Trade-Based Money Laundering
A Comprehensive Approach to Combat TBML
Table of Contents

Introduction to Trade Finance – The Basics 2
Introduction to TBML – The Basics 2
Key Challenges in Enforcing a TBML Program 3
Setting an Appropriate TBML Program Covering the Entire Spectrum of Risks Involved 5

TBML Controls and Specific Solution Requirements 7
  Review KYC / CDD Profile through Complete Deal Underwriting 7
  Name and Payment Screening 8
  AML Transaction Monitoring 9

The Use of Data Analytics to Identify TBML 9

The Evolution of TBML Monitoring in Banks 10
**Introduction to Trade Finance – The Basics**

**Trade Finance** is the financing for trade activity in both domestic and international markets. A **trade transaction** requires a seller of goods and services as well as a buyer. Various intermediaries such as banks and other financial institutions can facilitate these transactions by financing the trade.

Trade Finance includes activities such as lending, issuing letters of credit, factoring, export credit and insurance. Companies involved with trade finance include importers and exporters, banks and financiers, insurers and export credit agencies, and other service providers such as tax agents, lawyers, trade mediators, etc. Certain forms of trade finance were specifically crafted to supplement traditional financing.

Repayment terms relating to trade finance activities are generally short-term, with the majority being used solely for the completion of a particular business transaction. When used for legitimate purposes, this financing option forms a safety net, helping to protect the interests of buyers and sellers in the international marketplace and assisting in the completion of transactions that may involve multiple currencies, geographies and parties.

When used by the wrong people, however, Trade Finance can be one of the most effective and dangerous methods for money laundering and international movement of illicit funds.

**Trade-based money laundering** (further referred to as “TBML”) is the process by which criminals use a legitimate trade to disguise their criminal proceeds from unscrupulous sources. The crime involves a number of schemes in order to complicate the documentation of legitimate trade transactions; such actions may include moving illicit goods, falsifying documents, misrepresenting financial transactions, and under- or over-invoicing the value of goods. The strategy report of the International Narcotics Control Board shows that through TBML schemes, criminals launder hundreds of billions of dollars annually. Additionally, the US Department of Treasury, in its National Anti-Money Laundering Risk Assessment, stated that TBML can have a more destructive impact on legitimate commerce than any other form of money laundering activity.

**Introduction to TBML – The Basics**

TBML has become a widely used term, covering a broad spectrum of services and products, including those referred to as Trade Finance. In reality, the majority of international trade is carried out under “Open Account” terms, under which, unless the financial institution is providing credit facilities, the financial institution’s involvement will be limited to the actual payment – money transfer, and it will not generally be aware of the underlying reason for the payment. In such a case, the financial institution does not have the ability to execute anything other than the standard AML Transaction Monitoring and Sanctions Screening on the final payment that was sent (such as the case with a “Funnel Account”). However, in the case where the financial institution provides any sort of ‘Credit Facilities’ in relation to the trade, there are several other opportunities to better understand the business rationale, the risk involved, and the movements of funds.
Trade Finance is a document-centric process involving numerous contracts, product descriptions, brochures, bids, shipping manifests, invoices, etc. In some cases, the terms and conditions, as well as side agreements, may not be documented in writing or disclosed to the bank. Due to this fact and using existing technology, the process is heavily dependent on human review and manual screening, and highly reliant on the experience of the individual banker.

In its right form, the TBML program should include complete deal underwriting as part of the KYC and CDD effort, proper screening of all parties involved, the detection of suspicious transactonal activity across current and deposit accounts, and finally payment screening for sanctions. We will further discuss best practices and the proper implementation of each of these contact points later in this paper.

Indeed, banks are the central clearinghouse for all financial transactions pertaining to Trade Finance. They have access to the complete documentation and profiles of their customers, and are therefore best placed to govern Trade Finance activities. Thus, it is no surprise that regulators and other law enforcement agencies have shifted their focus to banks in an effort to clamp down on TBML. However, regardless of how good the banks are positioned to tackle TBML, the multitude of challenges they face may sometimes debilitate the effort or even dissuade the entire process.

Trade Finance is a document-centric process (involving numerous contracts, product descriptions, brochures, bids, shipping manifests, invoices, etc.) and in some cases the terms and conditions, as well as side agreements (which may be essential to understand the true nature of the business transaction), may not be documented in writing or disclosed to the bank. Due to this fact and using existing technology, the process is dependent heavily on human review and manual screening, and highly reliant on the experience of individual bank personnel. Furthermore, creating an organizational capability to conduct impartial and consistent manual review, and implementing decision-making standards across a team of analysts is a well-known challenge that requires significant investment in complex training and monitoring.

Taking into consideration the aforementioned challenges, coupled with the fact that digitalization of scanned documents and running analytics on unstructured data (such as bill of lading, SWIFT MT7XX messages, etc.) remains a challenge to many financial institutions, the inherent difficulties of automated monitoring are obvious.

Key Challenges in Enforcing a TBML Program

As introduced above, there are several significant challenges in implementing and maintaining a resilient TBML program, with scope spanning geography, data protection, and data availability to name a few. Below are several key challenges and the possible approaches financial institutions may consider while crafting their own strategy.

» Data Protection is one of the most significant challenges faced by financial institutions managing a TBML program. Data protection rules and cross border exchange of information restrict the ability of financial institutions, as parties to a trade transaction, from accessing required KYC/CDD information when completing the appropriate due diligence process on the parties involved, beyond those entities and individuals who are direct customers of the bank. This challenge will have an impact to the TBML program on all levels, from KYC/CDD to transaction monitoring through to sanctions screening and beyond.

» Global bodies have yet to set agreed standards for the appropriate levels of KYC and CDD. In practice, each financial institution will need to comply with differing local jurisdictional standards, which in some countries are known to be less stringent than in others. Such differences can lead to issues with respect to reliance on 3rd parties to conduct appropriate due diligence on their customers. Furthermore, it is important to recognize that different financial institutions,
especially those located in developing countries, are at different levels of maturity as far their AML controls, deployed solutions and banking operations (variations in the level of sophistication of systems, internal processes and training can be extreme, even within the same country in the industrial world). It is recommended that an assessment be made when reviewing Trade Finance documentation and underwriting contracts as the level of KYC, sanction screening and AML transaction monitoring employed by counterparty financial institutions may not be in-line with the organizational standards or the level required by the local regulator.

» The application of Sanctions screening and the lists used in different jurisdictions, which may create disparate or conflicting legal obligations for financial institutions, may present challenges relating to specific transactions and the assessments of a Customer or a Non-Customer relationship the bank is maintaining.

» The identification of potentially Dual Use Goods, such as software, technology, documents, manuals and diagrams, which may have both civil and military applications, is challenging given their natural complexity and technical nature. While financial institutions may use specific lists to identify obvious Dual Use Goods products (such as chemicals, fertilizers, metal pipes etc.) their ability to recognize a multitude of other items, that may have dangerous applications, remains questionable.

» Commodity price verification is difficult as financial institutions are typically not in a position to make appropriate or meaningful judgement of the validity of stated unit pricing due to the lack of relevant information such as the terms of specific business relationship, discounting for bulk purchase, quality of goods involved in specific transaction, non-publicly traded products, etc.

» The identification of attempts to overcome Trade restrictions and Sanctions. There are many methods used by criminals and sanctioned parties (individuals, organizations, and countries) to hide the ultimate user of a product, either through the use of intermediaries or by masking the actual application or the intended use of the product (such as concrete and metal rods to build bunkers in conflict areas rather than housing). These are all very much applicable to the monitoring of TBML. Financial institutions must pay greater attention and exercise diligence when underwriting trade finance engagements involving multiple (and unjustified) parties or involving jurisdictions in close proximity or associated with low AML enforcement regions, countries in armed conflict, or sanctioned countries. The main challenge financial institutions are facing is the lack of available information to identify “transfer of ownership” and the “disguise of the true nature of a transaction.” However, appropriate red flags must be raised to systematically highlight any apparent discrepancy.

Ongoing AML Training – expanding current practices beyond compliance team members and initiating training of Risk Managers, transaction processing, as well as other front and middle office staff engaged in regular business operations. Such training should cover subjects such as AML awareness, standard operating model, step-by-step guidance on how to perform analysis of commodity pricing, how to identify unusual unit pricing, identification of goods that may have both civil and military applications, as well as the escalation path that should be initiated once the slightest doubt has been raised.

To summarize, there are several key factors that contribute to the inherent risks of TBML that pose key challenges to the ability of financial institutions to monitor such risks. These include:

» Involvement of a high number of parties on either sides of the trade
» Possible collusion between buyers and sellers
3 LAYERS OF DEFENSE

» Business Operations
Day-to-day operations must ensure that an appropriate risk and control environment is established.

» Oversight
Effective oversight functions must set clear boundaries by drafting and implementing adequate policies and procedures.

» Internal Audit
This function is an essential factor for the success of any program as the audit role is to provide independent, objective assurance for the program.

> The document-centric nature of TBML, more so than with any other banking facilities
> The absence of reliable sources of information to verify transactions (such as commodity price lists, people who were denied export licenses, etc.)
> Reliance on third parties in identifying key players in the transaction, the use of shell corporations, offshore companies or representative offices is shady locations, etc.

Setting an Appropriate TBML Program Covering the Entire Spectrum of Risks Involved

When designing appropriate measures to counter TBML risks, banks must consider that just as for many other complex financial crime schemes, a consolidated, sophisticated detection system functioning in tandem with a backbone of layered controls and processes is required to ensure success.

All lines of defense accessing same data, regardless of it’s use (AML Transaction Monitoring, KYC/CDD, FATCA, Fraud) = greater consistency, easy to audit etc.

It is recommended that banks follow a “3 layers of defense approach” that encompasses business operations, oversight, and audit controls, to appropriately cover a multitude of TBML risks.

» Business Operations: Day-to-day operations must ensure that an appropriate risk and control environment is established, including an array of tools deployed across programs, processes and people. Line management should be adequately skilled to create risk definitions and perform on-going risk assessments.

» Oversight: Effective oversight functions must set clear boundaries by drafting and implementing adequate policies and procedures, as well as, ensuring such policies and procedures are followed and executed. Escalations from operational functions will be handled at this level and a mechanism to manage quality with a system of random quality assurance checks must be put into place.

» Internal Audit: This function is an essential factor for the success of any program as the audit role is to provide independent, objective assurance for the implementation of the program as a whole by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
When attempting to implement an appropriate TBML program, banks should deploy a combination of the above, ensuring that system coverage as well as processes, procedures, oversight and auditing are each put into place. As illustrated below, only a holistic TBML program can appropriately tackle the multitude of challenges involved in money laundering through Trade Finance, providing an appropriate control over the bank’s risk.

For the application of an appropriate AML program covering the main TBML risks, banks can leverage their existing AML investment (if an appropriate one already exists) to add the key capabilities required to cover specific areas and controls as required. At each stage, the decision to refer or continue and the rationale needs to be recorded and kept on file.

Details of key areas required can be found below:
TBML Controls and Specific Solution Requirements

This section will cover the specific controls and system capabilities deemed essential to cover basic TBML requirements considering most relevant regulations. Record keeping is a key mandatory requirement; financial institutions must retain evidence relating to any decision taken and/or any escalation process while processing any transaction. All records must be made available for review post transaction completion.

It is recommended that financial institutions conduct risk based quality assurance reviews to determine, within a reasonable timeframe, that the customer KYC file is valid and current as well as that previous transactions had been appropriately evaluated and managed.

Financial institutions are required to demonstrate that they have robust control and review processes, that internal procedures are in place, that alert management flows are maintained, and that appropriate escalation processes are in place and being used when appropriate. All approvals of exceptional conditions and acceptance of high-risk customers must be retained by the financial institution.

Review KYC / CDD Profile through Complete Deal Underwriting

The Know Your Customer and Customer Due Diligence process has a significant influence on a financial institution’s ability to prevent money laundering. Due to the known challenges of TBML prevention, deal complexity, relationship between parties, and the availability of data, the biggest and probably most impactful element of any prevention effort is the appropriate due diligence and full deal underwriting of a trade related financial product. To appropriately comply with new TBML regulatory requirements, financial institutions are expected to enhance deal underwriting efforts when higher risk circumstances are recognized.

Financial institutions are expected to leverage a risk-based approach in the on-boarding process and the retention of customers by adhering to best practices of CDD reviews for trade account customers and to have a true and complete understanding of the business model, the counterparties, the countries where the different entities are operating from and the goods or services that are exchanged, as well as the expected annual transaction volumes and money flows.

Depending on the financial institution’s procedures and calculated risk, Enhanced Due Diligence (EDD) may be required where the countries, products, or customers involved are deemed to be posing higher risk, or where high risk financial products are sold.

Also, financial institutions are expected to conduct a full EDD process whenever previous reviews have discovered that the goods sold are of high risk or of a dual use nature.

As in any appropriate KYC/CDD process, it is expected that a loop-back mechanism is made available to trigger a re-evaluation process in any case where transactions or other trigger events reveal new information on the nature of a relationship or the accuracy of the data available.
Once a trigger event occurs, the financial institution is expected to initiate a full KYC/CDD re-evaluation of the customer to ensure that their Customer Risk Profile is accurate and current. The results of such a review process may vary from simply confirming that the information on file is valid and no change is required, to an adverse finding that leads to a change in the Customer (or related party) Risk Profile and escalation to a higher level for deliberation on next steps. Next steps may include the imposition of controls on account/s, limitations on transactions or, in severe circumstances, exiting the relationship.

Name and Payment Screening

The requirement to screen customers against a wide variety of lists has been followed by financial institutions globally for the past several years through the implementation of a name matching mechanism of some sort. The matching capabilities of a specific system and its accuracy depend heavily on the matching logic, technique used, and quality of available data.

Financial institutions must be cautious when conducting customer and payment screening as the matching logic must be designed to screen the specific data. By screening names or payments through systems that were not built for that specific purpose, e.g. screening payment transactions (i.e., MT103 or MT700 messages) for Sanctions or Dual Use Goods with a matching algorithm that was built for the purpose of name matching (i.e., culture-based matching), the results are likely to be insufficient, generate a high level of false positives and more severely, fail to detect sanctioned entities.

Financial institutions are expected to screen both direct customers (the client of the processing bank) as well as to screen ALL relevant entities including related parties (directors, signatories, guarantors, etc.), counterparties (such as suppliers, tax agents, lawyers etc.), vessels, ports, products purchased and others. Furthermore, payment transaction screening is expected to be carried out against sanctioned countries, ports, customers, entities, accounts as well as Dual Use Goods, etc.

The ability to screen multiple parties needs to be in place to ensure that the transactions do not violate UN or applicable global and local sanctions against named individuals, legal entities and countries.

Financial institutions are expected to retain records to prove that all relevant entities were screened, indicating any finding (or lack thereof). Financial institutions are expected to properly evaluate any potential matches found and record the evaluation process for audit purposes.

In the case of a positive match, a feedback mechanism is expected to be used to notify the KYC system and trigger a review process as discussed in the previous section.
AML Transaction Monitoring

From a transaction monitoring perspective, financial institutions are expected to evaluate both payments and financing transactions, either through automated or through manual process, against a list of scenarios to identify suspicious activity or highlight any unusual patterns and anomalies against customer specific historical activity.

Regulators are expecting financial institutions to monitor transactions across a variety of channels, banking services and product types (including trade products) as well as payment transactions made to or from current and deposit accounts. Detection of money flow and suspicious transactions in “Funnel Accounts” requires the use of a comprehensive set of detection scenarios as well as advanced profiling capabilities to identify anomalies.

Below are sample typologies used in the detection of TBML:

» Frequent amendments to letters of credit
» Excessive defaults on trade finance guarantees
» Trade finance activity involving high risk destinations
» Trade structure is unnecessarily complex
» Trade in high risk goods
» Traded goods details discrepancies

Below is a sample set of typologies used for the detection of suspicious money laundering activity across “Funnel Accounts”:

» Payment structuring
» Flow through funds
» Burst in payment activity
» Rapid movement of funds
» Activity involving high risk geographies
» Change in behavior patterns

The Use of Data Analytics to Identify TBML

Financial institutions have been leveraging a range of traditional analytical techniques to identify potential money laundering activities. These existing techniques can be applied to monitor TBML specific typologies and Funnel Accounts:

» Rules Engines: These are used to execute algorithms built as business rules to check volume, velocity, and variance in transactions. Such business rules can also be executed in-line with more advanced modeling techniques such as customer profiling, account profiling, peer comparison, and text analysis to detect behavioral anomalies.

» Profile and Trend Analysis: These statistical tools can be used to accumulate transaction data into a predictive profile, established to serve as the baseline behavior of a customer and/or accounts, truncating historical transactions and seasonal trends into a condensed, easily accessible profile to identify changes in transaction patterns, customer relationships, deviation from expected behavior and many more.
» **Sequence Mining:** A form of data mining where the system is looking for a defined sequence of events, which can indicate wrong-doing (such as the sequence described in flow through of funds typology). For the detection of TBML, such sequence analysis is expected to expand to cover new typologies and identify new sequences, i.e. multiple shipment requests from a single customer or address, etc.

» **Link Analysis:** A technique used to identify hidden relationships between seemingly unrelated parties by detecting common links in both static (reference) or transaction data.

The main issue with the above mentioned traditional AML monitoring techniques is that all were designed to work on standardized, structured and accurate data-sets, but would yield unpredictable results and alert volume when applied to the monitoring of semi-structured or unstructured data, such as the case with Trade Finance.

Some of the newer analytical techniques used in the analysis of semi-structured or unstructured datasets include:

» **Text Analytics and Text Mining:** This method involves the use of natural language processing combined with statistical and machine learning techniques to model and structure information from textual sources to derive high quality information.

» **Big Data Analytics:** Big Data is usually characterized by one or more of the following: high volume, high velocity, or high variety data. Given that Trade Finance data comes from a variety of internal and external sources in multiple formats, and given the unstructured format of that data, big data analytics brings versatility to the data consumption process.

» **Enhancing Reference Databases:** Gaining access to a library of industries, products, channels, vessel names, dual use goods, high-risk countries, ports, etc. will bring greater accuracy to monitoring and efficiency to analysis of the money laundering activity. These lists can be bought from external list consolidators and can also be managed internally by leveraging advanced tools to enhance data availability and versatility.

» **Advanced Statistical Analytics:** A process of quantitatively describing the main features in a dataset, which can, through mathematical models, be compared against global or regional benchmarks for congruence (or lack thereof).

» **Predictive Analytics:** Advanced statistical models can help banks anticipate possible future outcomes and the likelihood of wrongdoing based on the detection of indicative parameters or a specific pattern.

» **Web Analytics:** Web crawling software can be used to download relevant web pages matching specific search terms and criteria, (i.e. container details, negative news, etc.) to indicate TBML acts. Such techniques can also be used to gather social media data to be later used for the purpose of link-analysis and the detection of networks and related parties.

» **Image Analytics:** Converting hardcopy documents to consumable formats to reduce the effort of gathering and structuring data.

The Evolution of TBML Monitoring in Banks

While the benefits of an automated and fully integrated TBML monitoring system are overwhelming, it may be too ambitious a goal for banks to dive straight into it, especially if multiple legacy systems and complex data management processes are involved.
Financial institutions are encouraged to take incremental steps towards automation, through progressive enhancement of each of the key areas discussed in this article – from improving KYC and CDD processes through enhancement of screening tools, list management capabilities, the availability of data, advanced analytics, and obviously investment in training of the FI’s last line of defense – it is human capital: front and middle office employees.

For ease of discussion and to illustrate the concepts as presented in this paper, let's review different stages of readiness of different TBML programs according to the TBML Maturity Level as described in the graph below.

When a financial institution is positioned at the **Limited Phase** in the maturity spectrum of TBML programs, processes are likely to be manual, coupled with inconsistent and rudimentary screening practices. The required data will either be unavailable in electronic form or spread across multiple systems. Analytical capabilities will be limited and will consist of at most a basic rule set. For the prevention and detection of TBML anomalies, the bank will depend upon its front office personnel and document checker staff to escalate any discrepancies found.

Many banks have already recognized the benefits of automating TBML monitoring, and are implementing relevant technologies and enhancing existing processes. Such financial institutions fall into the **Core Phase** of the maturity spectrum, these banks have achieved a certain degree of automation and established pre-transaction underwriting and screening processes. They are still partially dependent on manual document checking, and analytical capabilities can be further enhanced once data availability has been improved, but importantly they are performing well and have introduced basic controls into place.

Banks in the **Enhanced Phase** of the maturity spectrum have implemented full automation of their TBML processes and are running pre-approval review, screening and post-transaction monitoring for a more comprehensive process throughout the trade finance lifecycle. While trade finance data is more enriched, these financial institutions are still accessing data across different silos. Banks at this stage will have put in place a
specialized TBML prevention team capable of running diagnostic analytics on available data.

A financial institution can consider itself at the **Leading Phase** of the maturity spectrum only when it has completed trade finance related data consolidation within its financial crimes data-mart across the enterprise, allowing it to run predictive analytics capabilities and screening both pre and post-transaction as well as across the entire trade finance lifecycle. The different systems used for TBML and AML monitoring are capable of sharing ‘trigger events’ seamlessly.

Finally, banks at this maturity level have a specialized TBML team in place, able to appropriately review any exception report generated and truly understand the business reasoning behind business agreements and import/export engagements. A bank at this stage has successfully optimized the balance between people, processes, and technology.

No matter which phase the financial institution is in, countering TBML risks with a consolidated and sophisticated detection system is the key to success. Predictive analysis and machine learning are no longer ‘techniques of the future’ – innovative institutions are implementing these techniques today to stay ahead of the competition... and the criminals.