Hidden Cargo: How Trump's 2025 Tariff War Supercharged Trade-Based Money Laundering

By Leon Kort (Co-Founder & COO, Compliance Champs), Laurent Claassen (Financial Crime Expert, Ambassador Compliance Champs) & Melissa Santonocito (Consultant Crypto Compliance, Compliance Champs)

Compliance Champs

A wake-up call at the intersection of trade, finance, and risk

In 2025, Donald Trump returned to the White House with a familiar playbook: tariffs. Within weeks, sweeping duties were imposed on imports from China, the European Union, Canada and Latin America, reigniting a full-spectrum trade war. Economists warned of inflation. Supply chains scrambled. However beneath the policy headlines, a deeper threat has quietly taken hold. Trade-Based Money Laundering (hereinafter: 'TBML') has entered a new golden age.

The convergence of punitive tariffs, rerouted trade, and compliance gaps has created ideal conditions for laundering illicit funds under the guise of legitimate trade. Financial institutions, customs authorities, and policymakers now face a frontline threat they are ill-prepared to detect. The time to act is not "soon." It is now.

What is TBML?

TBML is the process of disguising the proceeds of crime and transferring value across borders using trade transactions. It typically involves over- or under-invoicing, falsely describing goods, misclassifying origin, or issuing multiple invoices for a single shipment.[1] Unlike traditional money laundering, which tends to pass through banking or financial instruments, TBML exploits the complexity and volume of global trade to embed illicit flows into seemingly legitimate commerce.[2]

Despite its scale, TBML remains one of the most under-detected and under-regulated forms of money laundering globally. Many institutions still rely on outdated, manual controls that offer little more than "window dressing" in the face of increasingly sophisticated TBML schemes. A shift towards data-driven, risk-based trade surveillance is essential to close detection gaps and meaningfully disrupt trade-based financial crime. [3]

The tariff effect: how protectionism fuels criminal trade

The 2025 tariffs were designed to curb strategic dependence on adversarial economies. But in practice, they have given illicit actors exactly what they need: cover. By disrupting price norms, fragmenting supply chains, and forcing trade through obscure channels, the tariffs have unintentionally supercharged TBML activity.

TBML thrives on three conditions: opacity, complexity, and plausible deniability. The current tariff climate offers all three.

[1] Financial Action Task Force (FATF). Trade-Based Money Laundering: Risk Indicators. FATF, 2021.

[2] https://www.amlc.nl/witwassen-via-trade-based-money-laundering/

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

1. Volatile prices mask manipulation

As part of the TBML checks the FATF has indicated that they expect financial institutions to look at differences in prices of goods[4]. When market prices are distorted by high duties, there is no longer a reliable benchmark for what goods "should" cost.[5] A 40% markup on a shipment of semiconductors, which might once have triggered a red flag, can now be explained away as price volatility. For money launderers, this offers the perfect alibi. Financial institutions face a narrow window to recalibrate their systems before the new trade environment becomes a blind spot for illicit finance.[6]

2. Transshipment blurs the truth

In response to tariffs, exporters reroute goods through third countries and falsify origin documents. This "origin washing" makes for example Chinese steel appear Turkish, or Chinese electronics appear Vietnamese. The Financial Times reports that social media platforms in Asia now openly advertise origin falsification services, reflecting how deeply entrenched this practice has become. In the absence of robust customs inspection, this deception is rarely detected[7] - though technology providers like MonetaGo[8] are now helping financial institutions detect such fraud by verifying trade document authenticity.

3. New routes, weaker controls

Tariff pressure has shifted trade flows toward ports and free trade zones with minimal AML enforcement. The Organisation for Economic Co-operation and Development (OECD) has repeatedly warned that these environments, with little oversight and fragmented accountability, are breeding grounds for TBML. Smaller ports and re-export hubs are now key points of vulnerability, where manipulated invoices and phantom cargo easily slip through.[9]

The paradox is clear: tariffs aimed at tightening control have instead multiplied the weak spots through which dirty money now flows, disguised not as finance, but as freight.

Real-world case examples: when trade masks crime

As protectionist trade policies accelerate, so too does the misuse of trade routes for criminal gain. The following cases, drawn from both U.S. and European enforcement data, illustrate how the 2025 tariffs have created ideal conditions for TBML to scale.

[4] Financial Action Task Force (FATF). Trade-Based Money Laundering: Risk Indicators. FATF, 2021.

[5] https://www.amlc.nl/wp-content/uploads/2022/02/Trade-Based-Money-Laundering-Risk-Indicators-2021.pdf

[6] https://www.moneylaunderingbulletin.com/risksandcontrols/tradefinance/forgotten-threat-to-frontline-risk-tbml-159081.htm

[7] https://www.ft.com/content/147fddbb-7031-4347-9251-4425614e138d

[8] https://www.monetago.com/

[9] https://www.oecd.org/tax/crime/trade-based-money-laundering-report.htm

1. Transshipment laundering: Qingdao Haiyan group and BGI group

In 2022 and continuing into the post-2025 tariff era, U.S. Customs and Border Protection (CBP) uncovered two major schemes involving Chinese firms, Qingdao Haiyan Group and BGI Group.[10] Both were rerouting Chinese-made cabinetry and electronics through Malaysia and Vietnam, mislabelling the goods to fraudulently claim non-Chinese origin. The objective: evade U.S. tariffs by fabricating "Made in Malaysia" or "Made in Vietnam" declarations.

These schemes were not flagged by financial institutions or trade finance controls, but instead came to light following complaints from U.S. importers. This raises a broader question: should banks be expected to detect such complex supply chain manipulation, or does effective oversight also require greater vigilance and due diligence by the companies importing the goods? As TBML techniques shift away from the financial layer and deeper into logistics and documentation, the responsibility for detection may need to be more evenly shared across the trade ecosystem.

2. The Central Asia trade surge: Europe's blind spot

In Europe, a striking pattern emerged following both the Russia sanctions and the evolving U.S. tariff regime. German exports of vehicles and auto parts to Kyrgyzstan surged by over 5,500% in 2023. Similar patterns were observed in exports to Kazakhstan (720%), Armenia (450%), and Georgia (340%). [11] Recently, a further push for new tariffs on German car makers has been seen by the Trump administration[12].

The problem? These states had no plausible economic capacity to absorb such increases — nor were these exports matched by consumption or legitimate re-export figures. Euro-denominated payments flowed through major European banks, none of which flagged the transactions. Authorities now believe that this corridor was exploited to launder funds by mispricing and misdeclaring high-value goods — classic TBML under the cover of legitimate trade flows

3. Shell intermediaries and phantom freight

Tariffs have also incentivised more elaborate trade routes. A container that once moved from Shanghai to Los Angeles might now pass through Kuala Lumpur, Dubai, and finally New York.

[10] https://www.moneylaunderingbulletin.com/risksandcontrols/tradefinance/forgotten-threat-to-frontline-risk-tbml-159081.htm

[11] https://www.moneylaunderingbulletin.com/risksandcontrols/tradefinance/forgotten-threat-to-frontline-risk-tbml-159081.htm

[12] German car manufacturers incurred costs of half a billion euros in April due to tariffs, says VDA | Reuters

Each stop is an opportunity to insert a shell intermediary, generate fictitious freight charges, or alter the declared origin of goods.[13]

These phantom supply chains, often backed by companies with no staff, no warehouses, and no commercial footprint, are used to disguise illicit payments as trade settlements. Without access to underlying shipping documents or verified cargo data, banks remain largely blind to this laundering activity.

A systemic blind spot in the trade chain

TBML exploits not only the trade system itself but also the fragmented responsibilities that govern it. While Anti-Money Laundering (AML) controls in banking have evolved rapidly to address digital and crypto risks, trade finance remains heavily under-regulated, paper-based, and poorly integrated across actors.

As highlighted in a 2023 report of International Coalition Against Illicit Economies (ICAIE), this systemic blind spot is further deepened by the structure of modern global supply chains, which are "highly fragmented, multi-jurisdictional, and often opaque, especially in high-risk sectors such as automotive parts, electronics, and precious metals."[14]These conditions enable illicit actors to exploit free trade zones, shell intermediaries, and re-export hubs to obscure the origin, value, and destination of goods. In such an environment, even basic due diligence is often bypassed, especially when financial institutions rely solely on surface-level trade documentation.

The result: an entrenched blind spot where criminals can launder value through legitimate trade infrastructure, facing minimal detection and even less enforcement.

To address this, institutions must move beyond financial flow analysis and implement integrated trade intelligence capabilities. This includes:

- Embedding customs and logistics data into AML systems to detect misinvoicing and rerouting patterns;
- Enhancing collaboration across departments (e.g., compliance, trade ops, and legal) to share red flags more effectively;
- Applying risk-based monitoring to free trade zones and high-risk commodities, as emphasized by ICAIE; and
- Investing in public–private data sharing platforms that connect banks with port authorities and customs intelligence in near real time. An example of one of the

[13] https://www.oecd.org/tax/crime/trade-based-money-laundering-report.htm

[14] ICAIE, *The Dark Side of Illicit Economies: Trade-Based Money Laundering, Free Trade Zones, Ports and Financial Safe Havens* (March 2023) https://icaie.com/wp-content/uploads/2023/03/ICAIE-New-Report-The-Dark-Side-of-Illicit-Economies-and-TBML-Free-Trade-Zones-Ports-and-Financial-Safe-Havens.pdf

companies currently focusing on this is Monetago[15], which provides authentication of trade documents against trusted third-party sources, such as trade and maritime data aggegators and government agencies. However, these companies are only successful if a large portion of the financial institutions and trade organizations are collaborating with the same company.

Who's supposed to catch this?

- Banks issue trade finance, process payments, and operate AML compliance programmes but they have little to no visibility into the actual movement or classification of goods.
- Shipping and logistics companies handle the cargo but rarely scrutinise pricing anomalies or shell intermediaries.
- Customs officials are tasked with origin verification but often lack real-time intelligence or the resources to conduct deeper inspections.
- Policymakers set trade frameworks but rarely coordinate with financial crime units when adjusting tariffs or sanctions.

In effect, no single actor owns the full risk picture. The case of German car exports to Central Asia is illustrative: massive, unjustified volume spikes flowed through euro payment systems, yet not a single institution raised a red flag.[16] This is not a failure of tools, but of integration.

This fragmentation is not a new finding. The Financial Action Task Force (FATF) and Egmont Group have warned since 2020 that institutional silos prevent effective detection of TBML, particularly in relation to layered invoicing and disguised trade routes.[17] The OECD has similarly stressed that free trade zones and transshipment hubs lack sufficient oversight and are regularly exploited to move illicit value.[18] Meanwhile, Global Financial Integrity (GFI) reports that over 80% of illicit flows from developing countries stem from mispriced trade transactions and that detection is virtually impossible without meaningful data-sharing between logistics, finance, and enforcement authorities.[19]

The result is a system where criminals understand the gaps better than the regulators do and exploit them with increasing sophistication.

[15] https://www.monetago.com/

[16] 'We Know No Borders': How Kyrgyzstan Became a Hub for Sanctioned Car Exports to Russia | OCCRP

[17] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

[18] https://www.oecd.org/en/publications/trade-based-money-laundering_9789264018082-en.html

[19] https://gfintegrity.org/wp-content/uploads/2023/02/TBML-Policy-Brief-Final..pdf

What must happen now: TBML response plan

The fight against TBML cannot be won with financial crime frameworks alone. What is needed is a trade-first, intelligence-led strategy, one that rethinks how we monitor cargo, verify value, and coordinate across sectors.[20]

Here is a five-point plan for institutions and governments seeking to close the TBML blind spots widened by the 2025 tariff war:

1. Shift from KYC to KYT — Know Your Trade

Banks and regulators must look beyond customer profiles. They need visibility into shipping patterns, transshipment hubs, and pricing anomalies across trade routes. Trade-based red flags, such as circular routing, sudden changes in commodity type, or abnormal shipment volumes, must be incorporated into AML systems. However, this is easier for commodities with publicly available data, but a lot more cumbersome for other commodities.

As the FATF and the World Bank have repeatedly urged, integrating trade data into risk assessment tools is essential to identifying abuse before trades actually reach the payment stage.[21] [22]

2. Leverage pre-arrival shipment data through ICS2

The European Union's Import Control System 2 (ICS2)[23] offers a concrete opportunity to enhance TBML detection. ICS2 requires pre-loading and pre-arrival data submissions for all goods entering the EU, enabling earlier risk analysis and targeting of suspicious shipments.

This system can be a powerful tool in identifying red flags—such as inconsistent commodity declarations, transshipment through high-risk jurisdictions, or improbable routes—*before* goods clear customs or are financed. Banks, customs authorities, and logistics actors should explore how ICS2 data can feed into their TBML risk engines, enabling a more predictive and intelligence-led approach to trade monitoring.
By aligning trade finance and AML controls with customs data like ICS2, institutions can start to close the timing gap that TBML schemes often exploit.

[20] https://www.amlc.nl/wp-content/uploads/2018/11/baft17_tmbl_paper.pdf
[21] https://www.fatf-gafi.org/en/publications/Methodsandtrends/trade-based-money-laundering.html
[22] https://documents1.worldbank.org/curated/en/778831468153277265/pdf/WPS5672.pdf
[23] https://taxation-customs.ec.europa.eu/customs/customs-security/import-control-system-2_en

3. Build a global TBML risk index

The industry needs a shared intelligence platform: a real-time index of high-risk commodities, routes, and jurisdictions. This would allow financial institutions, customs authorities, and logistics actors to access and feed into a central database that flags TBML risks as they emerge.

Tools like Global Trade Alert or UNCTAD's maritime statistics can offer a baseline. However a purpose-built TBML index, drawing on behavioural patterns - not just trade volumes - is now overdue.[24] [25] Platforms like Sayari[26], which already aggregate corporate ownership and trade data to expose illicit networks, offer a valuable model for how such a system could be structured and operationalised and is already used by multiple financial institutions.

4. Create cross-sector TBML task forces

AML teams, customs officers, and logistics providers often operate in silos. However, criminals do not. Task forces that unite public and private actors across the trade chain - including port authorities, freight carriers, and financial intelligence units - are the only realistic way to track illicit cargo and value simultaneously. The Egmont Group has recommended creating fusion cells at key trade chokepoints particularly in jurisdictions vulnerable to transshipment laundering [27].

In March 2025, the UK Government's Tackling Trade-Based Money Laundering programme, coordinated via United Kingdom's Tax, Payments and Customers Authority (His Majesty's Revenue and Customers (HRMC)) and supported by the World Customs Organization, formed a TBML Working Group with customs, tax authorities, logistics operators, and private-sector banks. [28] Its remit: share intelligence regularly, review high-risk commodity flows, and pilot real-time border-finance data integration at key entry points.

The UK model demonstrates several best practices:

- Embedding cross-functional teams within a dedicated TBML task force (customs + AML + logistics + FIU);
- Leveraging data analytics jointly, with real-time customs and trade finance transaction screening;

[24] https://www.globaltradealert.org/
[25] https://unctadstat.unctad.org/EN/Index.html
[26] http://www.sayari.com
[27] https://ripjar.com/blog/4-key-takeaways-for-fius-from-the-egmont-groups-strategic-plan-2022-2027/
[28] HMRC / WCO, *Tackling Trade Based Money Laundering: The UK Government's approach* (WCO News, Mar 2025)

- Enabling public–private collaboration to detect mispricing, misclassification, or unusual flows;
- Focusing on risk-identified trade corridors, particularly involving high-value goods and free-trade zones.

However, more effective collaboration also depends on data sharing across institutions and jurisdictions. Under the current EU Anti-Money Laundering Regulation (AMLR), Article 75, such sharing is limited to high-risk customers, creating a barrier to proactive TBML detection. As part of the 2026 AMLR consultation phase (July 2026), policymakers should consider amending Article 75 to adopt a more risk-based and use-case-driven approach, allowing for targeted sharing of trade-related data where abuse patterns—not just customer risk levels—justify cooperation.

Certain checks, such as duplicate invoice detection, are also ineffective when performed in isolation. Criminals often spread their activities across multiple banks, rendering such checks resource-intensive but ultimately low-impact when done at the individual institution level. A shared, cross-bank approach to key controls—especially those vulnerable to arbitrage between financial institutions—would drastically improve both efficiency and effectiveness.

By modelling this approach, jurisdictions worldwide can finally begin to break the silos and close the TBML blind spot — not by adding more tools, but by integrating people, data, and authority across sectors.

5. Mandate digital, interoperable trade documentation

As long as bills of lading and invoices remain paper-based and different formats are used globally, TBML will remain difficult to detect. A global mandate for encrypted standardised trade documentation is essential. The ICC Digital Standards Initiative is working on this, but without regulatory backing and individual countries support implementation will be too slow. [29]

Digital documentation ensures audit trails, timestamps, and data verification, all critical to identifying fabricated or manipulated transactions. Blockchain technology can further enhance this by providing a tamper-proof, decentralised ledger of trade records, strengthening data integrity and enabling real-time cross-border verification.

[29] https://www.dsi.iccwbo.org/

6. Recognise TBML as a national security threat

TBML is no longer a niche financial crime. It is a strategic risk that affects state revenue, supply chain integrity, and geopolitical leverage. Governments must treat it accordingly. That means integrating TBML into national risk assessments, funding enforcement mechanisms, and requiring that free trade zones also meet applicable AML compliance standards.

As the OECD notes, failing to act not only enables crime, but it also undermines the rule-based trade system itself.[30]

Conclusion: the hidden cargo is not the goods – It's the risk

The second wave of Trump-era tariffs was meant to punish unfair trade practices. Instead, it has fractured supply chains and opened dangerous cracks in the global trade system, cracks through which billions in illicit value now flow.

TBML no longer hides in the margins. It is embedded in the mechanisms of global commerce: in rerouted containers, manipulated invoices, and shell intermediaries camouflaged as trading firms. The tools that once sufficed, checkbox due diligence, sanctions screening, and reactive investigations, are no longer fit for purpose.

The warning signs are everywhere: unexplained spikes in trade volume, falsified origins, phantom freight charges, and criminal infiltration of shipping corridors. These are not accounting anomalies, but structural failures.

To respond, we need a shift in mindset, not just in regulation, but in coordination. Financial institutions must work in lockstep with customs agencies, shipping operators, and international watchdogs. Compliance must stop chasing money alone. It must follow the containers too.

The threat has already landed, in our ports, on our runways, and across our trade routes. We can no longer afford to treat TBML as a secondary concern. The hidden cargo is not just illicit goods. It is systemic vulnerability.

Now is the time to act decisively, collaboratively, and across borders.

[30] https://www.oecd.org/en/topics/tax-and-crime.html

How we can help

At Compliance Champs, we partner with financial institutions, logistics firms, and regulators to identify, assess, and disrupt trade-based money laundering (TBML) risks at every stage of the supply chain.

Our team brings deep expertise in cross-border trade, AML, sanctions compliance, and financial crime investigations. We partner with technology providers which provide cutting-edge tools for trade data analysis and blockchain-enabled documentation tracing.

Whether you're looking to strengthen your due diligence processes, train your teams, or investigate red flags in trade flows, we're here to help you stay ahead of evolving TBML threats.

Let's work together to secure global trade. Contact us to start a conversation.

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

Leon Kort
Chief Operational Officer

+31 6 44 38 82 54
leonkort@compliancechamps.com

Laurent Claassen
Ambassador Compliance Champs

+31 6 44 38 82 54
laurent.claassen@compliancechamps.com

Melissa Santonocito
Consultant Crypto Compliance

+39 3391529276
melissasantonocito@compliancechamps.com

www.compliancechamps.com