Elevating TBML Risk Management: from window dressing to data-driven approach

WRITTEN BY **LEON KORT**
LAURENT CLAASSEN

Money laundering is a critical global issue as it facilitates the flow of illicit funds derived from criminal activities. By disguising the origins of these proceeds, money laundering allows criminals to enjoy the benefits of their illegal activities without detection. This undermines the integrity of financial systems, erodes public trust in financial institutions, and can distort economic development by channelling resources into unproductive or harmful areas. Furthermore, money laundering poses significant challenges to law enforcement and regulatory bodies, as the complexity and cross-border nature of these transactions often hinder detection and prosecution efforts. Addressing money laundering is therefore essential to maintaining the stability and security of financial systems worldwide.

Trade-Based Money Laundering (hereinafter: 'TBML') is high on the agenda of supervisors and financial institutions. TBML refers to *the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origin*[1]. As one of the most sophisticated forms of money laundering, TBML exploits the complexity of international trade and the high volume of trade flows, making detection and prevention a significant challenge for both authorities and financial institutions. This way, criminals can use TBML to finance a range of illegal activities such as tax crimes, drug trafficking, arms smuggling and environmental crimes[2]. This is often done by moving value across borders by:

- **Over-Invoicin**g: A company exports goods or services for a price higher than their actual value. The importer then pays the inflated invoice amount, effectively moving excess value to the exporter, which can be laundered funds.

- **Under-Invoicing:** Goods or services are exported at a price lower than their actual value. The importer pays the reduced amount, and the difference is settled through illicit funds, thus transferring value to the importer.

- **Multiple Invoicing:** A single shipment of goods is invoiced multiple times to justify multiple payments. This creates a mechanism to transfer illicit funds under the guise of legitimate trade transactions.

- **Over- and Under-shipments:** The quantity of goods shipped is misrepresented on documents. For example, shipping fewer goods than invoiced (under-shipment) allows the importer to justify the transfer of excess money. Conversely, over-shipment involves sending more goods than invoiced, allowing the importer to receive excess value without proper documentation.

[1] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html
[2] Article 2 of the 6th Anti-Money Laundering Directive (AMLD6) provides a list of 22 predicate offenses that constitute money laundering.

- **Phantom Shipping:** No goods are actually shipped, but documentation is created to show a trade transaction took place. This can justify the transfer of funds internationally without any legitimate business activity.

- **Misrepresentation of Goods:** The quality or type of goods is misrepresented. For example, lower-quality goods are invoiced at the price of higher-quality goods, facilitating the transfer of excess value;

- **Round-Tripping:** Goods are exported and then re-imported, often with multiple steps and involving different countries. Each step creates an opportunity to alter the value or quantity of goods, thereby moving illegal funds through complex trade routes.

- **Third Party Payments:** Engaging unrelated third parties to make payments on behalf of the parties involved in the trade transaction. This adds another layer of complexity and makes it more difficult to trace the flow of funds;

- **Use of shell companies and front companies:** Creating or utilizing companies that have no substantial business activities to conduct fictitious trade transactions. These companies often exist only on paper and are used to facilitate the movement of illegal funds.

Regulatory Framework for TBML

The regulatory framework for TBML is designed to prevent, detect, and combat the illicit flow of funds through trade transactions. This framework is primarily shaped by international standards set by the Financial Action Task Force (FATF[3]), which provides comprehensive guidelines for countries to develop robust anti-money laundering (AML) and counter-terrorist financing (CTF) measures. The FATF recommendations emphasize the importance of risk-based approaches, enhanced due diligence, and strong reporting requirements. National regulators, such as the Financial Crimes Enforcement Network (FinCEN) in the United States, the Financial Conduct Authority (FCA) in the United Kingdom and the Dutch Central Bank (DNB) in The Netherlands, enforce these standards through specific regulations and guidelines tailored to their respective jurisdictions. These include requirements for financial institutions to implement effective customer due diligence (CDD), know your customer (KYC) procedures, and continuous monitoring of trade transactions.

Additionally, international cooperation and information sharing among regulatory bodies, financial institutions, and law enforcement agencies are crucial components of the TBML regulatory framework, ensuring a coordinated and comprehensive response to the evolving threats posed by TBML. An important example is the

[3] FATF is the global money laundering and terrorist financing watchdog. The intern-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring out national legislative and regulatory reforms in these areas.

collaboration between The Wolfsberg Group[4], International Chamber of Commerce (ICC)[5] and Bankers Association for Finance and Trade (BAFT[6]) who collectively developed Trade Finance Principles[7], outlining the standards for the control of financial crime risks (FCRs) associated with Trade Finance activities.

Upcoming AML/CTF regulations like the Anti-Money Laundering Regulation (AMLR[8]) and the 6th Anti-Money Laundering Directive (AMLD6[9]) continue to enhance existing frameworks by introducing stricter compliance obligations, leveraging technological advancements for better monitoring and reporting. Although the final texts AMLR and the AMLD are not yet available, it appears that AMLR provides a framework for information exchange between partnerships, covering both private and public partnerships. It seems that information that may be shared within partnerships can relate to KYC information of customers and where applicable their UBOs, but also transactional data. Such information-sharing obviously must comply with GDPR requirements and therefore measures are required[10]. However, this enhanced information exchange could lead to significant opportunities to improve TBML risk management. Before we dive deeper into this, let's take a look at the role of banks and the TBML risks they are exposed to.

How are banks exposed to TBML risks?

FATF recognized TBML as one of the main methods by which organized criminal groups launder funds[11]. Globally, TBML poses a significant threat due to its ability to penetrate legitimate trade networks and exploit gaps in international regulatory frameworks. In the most recent National Risk Assessment (NRA) Money Laundering 2023[12], TBML has been defined as one of the eighteen key money laundering threats[13] for The Netherlands and therefore requires sufficient attention from financial institutions while performing their role as a gatekeeper. In this article we specifically focus on the role of banks, highlighting their critical position in detecting and preventing TBML activities.

Banks can be exposed to TBML risks either through trade finance transactions or open account trading (also referred to as 'clean payments').

[4] The Wolfsberg Group is an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks.
[5] ICC is a global business organization that promotes international trade, responsible business conduct, and a global approach to regulation through advocacy, dispute resolution services, and setting international standards.
[6] BAFT is the leading global forum for bringing the financial community, its solution providers and stakeholders together to collaborate on defining best market practices that facilitate efficient delivery of trade and cash management products and service offerings for their clients.
[7] Source: The Wolfsberg Group, ICC and the BAFT Trade Finance Principles 2019.
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420
[9] 6th Anti-Money Laundering Directive (AMLD6)
[10] Partnerships must comply with GDPR requirements and a DPIA has to be carried out before the start of a partnership. AMLR is expected to set further minimum standards for information sharing.
[11] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html
[12] https://www.tweedekamer.nl/downloads/document?id=2024D13181
[13] In the NRA on Money Laundering 2023, TBML is also referred to as money laundering through trade constructions with goods and/or services.

Trade finance is *the provision of finance and services by financial institutions for the movement of goods and services between two points, either within a country (domestic) or cross border (international)*[14]. Most common trade finance products[15] are (non-exhaustive):

- **Letter of Credit:** a document issued by a bank on buyer's behalf that guarantees payment to the seller;

- **Documentary Collections:** a payment instrument where documents are submitted through a bank for collection of payment of the importer;

- **Bank Guarantees:** A default undertaking which secures a compensation payment to a named beneficiary in case another party failed to perform a specific action (as required under the contract).

Banks are generally introduced as a third party to a trade finance transaction instead of clean payments and generic lending to provide additional protection for the commercial parties and independent and impartial comfort when parties require some level of performance and payment security or when documentation is required for other purposes e.g., to comply with Customs, other regulatory requirements, control of goods and/or possible financial institution requirements.

Clean payments are *payments made by the buyer of the goods or services direct to the seller, i.e., not requiring presentation of the supporting trade documentation to the banks through which the payment is affected*[16]. In this case, the bank is only aware of the payment and will not be aware of the reason for the payment, unless the relevant details are included in the associated SWIFT messages. As banks are not required to investigate commercial transactions outside their knowledge, they would only gain better insight into the payment if documentation they see as part of the banking transaction gives rise to suspicion.

Due to their exposure to TBML risks, many banks highlight TBML as one of their top risks within the Systematic Integrity Risk Analysis (SIRA), reflecting their willingness to get in control of their TBML risks while fulfilling an important role in facilitating trade transactions.

[14] Source: The Wolfsberg Group, ICC and the BAFT Trade Finance Principles 2019.
[15] The ICC regulates trade finance products through a series of standardized rules and guidelines, including:
- *Uniform Customs and Practice for Documentary Credits (UCP 600): Governs the use of letters of credit.*
- *Uniform Rules for Demand Guarantees (URDG 758): Provides guidelines for demand guarantees.*
- *Uniform Rules for Collections (URC 522): Sets out the rules for documentary collections.*
- *International Standby Practices (ISP 98): Offers a framework for the use of standby letters of credit.*
- *Uniform Rules for Bank Payment Obligations (URBPO): Regulates bank payment obligations.*
- *Uniform Rules for Forfaiting (URF 800): Establishes guidelines for forfaiting transactions.*

[16] https://www.nvb.nl/media/3194/aml-ctf-sanctions-guidance-part-ii.pdf

The TBML gatekeeper debate

The debate on who should be the gatekeeper in combating TBML has gained momentum, underscoring the need for a multifaceted approach. Traditionally, banks have been at the forefront due to their central role in financial (payment) transactions and their regulatory obligations to detect and report suspicious activities. However, there is growing consensus that banks alone cannot effectively counter TBML. Public and private entities, including customs authorities, shipping companies, and freight forwarders, possess unique insights and touchpoints within the trade ecosystem. Customs authorities can monitor and flag discrepancies in trade documentation and goods declarations, while shipping companies can track and report suspicious cargo movements. This collaborative approach leverages the strengths of each party, fostering a comprehensive defence mechanism against TBML and enhancing the overall integrity of global trade.

Key TBML risk indicators

TBML risk indicators are critical for identifying and mitigating illicit financial activities disguised within legitimate trade transactions. These indicators can be categorized into several areas and are not limited to:

- Customer-related indicators include industries prone to TBML, particularly those dealing with high-value or easily transportable goods, and lack of a clear business rationale.
- Third-party risks involve the presence of unexplained intermediaries, counterparties in high-risk jurisdictions, or the use of shell companies[17].
- Goods and services indicators encompass practices such as over- or under-invoicing, misrepresentation of the quality or quantity of goods, and trade in goods that are hard to value or frequently associated with fraud.
- Shipping route risks involve complex or illogical trade routes, transshipment through high-risk jurisdictions, and discrepancies in shipping documentation.
- Trade documentation risks include inconsistencies or anomalies in invoices, bills of lading, and certificates of origin.
- Account and transaction activity risks are identified through unusual account behaviours, such as large or frequent transactions inconsistent with the customer's business activities.

Monitoring these diverse risk indicators enables banks and regulatory bodies to more effectively detect and prevent TBML schemes.

[17] A shell company is a company without active business operations or significant assets. These types of companies are not all necessarily illegal, but they are sometimes used illegitimately, such as to disguise business ownership from law enforcement or the public.

Key challenges in TBML risk management

Not surprisingly, banks face sufficient challenges in identifying and managing TBML risks. TBML is one of the most common but also one of the most difficult methods of money laundering to detect. It often involves import and export of goods, for which it is difficult to determine what goods are actually loaded and discharged, whether the prices are plausible and in line with actual market prices and whether the shipping route makes commercial sense. Within the retail domain additional complexities arise because a wide variety of products are mainly shipped in containers by established container shipping companies[18]. One ship could hold thousands of containers. Therefore, the plausibility of the shipping route could be hard to assess for banks as the goods and container of the bank's client are not always linked to the countries within the shipping route.

Past estimates suggest that only 20% of world trade is conducted by means of Trade Finance products and services, the rest is conducted through clean payments[19]. This emphasizes the fact that banks have limited visibility on the legitimacy and purpose on the majority of trade transactions. Banks only have access to documents that they receive as part of a trade transaction. They do not have access to underlying goods that are actually shipped, which makes it hard to assess TBML risks of a transaction.

Furthermore, each country has its own regulations and requirements for international trade, including customs procedures, tax regulations and documentation requirements. Due to the complexity of the cross-border nature of international trade transactions, the involvement of a wide variety of counterparties and vast array of trading arrangements, TBML risk management requires an innovative and data-driven approach. In order to sufficiently assess the money laundering and terrorism financing risks of a trade transaction, sufficient trade data is required. Key TBML data points are mainly related but not limited to information on clients (e.g. information on business activities) and historical transaction behavior, goods/services that are imported/exported, prices, countries, shipping routes, counterparties, shipping companies and vessels.

Unfortunately, trade data is disaggregated. First of all, no single organization has ownership or access to all information that would assist in identifying TBML. As mentioned, banks only have access to documents that they receive as part of a trade transaction, and not the goods. Therefore, banks do not have the full picture and have insufficient insights into supply chains. Other parties in the trade chain hold relevant data that could be leveraged for TBML risk management purposes. For example, customs authorities play an important role in inspecting imported and exported goods. Global inspection rate for sea and air freight varies by region and type of cargo, but it generally remains quite low due to the vast volume of goods transported[20]. Furthermore, docks and shipment providers should have lists of

---

[18] This is different for wholesale, where commodities are shipped by bulk carriers.

[19] NVB: AML, CTF & Sanctions Guidance Part II, Chapter 9: Trade Finance

[20] On average, the inspection rate for sea freight is around 2% to 10%. This low percentage reflects the challenge of physically inspecting all shipments while maintaining the flow of global trade. For air freight, the inspection rate is slightly higher, ranging from approximately 5% to 20%, given the typically higher value and time-sensitive nature of air cargo. Sources: https://www.freightos.com/resources/global-freight-

shipments, contents and prices which could be disseminated to further analyse and help investigators. Another example relates to Lloyds List Intelligence[21] who have maritime data and therefore are able to deliver information on vessel movements and vessel ownership.

Another challenge is that the internal TBML data governance and data quality of banks requires further enhancement. Data is often scattered and stored in multiple data sources. Within a bank multiple trade and Customer Relationship Management (CRM) systems are used across international locations, which hampers national and international data exchange within the organization between trade departments, CDD analysts, account managers and the Compliance department. Furthermore, information on trade documents as part of a trade finance transaction is still often documented in an unstructured manner. For example, some banks still store trade documents as a PDF-file in the trade system, instead of extracting all relevant TBML data points and document them in structured data fields in the trade system. Having insufficient structured data available hampers the adoption of solutions to automate TBML checks and therefore often leads to inefficient and ineffective execution of TBML controls.

Despite the critical importance of combatting TBML and effectively managing trade finance products, knowledge and expertise in these areas remain insufficiently widespread within many banks. The complexity of TBML schemes poses significant challenges. Additionally, trade finance products require specialized understanding to manage and monitor effectively. However, many banks lack adequately trained staff who can navigate these intricacies, leaving gaps in the detection and prevention of fraudulent activities. The shortage of expertise not only hampers regulatory compliance but also exposes banks to significant financial and reputational risks, highlighting an urgent need for enhanced training and development programs in these critical areas.

Meanwhile, criminals leverage the weaknesses in the AML/CTF controls of banks.

Reshaping the gatekeeper role

These challenges show that there is plenty of room to further improve effectiveness of TBML risk management. The effectiveness of the AML/CTF laws and regulations is also currently subject to discussion in society. Over the past years, financial institutions heavily invested in their role as a gatekeeper[22]. In the Netherlands, 13,000 people are working in KYC/AML. Anti-money laundering costs for Dutch banks are 1.4 billion euros a year. However, of all reported signals of money laundering, 95% is false and of the half a million reports that are subsequently transferred to the Financial Intelligence Unit, less than 10% turned out to be suspicious. According to the Dutch Banking Association (NVB), the vast majority

---

outlook-november-2023/ / https://www.xeneta.com/blog/xeneta-ocean-and-air-freight-market-outlook-2023 / https://www.ti-insight.com/whitepapers/q2-2023-ocean-freight-rate-tracker/

[21] https://www.lloydslistintelligence.com/

[22] https://www.nvb.nl/publicaties/position-papers-statements/position-paper-nextgen-poortwachters/

(90%) of that suspect group were already known to the police and the judiciary. Furthermore, the current AML/CTF controls lead to unwanted side effects like de-risking and the fact that normal clients with legitim intentions increasingly experience inconveniences when arranging their bank affairs[23].

Managing TBML risks has often been likened to looking for needle in a haystack and sometimes feels like window dressing. In The Netherlands, very limited cases are known of criminals that are convicted for TBML. Although banks show their willingness to fulfil their role as a gatekeeper, they do not always understand where to look for. An important suggestion done by NVB in order to significantly improve effectiveness of AML/CTF is to apply a 'pull model' where financial information about criminal pins is extracted from banking systems based on available intelligence from public parties. Using this method could also open doors to a more effective way of combatting TBML.

Conclusion: a shift of approach how to 'fight against' TBML is needed.

Call to action: A more data-driven approach to TBML risk management

Using available intelligence from public parties as a starting point for TBML investigations could significantly enhance effectiveness. However, the complexity of trade transactions and the disaggregated character of the current TBML data landscape emphasize the need for exchange of relevant trade data between public and private parties in the trade chain.

Enhanced information-sharing could potentially create tremendous opportunities for a more effective TBML risk management. This type of data pooling can be much more cost effective than implementing new Artificial Intelligence (hereinafter: 'AI') strategies or other processes. Imagine that banks are able to exchange data with airports, ports and Customs Authorities on imported and exported goods. That vessel information, such as shipping routes, container contents, and trading partners, is shared with banks in real-time. This integration could enable banks to cross-reference transactional data with actual trade activities, identifying discrepancies indicative of TBML schemes. Furthermore, collaboration could extend to law enforcement agencies, leveraging their intelligence on criminal networks to flag suspicious TBML transactions.

Additionally, advanced data analytics, AI and machine learning algorithms could be employed to analyse large datasets from multiple sources, identifying patterns and anomalies that human analysts might miss. By creating a centralized repository of trade data accessible to all relevant parties, the entire trade chain could benefit from enhanced transparency and efficiency in detecting and preventing TBML.
Incorporating blockchain technology could further enhance data integrity and security, ensuring that shared information is tamper-proof and verifiable. This would

[23] https://www.nvb.nl/publicaties/position-papers-statements/position-paper-nextgen-poortwachters/

not only streamline compliance with AML regulations but also foster trust among public and private entities involved in the trade process.
In conclusion, the exchange of relevant trade data between public and private entities, supported by robust regulatory frameworks and advanced technologies, holds significant promise for improving TBML risk management. On the one hand this could lead to increased costs for banks due to the need for more resources to analyse the data and to conduct more thorough investigations. On the other hand, increased opportunities for automation could reduce the costs of TBML risk management. In any case, such collaboration could lead to more proactive and effective identification and mitigation of TBML risks, ultimately strengthening the integrity of the global trade system.

In order to address key challenges regarding TBML, banks could take the following actions into consideration:

- Actively focus on enhancement of the TBML data landscape by unifying the system landscape, making relevant trade data available in a structured manner to allow automation, and enhancing data by using external data suppliers (e.g., Lloyd's List Intelligence).

- Set up partnerships to facilitate the exchange of trade information between public and private parties.

- Invest in advanced analytics, AI and machine learning tools to analyse large volumes of trade and transactional data, identifying patterns and anomalies indicative of TBML.

- Implement robust data governance frameworks to ensure the quality, accuracy, and security of the data being used and shared.

- Develop comprehensive training programs for staff to improve their understanding of TBML risks and the importance of accurate data management and analysis.

- Advocate for and participate in industry-wide initiatives to standardize data formats and sharing protocols, facilitating smoother and more effective data exchanges.

- Leverage blockchain technology to enhance the transparency and traceability of trade transactions, ensuring that data shared across the network is secure and tamper-proof.

- Engage with regulators and industry bodies to stay updated on evolving AML regulations and ensure compliance with the latest standards and best practices.

How we can help

Compliance Champs is uniquely positioned to help banks enhancing their compliance risk management framework. Leveraging our TBML related knowledge and experience, our team of experts – together with our business partners - can assist banks in:

- Performing a maturity assessment on current state to identify key development areas for achieving desired TBML maturity;

- Developing and implementing TBML policies and procedures;

- Facilitating training and awareness sessions to improve TBML knowledge and expertise;
    - Participate in our online training on TBML: https://learning.compliancechamps.com/courses/trade-based-money-laundering-tbml/

- Enhancing TBML data landscape, ensuring that relevant trade data is structured and accessible for effective automation. We collaborate closely with external data suppliers to enrich banks' datasets, providing valuable insights into trade transactions and vessel movements.

Tensig helps companies stay on top of their compliance obligations and the management of compliance risks by providing user-friendly, efficient, and cost-effective compliance software solutions through the so-called ITTS Compliance Platform.

Next to straightforward Client Screening, Customer Due Diligence (KYC/CDD) and Transaction Screening the ITTS platform also supports:

- Detecting omissions in logistics, transportation, and freight, including transaction-based checks of air waybills, export controls, and dual use items;

- Customs' related business processes and IT-infrastructure, including declaration systems, existing risk engines, container scanners, ship movements, etc.

Is your organization ready to step-up their TBML Risk Management? Get in touch with our TBML experts!

CACEE

Laurent Claassen
Senior Advisor to Boards & Executives

+ 31 6 44 38 82 54

clamanco@outlook.com

www.cacee.hu

Compliance Champs

Leon Kort
Chief Operational Officer

+ 31 6 83 33 02 13

leonkort@compliancechamps.com

www.compliancechamps.com