RegTech and IWT

Anti-money laundering (AML) and combating the financing of terrorism (CFT) have been key areas of RegTech development in recent years. Financial institutions (FIs) today use technologies such as transaction monitoring, sanction screening, adverse media screening and KYC systems to help detect and identify potential IWT activity and links.

The importance of technology in addressing IWT risks was underlined by the financial sector professionals surveyed by Themis as part of this IWT research, with 82% of respondents pointing out the effectiveness of transaction monitoring, 66% citing adverse media searches and 56% highlighting sanctions lists. The overwhelming majority of respondents (96%) also said they welcomed further guidance on how to detect potential links to the IWT, including with regard to relevant RegTech systems and tools.

By understanding a FIs risks following a rigorous company-wide Risk Assessment, the appropriate technology can be selected for each specific use case with different options listed in the Toolkit.

Solutions with advanced data analytics categorisation such as Big Data, Natural Language Processing, Artificial Intelligence and Machine Learning allow FI's to accelerate investigations and find linkages in accounts to criminal networks and organised crime that may have remained hidden when manual processes were relied upon.

Broader, strategic adoption of these forms of technologies and integration into financial crime compliance programs will enable more targeted, intelligence-driven capabilities which will result in a higher number of effective STR submissions by FIs to the relevant authorities.

Due to the complexity of IWT, its inextricable links to large scale criminal organisations and serious crime syndicates and the continuous evolution of red flag typologies, the need for these forms of technologies to help detect and report suspicious activity associated with IWT continues to grow.

This guide provides further recommendations and case studies on:

1. Configuring detection logic in existing technologies
2. Considering the implementation of new RegTech solutions to combat IWT

Configuring Detection Logic in Existing Technologies

This section discusses specific use cases that illustrate how a bank's existing RegTech solutions can increase both the efficiency and the effectiveness of efforts to combat IWT.

Use Case 1: Auditing and Testing of Existing AML/CFT Systems

Financial Institutions should first ensure that they have the correct AML/CFT technologies in place to detect IWT indicators. This should include a robust sanction screening system which is set up to alert against names on globally important sanction lists and tuned to flag sanctioned names even when they have been altered using algorithms to assess the fuzzy logic matching capabilities of a screening system.

Algorithmic manipulation will stress test a screening system and make it harder for a system to identify and alert against sanction records. The system should also be capable of alerting against key words associated with IWT as part of a bank's transaction screening process.

Sanction screening systems should be tested regularly to ensure that they are working as expected and that the number of false positives generated by the system is manageable and does not overwhelm available resources.

As part of a system audit, FIs should ensure that their sanction list data is updated frequently as changes to globally important sanction lists often happen on a daily basis. The same applies to adverse media sources as this data should be used for up-to-the-minute KYC, CDD and EDD checks to mitigate all AML/CFT risks – including those associated specifically with IWT.

In terms of transaction monitoring technologies, such systems should provide a bank with an entire picture of a customer's financial activity. It should cover risk levels and predict future activity within an ascertained customer risk profile, alerting when a transaction takes place that falls outside of this defined risk profile.

Transaction monitoring system testing and validation of IWT rules will highlight any inaccuracies and will identify incorrect threshold parameters that can cause a transaction monitoring system to produce unnecessary alerts or miss specific IWT behavioural-type transactions.

Use Case 2: Tuning and Optimisation of Existing AML/CFT Systems

Sanction screening system testing will help a bank to understand a system's configuration whilst determining its weaknesses within pre-defined detection parameters. Testing will facilitate improvement and enhancement of system performance through ongoing iterative tuning to optimise the efficiency and effectiveness of a sanction screening system. This will impact positivity on a bank's capability to detect keywords that are known to be associated with IWT.

Transaction monitoring system testing and validation will identify vulnerabilities in a transaction monitoring system's alerting capabilities. It will provide the intelligence required by a bank's team of system technicians to understand their existing IWT red flag assumptions and to then carry out remediation and post-testing enhancement activities to rid the system of time-wasting inaccuracies.

Tuning the system will allow analysts to identify transactional patterns and behaviours consistent with known IWT typologies more easily, allowing teams to work more efficiently and to submit a higher number of quality STRs to the authorities.

Use Case 3: Ongoing Monitoring of AML/CFT System Efficiency and Effectiveness

The final step involves the continued, ongoing monitoring of sanction screening and transaction monitoring system efficiency and effectiveness. All AML/CFT technologies should be monitored on an ongoing basis to ensure that they remain correctly calibrated and that the number of false positives generated the system remains at a manageable level.

A highly tuned AML/CFT system that is fit-for-purpose leads to relevant and valid IWT alerts without the interference of excess system noise caused by numerous irrelevant false positives.

Implement New RegTech Solutions to Combat IWT

Outside of updating current systems to ensure they detect IWT typologies adequately and accurately, the uptake and usage of new technologies to help combat specific IWT risks will be beneficial. In their implementation of a risk-based approach, some FIs will need to implement further technologies to tighten controls and ensure detection of potential IWT risks.

Listed below are a range of specific use cases of new RegTech that are currently in practice today to combat IWT:

Use Case 4: Enhanced Customer Risk Profiling
RegTech Category: Machine Learning (ML)

Adoption of additional ML models to overlay existing technologies can enrich the capability of transaction monitoring systems to identify suspicious transactions by enhancing defined customer risk profiles. ML can assist with the adjustment of behavioural profiling system settings that operate in real-time and can help spot anomalies in a bank account which would otherwise remain undetectable. ML models can be tailored specifically to detect IWT indicators.

Use Case 5: Detection of IWT Red Flags Associated with TBML
RegTech Category: Maritime AI

Regulatory risk can be associated with all aspects of a trade transaction, including the buyer, seller, city, region, port, goods and vessels involved in the shipping process of goods.

Trade-based money laundering (TBML) continues to be a significant area of focus for IWT traffickers and profiteers to hide illicit goods and launder funds. New AI technologies, targeted specifically for the marine industry, enable the tracking of shipments and shipping activity to monitor potential smuggling routes, cargoes and the actual weight of cargos compared to the description provided on shipping documents.

Use Case 6: Managing and Reporting Data More Effectively
RegTech Category: Governance Risk and Compliance (GRC) Reporting Platforms

Most prevalent in recent years has been the increased usage of GRC platforms to automate a bank's reporting obligations, particularly through the submission of STR's. These systems automate and enhance transparency in the reporting of information through to regulatory bodies and, in some circumstances, to public-private partnerships (PPPs).

Tailored to specific illicit activities and money laundering typologies, such as IWT, GRC platforms can draw together various data feeds to build a comprehensive and accurate report in real time.

The Importance of Technology

Technology continues to be the driving force for change within many organisations. This of course applies to ground-breaking RegTech solutions that can be targeted specifically to disrupt IWT. In order to power such innovation, relevant, accurate and clean data must first be accessible to banks, and then understood so that valuable insights can be derived and used to enable better decision making to mitigate financial crime risk.

PPPs

Public-Private Partnerships (PPPs) are also an important aspect of the fight against IWT in which the industry is moving toward with support from numerous government bodies. Globally there is a groundswell of support from the compliance industry to enable the transfer of information with regard to illicit financial activity; IWT is a large aspect of this due to the global nature of supply chains and financial flows.

PPPs incorporating NGOs, governments, and the private sector are critical where information is readily available to facilitate an industry-wide approach to de-banking and facilitating the prevention of illicit money flows to help advance the global fight against IWT. This is work in progress and one in which all banks and other financial institutions have a key role to play.

This guide is brought to you in partnership with: