WHITE PAPER

ANTI-MONEY LAUNDERING (AML) NAME SCREENING — KEY CHALLENGES AND SOLUTIONS

Abstract

Money laundering continues to remain a huge concern for the global financial system. Resultantly, financial institutions (FIs) have been focusing on strengthening their anti-money laundering (AML) capabilities.

Name screening is a key activity within the AML process — it is performed by FIs in several stages of their AML workflow. Name screening is also a regulatory AML requirement under several jurisdictions. Unfortunately, FIs face several challenges in effectively executing their AML name screening processes. Firms therefore need to adopt new-age screening solutions and strengthen their related screening processes, practices, and capabilities. This whitepaper shares insights on the key challenges faced by FIs in their AML name screening process. Further, it offers actionable solutions to overcome these challenges.

Infosys®
Navigate your next

Introduction

It's said that money laundering is the oxygen for organized crime. As per the UNODC, each year, the value of money laundered globally constitute 2 - 5% of the global GDP (which amounts to USD 800 billion – USD 2 trillion in absolute terms).[1] Refer below an illustration of a typical money laundering scheme.

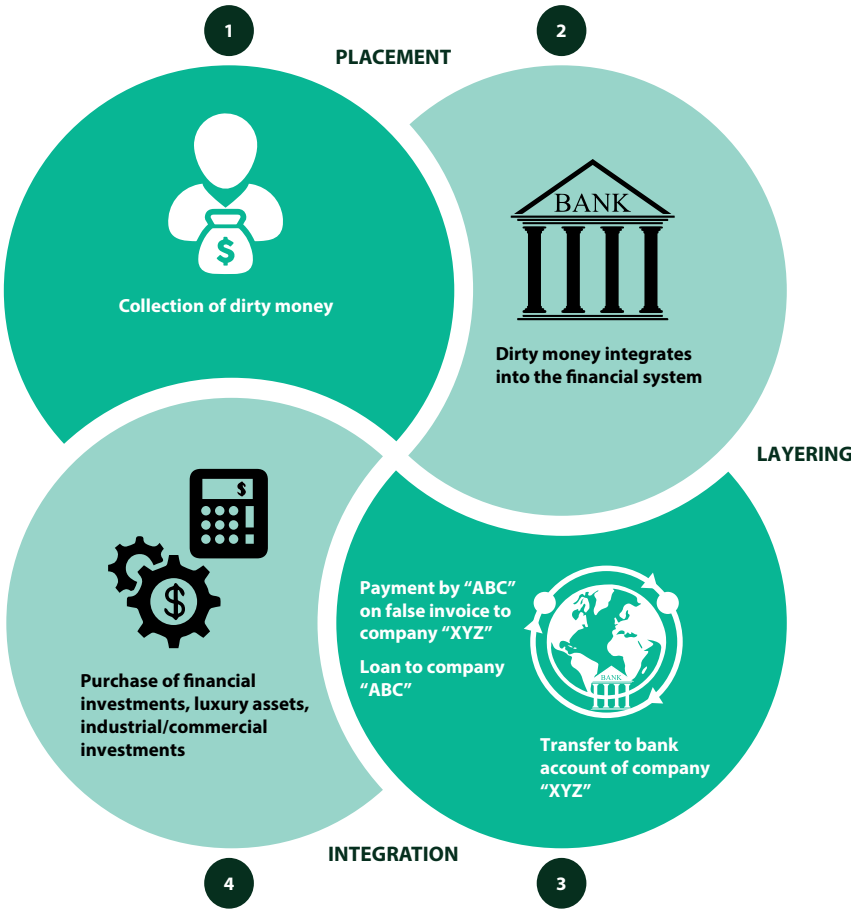

Figure 1: Typical Money Laundering Scheme

AML Name Screening

Name screening is a key activity in the AML process. It is utilized by FIs to assess the AML-related risks of their existing or potential customers. It involves screening the customer's names against sanctions, PEP, watchlist and internal blacklist databases, and against the adverse media and negative news. Refer below examples of AML name screening databases.

◆ UN sanctions lists
◆ OFAC's SDN List
◆ HM Treasury List
◆ Enhanced Sanctioned Countries List
◆ European Union Designated Terrorists Consolidated List
◆ EU Consolidated Sanctions List & EU Most Wanted Warnings
◆ US DOJ (FBI, DEA, US Marshals, and others)
◆ FBI — Hijack Suspects List; Most-Wanted List; Most-Wanted Terrorists List; Seeking Information List
◆ State Department Foreign Terrorist Organizations List and Non-Proliferation List
◆ State Department Terrorist Exclusion List
◆ World Bank Listing of Ineligible Firms and Individuals (WBNK)
◆ OCC Unauthorized Banks List
◆ FINCEN Money Laundering Concerns List
◆ Australia Consolidated List (AUCL)
◆ US – Bureau of Industry and Security List
◆ Third-party commercial screening databases (e.g., Dow Jones Factiva, Refinitiv World-Check, Accuity)
◆ Other federal, state, and international watchlists
◆ News sites for adverse media screening

Figure 2: Examples of Name Screening Databases

Name screening is performed by FIs in several stages of their AML workflow — including new customer onboarding; account opening; KYC, CDD, EDD procedures; UBO checks; KYC refresh; and payment processing. Name screening is also a regulatory AML requirement under several jurisdictions. Today, the scope of name screening has expanded beyond customers to include employees, counterparties, vendors and third parties.

AML Name Screening: Key Challenges

Refer below some of the key challenges faced by FIs vis-à-vis AML name screening.

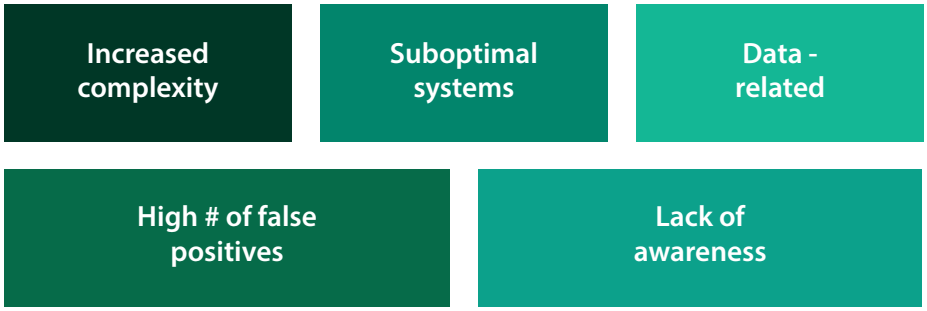

Figure 3: Key Challenges Faced by FIs in AML Name Screening

1) Increased complexity: Today, the sanctions and other screening databases have become highly dynamic in nature. They are constantly evolving — people get added and removed to the lists daily. Moreover, with the increased globalization and cross-border businesses, the number of sanctioning bodies and screening databases have also multiplied.

Also, unlike in the past, when sanctions were levied mostly against organizations or states, today the sanctions' scope has increased manifold and includes a myriad of industry sectors and categories of individuals. To add to the complexity, AML screening-related regulatory obligations continue to constantly evolve across jurisdictions. This has significantly raised the risks of non-compliance for FIs.

2) Suboptimal systems: FIs legacy rules-based screening systems lack optimal automation and effectiveness. For example, these systems utilize static lists of known spelling variations of names. They are unable to track minor data anomalies or name-related nuances — such as common misspellings, name variants, salutations, titles, abbreviations, order of names, etc. They fail to effectively account for the prevalent usage of alternative names and aliases. Also, these systems are unable to deal with the diversity of naming conventions across cultures and languages — such as contractions (e.g., F'lar, O'Sullivan), usage of non-Latin characters (e.g., Jesse-James), etc.

Many existing solutions lack robust language translation and transliteration capabilities — this creates challenges in screening against non-English databases. Moreover, many existing screening systems don't support unstructured data capabilities. As a result, FIs face challenges with matching names in different scripts and languages, in enabling simplified watchlists, and in performing automated monitoring of negative news on social and news media. Several FIs have also mindlessly adopted vendor-provided screening solutions without customizing them for their specific needs.

Today, AML teams need to spend a substantial amount of manual effort — like gathering and scanning data across various internal and external systems — to execute the screening process. For several global FIs, screening constitutes over 20% of their AML-KYC technology program spend.[2]

3) Data-related: Effective name matching is highly dependent upon the completeness, accuracy and consistency of the screening-related data in an FI's internal databases.

Alas, several FIs struggle on this key aspect. Firms also lack optimal integration with the relevant internal and external data sources. The official screening databases (e.g., sanctions lists) don't follow consistent formats. Many of these lists don't provide all required data attributes (e.g., date of birth information). Additionaly, these lists get updated at different frequencies and suffer from several data quality issues. Such internal and external data-related challenges severely impact an FI's name screening efficiency and effectiveness.

4) High number of false positives: FIs' legacy rule-based systems follow a simple deterministic name matching approach. These systems fail to consider name-related nuances and the additional secondary identifiers. Resultantly, they generate very high number of false positives. As an example, these system may block payments to a person living in Kerman, California due to incorrect application of the rule set for city of Kerman in Iran.

For many FIs, over 99% of false positives alerts are generated by their screening engines.[3] Firms end up spending substantial time, effort and money in investigating the false positives.

5) Lack of awareness: Several FIs' AML and other concerned screening teams lack thorough understanding of the regulatory expectations and obligations across the regions that the firm operates in. Also, staff lack good understanding of, and therefore unable to optimally leverage, the reputed lists of relevant government-supplied and commerical screening databases.

AML Name Screening: Solution Recommendations

Some key recommendations for FIs to overcome their main AML name screening-related challenges are given below:

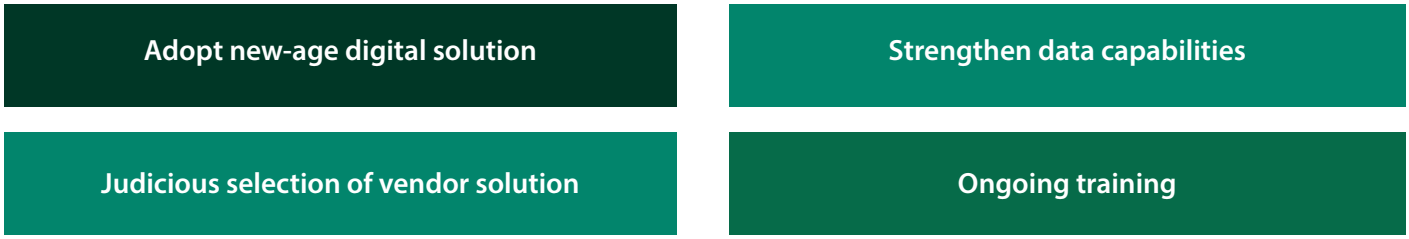

Figure 4: AML Name Screening — Key Solution Recommendations

1) Adopt new-age digital solution: FIs should adopt advanced screening solutions having new-age digital capabilities such as advanced analytics, sentiment analytics, AI, ML, deep learning, RPA, graph database, NLP, and NLG. Illustrative screening-related capabilities offered by these new-age solutions are outlined below.

◆ Intelligent risk-based screening — accounts for transliteration errors, phonetic misunderstanding, misspelling, and orthographic (capitalization, hyphenation, punctuation, word breaks etc.) and phonological (sound pattern across languages) variations
◆ Sophisticated and accurate name matching — using advanced matching techniques such as fuzzy matching (e.g., Levenshtein distance), Beider-Morse phonetic matching, concatenated name matching, synonym matching, dependency parsing, co-reference resolution etc. (Note: Fuzzy matching, for example, would help accurately screen even in cases where there are slight alterations to name, aliases, birthdays, location, etc.)
◆ High-volume and real-time screening and adverse media monitoring — against wide variety of structured and unstructured global data sources in multiple languages and scripts (including lists provided by government agencies, regulatory bodies, industry-leading third parties, custom lists, news sites, and social media)
◆ Sophisticated alert ranking and scoring — to aid alert prioritization (Note: The score indicates the level of confidence on how closely a name matches against the screened databases.)
◆ Dynamic finetuning of screening models through self-learning and usage of alert investigation feedback — this results in substantial reduction of false positives and false negatives
◆ Advanced reporting (on alert volumes, false positives ratio, analyst productivity, SARs filed, etc.) and dynamic dashboards (that support intelligent data visualization and easy referencing)
◆ Intelligent workflow automation using cognitive RPA, ML, NLP, and NLG capabilities — e.g., on maintenance of internal lists, alert routing, alert and case enrichment, auto or low-touch closure of low-risk alerts, case management workflow, etc.

Figure 5: Illustrative System Capabilities of new-age Digital AML Name Screening Solutions

2) Strengthen data capabilities: For effective AML screening, it is important that all required information — on customers; accounts; UBOs, directors and other key stakeholders (for corporate client), etc. — are accurately updated and are accessible in the FI's internal systems (KYC, CRM etc.). Staff must take care to ensure data accuracy and completeness while entering such information — during customer onboarding, CDD, EDD, KYC refresh, etc.

Firms must also work on enabling robust integration of all relevant internal data sources to ensure automated and timely data availability.

FIs should also focus on their screening-related data enrichment. For example, strengthening the customer profiles by using additional secondary identifiers such as aliases, date and city of birth, passport information, driving license information, data on any membership or affiliation with political party, corporate identification data, etc. Enriched data using additional secondary identifiers would help significantly reduce the false positives.

Further, FIs must ensure that they are leveraging optimal number of reputed and relevant screening databases, including those provided by government agencies, regulatory bodies, industry-leading third parties, and other adverse media sources.

3) Judicious selection of vendor solution: When FIs decide to adopt vendor solutions for AML screening, they should carefully consider the below key aspects.

◆ The vendor and solution's capabilities and credentials — in terms of maturity; performance and scalability; scope and breadth of coverage (channels, products, etc. supported); integration capability (with the FI's other relavant AML and FCRM solutions), UX aspects (of reports and dashboards, availability of self-help and customization tools, etc.); ongoing service and support, etc.
◆ The solution's alignment with the firm's specific screening needs
◆ Ability and flexibility of the vendor to customize their solution as per the FI's specific needs
◆ The list of external databases and sources leveraged for screening

Figure 6: Key Considerations While Selecting A Vendor Solution for AML Name Screening

4) Ongoing training: FIs should invest on ongoing training and orientation of their AML and other staff involved in the screening process. The aim should be to ensure that all concerned employees are fully aware of the relevant screening-related databases; the firm's policies, processes, and systems; key regulatory obligations; and screening best-practices.

Real-world examples of the new-age AML name screening solutions

Entity	Elaboration
Nice Actimize[4, 5]	◆ Its WL-X next-generation watchlist screening solution leverages AI and biometrics capabilities — for enabling a) advanced real-time and on-demand screening against global PEPs, sanctions, adverse media, and other lists; b) superior data management; and c) frictionless customer onboarding ◆ The solution offers best-in-class screening using advanced facial biometrics, intelligent ISO20022-compliant payment parsing, and advanced culture/name matching technology ◆ In addition to several key government-provided lists, the solution also aggregates and orchestrates list data from public and premium sources to enable comprehensive screening
BAE Systems[6]	◆ Its flagship NetReveal Transaction Filtering solution leverages Match Exclusion — a sophisticated algorithm engine that utilizes a combination of rules and algorithms to identify suspicious transactions ◆ The engine has helped reduce the number of false positives by 40-60%
ZA Bank[7]	◆ ZA Bank — Hong Kong's first virtual bank — has adopted Accuity's suite of Firco screening solutions (including Firco Trust, Firco Continuity, and Firco Global WatchList). These solutions enable automated alert detection, false positives reduction, and high-risk alerts prioritization, and have helped the bank gain balance between ensuring robust risk management and enabling exceptional customer experiences ◆ Firco Trust — which is supported by unique filtering technology — can screen millions of customers during onboarding. Similarly, Firco Continuity can screen millions of transactions to enable fast settlement ◆ The solution's filtering technology can account for common variations in name typologies or structures — in English, simplified and traditional Chinese characters, and several other languages
Jumio[8]	◆ Its Jumio Screening solution leverages ComplyAdvantage's automated watchlist, sanctions, PEPs and adverse media monitoring and screening capabilities ◆ The solution leverages AI, ML, and computer vision technologies to screen and authenticate in seconds

Conclusion

AML name screening plays a key role in combating money laundering. FIs therefore need to adopt new-age technology screening solutions and strengthen their screening-related processes, data management capabilities, and the collaboration between concerned teams. Focus should be on ensuring effective risk-based screening, at reduced cost, and without compromising the user experience.

Glossary of terms

Acronym	Expansion
AI	Artificial Intelligence
AML	Anti-Money Laundering
AUCL	Australia Consolidated List
CDD	Customer Due Diligence
CRM	Customer Relationship Management
DEA	Drug Enforcement Administration
EDD	Enhanced Due Diligence
EU	European Union
FBI	Federal Bureau of Investigation
FCRM	Financial Crime Risk Management

Acronym	Expansion
FI	Financial Institution
FINCEN	Financial Crimes Enforcement Network
HM	Her Majesty's
KYC	Know Your Customer
ML	Machine Learning
NLG	Natural Language Generation
NLP	Natural Language Processing
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control

Acronym	Expansion
PEP	Politically Exposed Person
RPA	Robotic Process Automation
SDN	Specially Designated Nationals
UBO	Ultimate Beneficial Owner
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US DOJ	United States Department of Justice
UX	User Experience
WBNK	World Bank Listing of Ineligible Firms and Individuals

About the Authors

Anjani Kumar

Principal Consultant, Risk and Regulatory Tech Practices, Financial Services Domain Consulting Group, Infosys Limited

Anjani has over 20 years of comprehensive IT, domain, and process consulting experience. Currently, he manages and supports several strategic programs including Competency Development, Research, Thought Leadership, and Solution Enablement. He is an accomplished thought leader and has large number of whitepapers and point of views published on reputed external websites.

Prashanth Hande

Principal Consultant, Regulatory Tech Practice, Financial Services Domain Consulting Group, Infosys Limited

Prashanth is a seasoned professional, with 28+ years in IT, particularly in BFSI domain. He has rich experience in leading large transformational projects in core banking and in implementing programs in the risk and compliance domain — including broker compliance and anti-money laundering using Actimize and Oracle FCCM.

Shivashis Patri

Senior Associate Consultant, Regulatory Tech Practice, Financial Services Domain Consulting Group, Infosys Limited

Shivashis has over 6 years of experience ranging from requirement gathering for product functionalities to implementing solutions in risk and compliance domain for financial institutions. He has strong domain knowledge in the areas of anti-money laundering, fraud management, enterprise case management, and regulatory reporting.

References

1. United Nations — Office on Drugs and Crime
2. WL-X: Risk Screening with Precision, niceactimize.com
3. If screening engines present 99% false positives, how can we fix sanctions compliance?, ey.com
4. Nice Actimize applies AI to watchlist screening, Feb 11, 2021, finextra.com
5. WL-X: Risk Screening with Precision, niceactimize.com
6. BAE Systems improves AML screening algorithm, Oct 15, 2018, finextra.com
7. Hong Kong virtual bank Za implements Accuity screening tech, Sep 17, 2020, finextra.com
8. Jumio Unveils Automated AML Screening Solution, David Penn, Mar 19, 2019, finovate.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next