SHADOW TRANSACTIONS: THE HIDDEN NETWORK OF TRADE BASED MONEY LAUNDERING

Shubhangi Maheshwari, LLB (2026), ILS Law College, Pune

Kunal Warade, LLB (2026), ILS Law College, Pune

ABSTRACT

Trade Based Money Laundering (TBML) constitutes a major and complex challenge in the global financial system, as illegal funds are skillfully concealed within legitimate and lawful trade transactions. This research article provides a comprehensive examination of the operational dimensions of TBML, detailing the mechanisms by which trade data is manipulated—through techniques such as invoice misrepresentation, shipment irregularities, and the fabrication of trade papers—to obscure the origin of criminal proceeds.

This article critically evaluates current monitoring practices and legal frameworks, identifying significant gaps that hinder effective detection and enforcement of TBML. One of the major focus areas of this article is the stakeholders involved in the TBML process who hinder the development and implementation of TBML Regulations. It demonstrates that conventional red flag indicators, while useful, are often not sufficient because of the intricacies of international commerce and the adaptive strategies employed by money launderers. In light of these challenges, the article advocates for the application of a strategy more focused on risk, which prioritizes the scrutiny of high-risk transactions and sectors, integrates advanced technological solutions for enhanced data analysis, and fosters improved inter-agency coordination.

By addressing the multifaceted vulnerabilities in existing regulatory structures and proposing innovative strategies for TBML detection and prevention, this article aims to contribute to a more resilient and transparent global trade environment.

Introduction

On 29 December 2023, Indian and Hong Kong Customs, through effective bilateral cooperation and information exchange, uncovered a significant case of TBML or disguised money laundering. The case implicated exporters from Hong Kong and importers based in India. The joint operation codenamed "*Gem Crusher*" exposed a syndicate that laundered HK $500 million by falsely declaring low-value synthetic diamonds as high-value natural ones.[1] Despite the magnitude of this operation, TBML proceeds to receive insufficient attention.

Almost two decades after the release of Financial Action Task Force's first advisory report[2], TBML continues to be the most advanced way to transfer "*value*" both inside and outside of countries and launder illegal monies under the pretence of legal business dealings. TBML was originally described by the Financial Action Task Force (FATF) in 2006 as "*the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins*."

In simpler terms, TBML represents a method used to move illegal money obtained through commerce. It involves exploiting the value, amount or standard of goods or services in international trade to legitimize laundered funds. TBML exploits loopholes in trade finance systems, customs regulations, and financial oversight to transfer money across borders without triggering suspicion.

In the Indian context, despite having stringent regulations against money laundering, the lack of specific provisions targeting TBML leaves significant gaps in the detection and prevention, making trade channels vulnerable to exploitation. The Fifty-sixth Report on the "*Prevention of Money Laundering (Amendment) Bill, 2011*" introduced on 9 May 2012, further commented: "*The Committee would like the Department of Revenue to take into reckoning and incorporate incidence of trade-based money laundering, which has not been distinguished so far as a money-laundering offence"*

1 "*Indian and Hong Kong customs bust trade-based money laundering network, 4 held"*. Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1991583 (Accessed: 16 July 2025)

2 "*Trade Based Money Laundering,*" Financial Action Task Force, 2006. Available at: http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html (Accessed: 16 July 2025)

Methodology and Facilitators of TBML (who facilitates, who suffers, who benefits)

Several methods for money laundering through the global trade network have been studied by authors, institutions and organisations, such as the "*Department of Homeland Security, and US Immigration and Customs Enforcement (2005)*[3]*"*. This can be accomplished in practice by falsifying the cost, volume, or calibre of imports or exports.

This frequently involves exploitation of the financial structure through deceptive operations utilising a variety of financial transportation tools, including wire transfers. The fundamental methods of TBML consist of:

1. **Over and Under Invoicing of goods and services:**

   The main aspect of this method is the mis-valuation of value of the commodities /services so as to transfer more value between the exporter and the importer. The exporter by charging the goods or services at a rate less than the "*fair market price*", transfers value to the importer because when sold in the free open market, the importer will earn a higher price than the price for the goods or services.

   Although, it prima facie appears to be party autonomy, over- and under-invoicing affect the prevalent market prices by creating the appearance of an inflated price level.

   There are significant tax ramifications of over and under invoicing. The amount of the "*export tax credit" or "valued-added tax (VAT)"* refund, that one exporter gets can be significantly increased if he over invoices the value of the commodities he exports. Similarly, an importer can significantly bring down the amount of "*import duties" or "customs taxes"*, that he must pay if he gets an invoice that is undervalued for the goods. These two examples illustrate the link between tax system abuse and trade based money laundering.

   It is also worth highlighting that customs officials will have a more laborious time recognizing over and under invoicing and determining duties/taxes correctly if the commodities/services being trafficked are complex. That is partially because so various

[3] "*Trade Based Money Laundering,*" Financial Action Task Force, 2006. Available at: http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html (Accessed: 16 July 2025)

Customs Authorities lack the data and tools available to ascertain the "fair market prices" of several commodities.

While assessing the risk associated with TMBL by over- and under- invoicing the indicators that would be relevant are "*product taxonomy, category of goods, goods description, unit price and quantity of goods and market price of goods*".

2. Multiple Invoicing of goods and services

Issuance of multiple invoices for the same trade transaction is another way of facilitating TBML. The entity can account for various payments for the identical shipment of merchandise or delivery of services by issuing several bills for the same goods/services. The complexity of these transactions can be further heightened by making these additional payments through various financial institutions.

When evaluating the TMBL risk by "*multiple invoicing, transaction date, transaction amount, product description, invoice number and presence of account information of other banks on the invoice*" are the pertinent indicators.

3. Over and Under Shipments of goods and services

Along with changing the pricing of imports and exports, a money launderer might also artificially inflate or deflate the quantity of goods/services being transported. To the fullest extent, an exporter may even ship no products/services at all, rather he might conspire with an importer to perform all transportation, delivery, dispatch, and forwarding documentation involving this purported "*phantom shipment*" on a repeated basis. Unknowingly, banks and financial institutions (FIs) might be offering trade finance for these non-existent or phantom shipments.

This can be better understood with an illustration: "*An agricultural commodity exporter sent an invoice to his overseas buyer for a shipment of sugar. The invoice seemed valid, stating a reasonable price and amount. However, the container used in the shipment was empty i.e. the goods were never shipped. Notwithstanding that, the buyer proceeded to transfer funds to the exporter. In effect, funds exchanged hands even without goods delivered.*"

In assessing TMBL risk by phantom shipments, the key indications should be "*transaction date, quantity, unit price of goods, presence of transport document and validity of transport document.*"

4. Falsely Described goods and services

A money launderer can also manipulate the quality or kind of goods or services in addition to manipulating import and export prices. An exporter can, for example, export a relatively cheap item and falsely invoice it as a more expensive item or an entirely different item. This method of TBML can be understood from the above-mentioned Hong Kong and India customs' joint-operation, wherein diamonds of low quality were shown as diamonds of high quality for cross-border laundering of money.

A discrepancy between what is being transported and what appears on the shipping and customs documentation arises as a result of such manipulation. False descriptions may also be employed in the supply of services, such as market studies, financial advice, and consultancy. Additionally, there might be additional issues regarding valuing such services based on their fair market value.

TBML Hidden in Plain Sight

1. Use Of Gold in a TBML Scheme in USA (2017)[4]

In the United States, 4 Peruvian nationals were incriminated for their purported participation in a global gold-based money laundering operation worth billions of dollars. From 2013 to 2017, the suspects conspired and collaborated to acquire gold worth multi billion dollars from several countries in Latin America and the Caribbean , which they knew were the proceeds of criminal or illegal activity (including illegal mining, foreign bribery, and smuggling). The accused used a shell company based of Florida (USA), which functioned as a precious metals trading business to execute their plan. The gold was eventually sold to refineries in US completing the money laundering process. These refineries further made wire transfer payments that apparently seemed like legitimate

[4] "*Four Peruvian Members of Multi-Billion Dollar, International Gold (January 9, 2018)".* Available at: https://www.justice.gov/usao-sdfl/pr/four-peruvian-members-multi-billion-dollar-international-gold-money-laundering-scheme (Accessed: 16 July 2025)

transactions for bulk gold purchases.

2. Black Market Peso Exchange Scheme (BMPE)[5]

The U.S. Justice Department indicted seven Colombians and one Indian citizen in January 2020 for their involvement in a global money laundering scheme involving TBML and the utilization of a non-registered money transfer services. The operation was intended to launder the gains from drug trafficking, mostly through a "*Black Market Peso Exchange style approach"*. The scheme was founded upon by Colombian individuals that were said to be money brokers and who received the illegal proceeds from couriers dispersed all over the United States through international wire transfers that came in.

To prevent arousing of suspicion, the real money was incorporated into the US financial market prior to being moved to the Indian citizen's business bank account, who was a suspected complicit merchant. Customers worldwide, including importers in Colombia, bought consumer electronics (products) from the store.

The dealer sent approximately the equal quantity of products to Colombian importers, who made arrangements for the importers to pay for the products by having pesos sent to Colombian money brokers, who forwarded them to the trafficking group. The dealers were less likely to be caught because they did not have to attempt to move any money across borders. The case study emphasises how colludes exporters and importers continue to employ peso conversion systems and abuse legal commercial connections in order to transfer the comparable value from the US to Colombia.

Major Threats of TBML

TBML poses a major threat to financial integrity, enabling tax evasion, funding criminal enterprises, distorting trade markets, and undermining regulatory frameworks through sophisticated cross-border fraud.

1. Facilitating Organized Crime and Terrorism

TBML provides a mechanism for "*organized crime groups"* and *"terrorist organizations"*

[5] "*Trade Based Money Laundering-Trends and Development*", Financial Action Task Force Egmont Group, 2020 p.28

to finance their activities covertly. It enables them to integrate illicit funds into economies, avoiding detection by law enforcement agencies.

In 2016, the "*U.S. Drug Enforcement Administration (DEA)*" dismantled a TBML scheme linked to Hezbollah, where illicit drug proceeds from South America were funnelled through businesses in the Middle East and Africa.[6] Drug cartels in Colombia and Venezuela used trade routes to send money disguised as legitimate transactions to Hezbollah operatives, who then laundered it through used car sales and other businesses in West Africa.

2. Undermining Financial Systems and Markets

TBML erodes the integrity of global financial systems, making it challenging for regulatory bodies to track illicit money flows.

BMPE[7] is a common TBML method where drug traffickers in Colombia and Mexico sell their U.S. dollar drug proceeds to brokers. These brokers then use the money to purchase goods from U.S. businesses, which are shipped to Latin America and resold. This system launders billions of dollars annually while making it hard for law enforcement to identify the original source of money.

3. Enabling Tax Evasion and Unlawful Financial Flows

Criminals use TBML to manipulate invoice values to shift profits to low-tax jurisdictions, leading to significant losses in tax revenues for government authorities.

4. Destabilizing Emerging Economies

TBML can destabilize developing economies by promoting illegal capital outflows and creating artificial trade distortions. In Venezuela's Gold-for-Food Scheme from 2019, the Venezuelan government engaged in TBML by exporting illegally mined gold to Turkey in

---

[6] *"DEA and European Authorities Uncover Massive Hizballah Drug and Money Laundering Scheme (1 February 2016)"*. Available at: https://www.dea.gov/press-releases/2016/02/01/dea-and-european-authorities-uncover-massive-hizballah-drug-and-money (Accessed: 16 July 2025)

[7] "*Trade Based Money Laundering-Trends and Development"*, Financial Action Task Force Egmont Group, 2020 p.28

exchange for food and essential supplies. This scheme facilitated corruption, human rights abuse, and illegal financial flows, exacerbating Venezuela's economic crisis. [8]

The Silent Signals: Red Flags That Reveal TBML Schemes

Red flags in TBML are indicators that suggest a trade transaction may be used to launder money. These warning signs help financial institutions, Customs Authorities, and regulators detect potential illicit financial activities disguised as legitimate trade. TBML red flags can be categorized based on transaction patterns, documentation anomalies, pricing irregularities, and the nature of the goods involved. They include:[9]

1. Goods being exported or imported that don't align with the customer's usual line of business (for example, a steel manufacturer suddenly trading in paper products, or an IT firm engaging in large-scale pharmaceutical shipments);

2. Engaging in trade with countries known for high ML or sanctions risks;

3. Routing shipments through high-risk or non-cooperative jurisdictions, even if only in transit;

4. Dealing in goods or sectors considered high-risk, especially those subject to strict export/import controls (such as military or police equipment, weapons, ammunition, chemicals, sensitive defense items, nuclear materials, precious stones, or critical natural resources like crude oil and metal ores);

5. Using unnecessarily complicated transaction structures that seem designed to conceal the true purpose or nature of the deal;

6. Shipping arrangements that defy economic logic (for example, using a large 40-foot container to move a small quantity of low-value items);

[8] "T*reasury Disrupts Corruption Network Stealing from Venezuela's Food Distribution Program, CLAP"*, U.S. Department of The Treasury, 2019. Available at: https://home.treasury.gov/news/press-releases/sm741 (Accessed: 16 July 2025)
[9] Ross S. Delston & Stephen C. Walls, *"Reaching beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside the Financial Sector*",41 Case W Res J Int'l L, 2009 p.85

7. Transactions where funds come from, or are paid to, third parties who appear unrelated to the deal;

8. Deals that involve front companies or shell entities with little to no real business operations;

9. Shipping destinations or product details that don't match what's stated in the letter of credit;

10. Letters of credit that are heavily amended without clear justification, especially those that alter the beneficiary or payment location;

11. Major mismatches between how a product is described in shipping documents (like a bill of lading) versus the invoice;

12. Transactions relying on letters of credit that are constantly revised or repeatedly extended;

13. Routing goods through multiple countries with no clear economic reason;

14. Payment patterns that don't align with the expected risk or value of the transaction;

15. Trade involving goods often linked to money laundering, such as:

    (a) gemstones,

    (b) jewelry,

    (c) tobacco products,

    (d) consumer electronics and appliances,

    (e) prepaid or stored-value cards,

    (f) precious metals,

    (g) military equipment, arms, ammunition, or war-related materials, including software or components designed for weaponry.

Why Red Flags Are Not Sufficient to Regulate/Monitor TBML:

While red flags and indicators play a crucial role in detecting TBML, they are far from foolproof. A skilled money launderer can manipulate trade transactions to evade detection, rendering these indicators insufficient. The following are the reasons for inefficiency of established red flags:

1. **False Positives and Legitimate Trade Anomalies**

   Many of the red flags identified (e.g., mispricing, unusual transaction structures, shipment size inconsistencies) can occur in legitimate trade. Global trade is inherently complex, and discrepancies in invoices, values, and documentation are common due to fluctuating exchange rates, differing tax regimes, and market volatility. Flagging every anomaly could overwhelm financial institutions and Customs Authorities, leading to inefficiencies and wasted resources.

2. **The Subjectivity of Pricing and Valuation**

   Over- and under-invoicing rely on a "fair market value" standard but determining this is often difficult. Prices of goods fluctuate due to supply chain disruptions, tariffs, and market dynamics—what may seem over- or under-priced could be within a normal business range. Customs officials often lack expertise in pricing all traded goods, making it easy for launderers to justify manipulated prices.

3. **Adaptability of Criminal Networks**

   Money launderers continuously refine their methods to evade detection. Once a red flag becomes widely recognized, criminals adapt by altering trade routes, changing jurisdictions, or using new types of goods. Shell companies can be structured to appear legitimate and bypass financial institutions' due diligence efforts by establishing a fake paper trail. Further, launderers may exploit free trade zones (FTZs) or jurisdictions with lax regulations to conduct TBML unnoticed.

4. **Financial Transactions Are Not a Clear Indicator**

   TBML often involves indirect payment methods, such as third-party intermediaries or barter trade, making it difficult to detect illicit flows based on payment structures. Red flags focus on financial transactions linked to trade, but criminals often use alternate financial systems (e.g., Hawala, Cryptocurrencies, BMPE) to settle transactions outside traditional banking channels.

5. **High-Risk Jurisdictions Are Not the Only Problem**

   While transactions involving high-risk jurisdictions are flagged, sophisticated launderers often route illicit trade through low-risk countries with strong financial reputations. Some of the largest TBML schemes have involved developed countries where regulatory oversight is assumed to be strong (e.g., the U.S., Germany, and Hong Kong).

6. **Focus on Known Techniques Ignores Emerging Methods**

   Red flags are often based on past TBML cases, but new laundering techniques emerge constantly. The rise of e-commerce, digital payment systems, and blockchain-based transactions creates new TBML channels that these traditional indicators do not cover.

7. **Lack of International Cooperation and Data Sharing**

   Many TBML indicators require coordination between customs agencies, financial intelligence units, and banks across multiple countries. Countries often have inconsistent enforcement of trade regulations, making it easy for launderers to exploit regulatory gaps. The lack of centralized trade data means authorities may be working with incomplete information.

Fortifying Trade: Provisions to Regulate TBML

TBML operates at the intersection of international trade and financial crime, exploiting gaps in the regulatory oversight. While several legal instruments address money laundering in general, specific regulations targeting TBML remain underdeveloped.

1. **International Legal Framework**

   Although FATF identifies TBML as a major risk, its Forty Recommendations do not provide detailed guidance on combating TBML specifically. Further, "U*nited Nations Convention Against Transnational Organized Crime (UNTOC)*" encourages global cooperation in tackling ML, including TBML. The *World Customs Organization* (WCO)

Guidelines provides best practices for Customs Authorities to detect trade-based financial crimes.

Case Studies Highlighting Evolution of Regulation Of TBML:

a. Legal Framework in Germany[10]

In response to its attempts to address ML (Money Laundering) and TF (Terror Financing), Germany conducted its first "*National Risk Assessment (NRA)*" in December 2017. The review, led by the "*Federal Ministry of Finance*", engaged 35 federal and local authorities. The significance of TBML was highlighted by the inaugural NRA given Germany's trade volume. Shell corporations, double billing of goods/services, phantom transactions, over and under invoicing of goods/services, and investment of incriminated money in high-value goods (e.g., cars, watches, jewellery, gold, real estate, and paintings) were some of the prevalent TBML methods identified.

The better understanding of TBML risk in certain situation relies significantly on collaboration of public agencies with the private sector and the ability of the obligated parties to report suspicious transactions. The strategy of Germany by far leans towards incorporating understanding from the private sector and most importantly FIs, to have a proper understanding of the intended transaction and participants, without necessarily requiring them to comprehend the required documentation. This deeper understanding allows FIs, particularly banks, to effectively identify potential TBML indicators and report them to the "*Financial Intelligence Unit (FIU)* via "*Suspicious Transaction Reports (STRs)*".

b. Legal Framework in USA[11]

Within the framework of its "*National Risk Assessments*", the USA has defined TBML as both a threat and a vulnerability. Threats like "*transnational criminal groups (TCOs)"* in Mexico and Europe, and their drug trafficking activities, utilize TBML

[10] "*Trade Based Money Laundering-Trends and Development*", Financial Action Task Force Egmont Group, 2020 p.17

[11]"*Trade Based Money Laundering-Trends and Development",* Financial Action Task Force Egmont Group, 2020 p.18

operation due to their sophistication, which makes it challenging for law enforcement to identify them. The U.S. financial system and trade industry are being exploited for use of TBML.

The United States had already incorporated TBML in its "*National Money Laundering Threat Assessment"* in 2005. The "*2015 National Money Laundering Risk Assessment (NMLRA)"* highlighted an update on TBML schemes and found that maximum cases involved a front company or corrupt merchant in the United States receiving illegal proceeds in return for commodities. The U.S. Treasury Department made outreach to several FIs across the country to consider and debate these findings subsequent to the publication of this *NMLRA*. The US published an updated *NMLRA* and its "*National Illicit Finance Strategy"* in 2018. TBML is still a major ML mechanism associated with cartels and drug trafficking, as stated by the 2018 reports. These studies also showed the increased utilization of TBML by "*Professional Money Launderers*" and how it can cut off the connection between the base crime and related ML, thus increasing the difficulty in attributing money laundering to drug traffickers. Finally, the 2020 "*National Illicit Finance Strategy"* noted that "*TCOs are relying more on Asian PMLs who serve as money brokers in traditional TBML schemes. TBML was also highlighted as a possible explanation for a steady decrease in the number of bulk cash seizures throughout the U.S. The decrease in seizures could indicate that TCOs are increasing their use of more discreet methods of moving illicit money, such as TBML."*

2. Indian Legal Framework

The Fifty-sixth Report on the "*Prevention of Money Laundering (Amendment) Bill, 2011*" presented on 9 May 2012, sought to find the figurative number of cases registered that involves TBML and whether PMLA would be sufficient to deal with trade based money laundering situations. In their post evidence submission, the Ministry stated as below: "*Trade based money laundering has not been distinguished from other forms of money laundering as a distinct offence. Hence, no separate data is available showing the number of TBML cases. Whenever proceeds of crime generated out of offences listed in the Schedule to PMLA are laundered through trade, the necessary action of attachment of such proceeds and further legal proceedings under PMLA are initiated. In addition, offences* *under section 135 of the Customs Act, 1962 is also a scheduled offence under PMLA. As and when the Customs Department launches prosecution in cases of evasion of customs duties, the Directorate of Enforcement takes up investigation in such cases under PMLA*."

Direct or Indirect Defences/Promoters of TBML

The FATF report finds that major players in the supply chain, such as legitimate importers/exporters, auditors or accountants, are not questioned why an entirely unrelated third party is involved in the payment settlement process by the FIs even after being aware of the related risks with intermediaries. The following points illustrate why there is no 'will' to counter TBML:

1. **TBML as an Economic Stimulus**

   While TBML is illegal, it inadvertently contributes to economic growth by facilitating capital movement across borders. Many developing countries with strict currency controls or unstable financial systems benefit from informal capital flows that TBML enables. Some economists argue that TBML fills the gaps where formal banking structures fail, keeping businesses afloat and maintaining liquidity in fragile economies.

2. **Hypocrisy of Global Trade Regulations**

   Many major corporations and multinational banks have been implicated in trade fraud and financial crimes, yet they continue to operate with minimal repercussions. If large institutions use trade mispricing and tax havens to their advantage, why should small businesses or individuals be penalized for leveraging TBML techniques to survive? The difference between legal trade optimization and TBML is often subjective, depending on the jurisdiction and enforcement priorities.

3. **Survival Strategy for Businesses in High-Risk Jurisdictions**

   In countries suffering from hyperinflation, sanctions, or economic mismanagement, businesses need alternative methods to conduct international trade. TBML provides a workaround for companies that face arbitrary restrictions on capital flows or government inefficiency in trade financing. Some argue that anti-TBML measures disproportionately harm small businesses, while large corporations easily manipulate the system through legal loopholes.

4. **TBML as a Political Tool**

Governments and financial institutions often weaponize AML (Anti-Money Laundering) regulations against politically inconvenient nations, individuals, or industries. Many so-called "high-risk jurisdictions" are arbitrarily designated, ignoring that Western financial centres (London, New York, Zurich, etc.) have historically been hotbeds for money laundering. TBML enforcement can thus be selectively applied to serve political interests rather than genuine crime prevention.

5. **Is TBML Always "Money Laundering"?**

The very definition of TBML assumes that the movement of funds via trade must have criminal origins, but what if the money itself is not illicit? Entrepreneurs, expatriates, and businesses often engage in trade mispricing simply to circumvent unfair financial barriers or maximize profit margins in unpredictable markets. Why should a harsh regulatory system criminalize financial ingenuity that allows businesses to survive?

6. **Overregulation Kills Global Trade and Economic Growth:**

Efforts to regulate TBML often lead to unintended economic consequences, especially for businesses in emerging markets. Strict regulations force banks to engage in "de-risking" whereby they terminate relationships with legitimate businesses simply because they operate in high-risk jurisdictions. This stifles economic development, isolates certain regions from the global financial system, and prevents financial inclusion.

7. **The Cost of Compliance Outweighs the Benefits:**

The global financial industry spends billions of dollars annually on TBML compliance, yet successful prosecutions remain few and far in between. Compliance burdens are passed down to legitimate businesses, which spend more on reporting requirements than on actual trade operations. Financial institutions should focus on serving customers and facilitating trade rather than acting as government surveillance agents. If TBML regulations are unable to stop criminals, why should businesses and banks bear the cost?

Challenges in Detecting TBML: Technical Limitations Despite Strong Enforcement Efforts

TBML is particularly difficult to detect as it operates within legitimate trade channels, masking illicit financial flows through complex invoicing techniques, misdeclarations, and layered transactions across multiple jurisdictions.

Improved Inspections are Important, but they cannot be a complete solution for identifying cases of TBML. A recent conviction in Ireland serves as a reminder that more organisations than just financial institutions must be involved to effectively combat TBML. Only when Customs Authorities investigated a transport container and determined that the cargo clearly did not match the description of goods/products on the bill of lading did they uncover a "*customs fraud scheme*" that had been in existence for at least 5 years. The leader of one of Ireland's biggest distributors and producers of fruits and vegetables was consequently given a six-year prison sentence.

A perhaps more extreme case is described in the 2004 "*International Narcotics Control Strategy Report"*[12], where inconsistencies were uncovered only after a physical inspection of goods arriving from Dubai, revealing a trade-based money laundering scheme that was directly linked to a member of Al-Qaeda. However, stringent on-site and physical inspections of shipment cargos cannot be a response because of the cost, time delays, personnel and other resources needed. Screening is enhanced by voluntary initiatives such as the "*Customs-Trade Partnership Against Terrorism and Container Security (C-TPAT)"* initiative run by Customs and Border Protection, and statistics monitoring teams such as the "*Trade Transparency Units (TTUs)"* run by "*Immigration and Customs Enforcement (ICE)".*

"Trade Transparency Units (TTUs)" are useful tools, particularly for spotting clear cases of document fraud and flagging mismatches reported by two cooperating customs authorities. However, they currently don't produce enough data to effectively deter trade-based money laundering. Their capacity to catch irregularities is limited, especially when it comes to identifying discrepancies across all aspects of a transaction.

[12] Ross S. Delston & Stephen C. Walls, "*Strengthening Our Security: A New International Standard on Trade-Based Money Laundering Is Needed Now*", 44 Case W Res J Int'l L, 2011 p.737

Inefficiencies in the Current Monitoring and Regulating System

In contrast to capital flight and tax avoidance, which typically entail the cross-border transfer of legally obtained money, ML or TBML capital movements involve the proceeds of crime, which are more challenging to trace. The main challenge to regulate TBML stems from the fact that the shipments associated with TBML form a small fraction of the overall legitimate trade.

The difficulty investigators, FIU analysts, and other specialists encounter when attempting to analyse tax, trade, and financial data is a common obstacle in the detection of TBML. It is frequently necessary to piece together vast amounts of data from several sources, such as criminal databases, STRs, and customs records, in order to properly trace TBML. Many of these sources are maintained by various government agencies and are not always readily available or interconnected.

There may not be a formal procedure for timely information sharing with other agencies or the FIU, and each entity that possesses pertinent data frequently keeps it within its own internal systems. Even in cases where such techniques are present, automatic database cross-referencing may not be supported by them. Authorities are compelled to manually extract, analyse, and analyse data as a result, which slows down the overall identification of TBML activity and costs a lot of time and money.

Why a Risk Based Approach is Needed?

A "*Risk-Based Approach (RBA)*" to monitoring TBML is a strategic method that prioritizes resources and scrutiny on high-risk transactions, customers, industries, and jurisdictions rather than applying a uniform level of monitoring to all trade activities. Instead of treating all transactions equally, RBA assesses the level of risk associated with each trade and applies enhanced due diligence (EDD) wherever necessary.

How is RBA to TBML Monitoring Implemented?

1. **Recognizing TBML Risks**

   The first step would be identifying TBML risks by financial institutions, customs agencies, and trade regulators by examining customer risk (high-risk traders, shell companies, or businesses with unusual trade activities), jurisdictional risk (transactions involving high-risk countries with weak AML/CFT controls or tax havens), product risk (goods commonly used in TBML; gold, diamonds, luxury goods, electronics, pharmaceuticals) and payment risk (use of third-party payments, multiple invoicing, or cash-based transactions in trade finance).

2. **Risk Categorization and Profiling**

After identifying risks, transactions, and entities can be classified into "*low, medium, and high risk*" categories. Financial institutions apply "*Enhanced Due Diligence (EDD)*" and heightened scrutiny to high-risk transactions while applying "*Simplified Due Diligence (SDD)*" to low-risk ones.

a. Low-risk transactions (routine trade between well-established entities in compliant jurisdictions).

b. Medium-risk transactions (involve higher-risk goods, jurisdictions, or unusual trade patterns).

c. High-risk transactions (linked to shell companies, politically exposed persons, high-risk jurisdictions, complex transaction structures, or known TBML typologies).

3. **Monitoring and Detecting Suspicious Transactions**

Risk-based monitoring can be done by Automated Transaction Screening, i.e., by using "*Artificial Intelligence (AI)*" and "*Machine Learning (ML)*" to detect unusual trade patterns, such as over or under invoicing of goods, falsified or manipulated shipping documents, involvement of unrelated third parties in payment settlements. Further, Cross-Border Data Sharing can be used by establishing TTUs to facilitate real-time sharing of customs, financial, and trade data across jurisdictions.

4. **Suspicious Transaction Reporting (STR) and Regulatory Compliance**

If TBML is suspected, financial institutions must file an STR to the Financial Intelligence Unit (FIU) and alert customs agencies and law enforcement for further investigation. Implementation of corrective measures, such as freezing suspicious accounts or declining risky transactions would further strengthen monitoring effectively.

5. **Continuous Risk Assessment and Policy Improvement**

   Since TBML techniques constantly evolve, regulators and financial institutions must regularly update risk models based on emerging TBML trends, train compliance officers and trade professionals to recognize new TBML typologies and strengthen inter-agency and cross-border cooperation to combat TBML on a global scale.

Conclusion

The analysis reveals that TBML exploits vulnerabilities in international trade practices and regulatory frameworks, making it hard to trace and enforce existing anti-money laundering regulations. The review of current monitoring methods and legal structures highlights that conventional red flag indicators alone are insufficient to combat these complex schemes due to their inherent limitations and the adaptive strategies of criminals.

Moving forward, a paradigm shift is necessary. Embracing a risk-based approach that prioritizes high-risk transactions and sectors can significantly enhance recognition and prevention efforts. By integrating state of the art technologies such as AL and blockchain for real-time data analysis and fostering improved inter-agency coordination, stakeholders can build a more robust defense against TBML. Furthermore, strengthening legal frameworks at both international and national levels will be crucial to closing regulatory gaps and ensuring that enforcement is both effective and consistent.

In addition, addressing the challenges posed by stakeholders who inadvertently hinder the regulation process is essential. Engaging trade intermediaries, financial institutions, and other key players through targeted awareness programs, streamlined reporting mechanisms, and incentive-driven compliance frameworks can foster a more cooperative environment. Such collaborative efforts will reduce regulatory ambiguities and enhance the collective commitment to curbing TBML.

Ultimately, the way forward lies in a coordinated, technology-driven strategy that not only addresses the present challenges but is also adaptable to emerging risks. This approach will safeguard the integrity of international trade and contribute to a more transparent and resilient global financial system.