically challenged with managing not only these ad hoc list updates, but also the consolidation of data points from across disparate sources to perform screening.

6. Over-screening, limited identity information and weak aliases

Large FIs operate across jurisdictions and are governed not only by domestic regulations, but also by group-level procedures and cross-geographical guidelines. This invariably results in over-screening because domestic requirements (in the context of geographies, products and customer segments) are often overlaid by group-level guidelines. Such FIs, therefore, end up performing screening not only per domestic regulations, but also per group guidelines, which may result in further complexities.

Another aspect that adds to the overall complexity is that many of the screening watchlist records contain weak aliases for which minimal information is available. This makes them onerous to establish the identity of such records.

7. Data privacy and country level complexities

In certain countries there are strict data privacy laws and country-level complexities in maintaining and sharing customer information and watchlist data issued by the local regulators such as Hong Kong Monetary Authority (HKMA) has Personal data (Privacy) Ordinance (Cap.486) ("PDPO").[1] Data maintained in different systems and servers with varying levels of security makes it further difficult for FIs to manage, assess, review and investigate end-to-end data security matters and potentially lead to violation of data privacy laws.

Opportunities and solutions

Even as FIs continue to face multiple challenges in ensuring effectiveness of their screening and monitoring programmes, it is now more important than ever to explore the solutions and opportunities available to them. Some of the key opportunities are listed below.

1. Risk-based governance framework

It is essential for FIs to develop and update comprehensive policies and procedures that provide detailed definitions around screening requirements, particularly in context of the following fundamentals:

- Why screen
- Whom to screen
- When to screen
- What to screen against and at what frequency
- Where to screen (systems) to address the core risk factors and regulatory requirements.

Adoption of a risk based approach (RBA) will go a long way in supporting FIs with developing an effective name screening programme. Further, having comprehensive standard operating procedures (SOPs) that exhibit detailed alert disposition/investigation methodologies including regular and exceptional scenarios such as non-availability of adequate information and information availability from potentially unverified sources.

2. Leveraging suitable technology enablers

Several regulators including HKMA have encouraged FIs to leverage technologies like robotic process automation (RPA) and machine learning (ML) to transform the AML processes. Another example of regulators promoting tech-based innovation is the Insurance Regulatory and Development Authority of India (IRDAI), that has designed a "Regulatory Sandbox" to encourage innovation, particularly in the area of leveraging fin-tech solutions.

There are a number of use cases for leveraging

[1] https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf

technologies like AI and ML to improve efficiencies within the name screening process – particularly in the reduction of false positives, pattern-based disposition of alerts and leveraging induced ML capabilities to tune the name screening model/process.

FIs should note that these technology-enabled tools are not a matter of "plug and play" and do require customisation based on factors such as business operations, availability of data sets and regulatory expectation.

3. Match exclusion (ME) approach

FIs should consider adopting ME approach to generate quality alerts. ME approach is designed based on certain combinations of data attributes and matching logic to reduce false positives and enhance the effectiveness of the monitoring process. FIs spend a significant time on data collection and aggregation of information while reviewing screening results to arrive at a false positive conclusion. The ME approach enables elimination of false positives based on data attributes available in source system and watchlist.

The ME approach should be designed after careful consideration of all the associated risk factors in eliminating the generation of potential false positives.

Different screening approaches can be adopted for forward screening and for reverse screening based on the regulatory expectations and group requirements.

4. Ongoing testing and evaluation of screening system

FIs should design independent risk-based testing programmes to test the effectiveness of the screening process and systems. Testing is required to ensure that screening system is behaving or performing as per expectations and quality alerts are getting generated. This kind of result-oriented testing also enables FIs to take decisions on fine-tuning the screening model. Testing should be performed on a regular interval by a risk and functional specialist.

Conclusion

Balancing the dual aims of reducing cost of compliance and at the same time, ensuring effective compliance is more critical & complex than ever before.

With the surge in regulatory requirements and extent of databases to be screened, FIs need to consider adopting a strong risk-based governance model and couple that with an astute eye on efficiency and optimisation, which in turn, will largely be dependent on

- Dynamic fine-tuning of the screening model through AI and advanced analytics
- Robust evidence-based alert review mechanism through use of advanced workflows and automation
- Improvement in quality of data

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

ASHWIN KUMAR
Managing Director
Risk Advisory & Investigations - Financial Services
ashwin.kumar@fticonsulting.com

VINAY SINGH
Director
Risk Advisory & Investigations - Financial Services
vinay.singh@fticonsulting.com