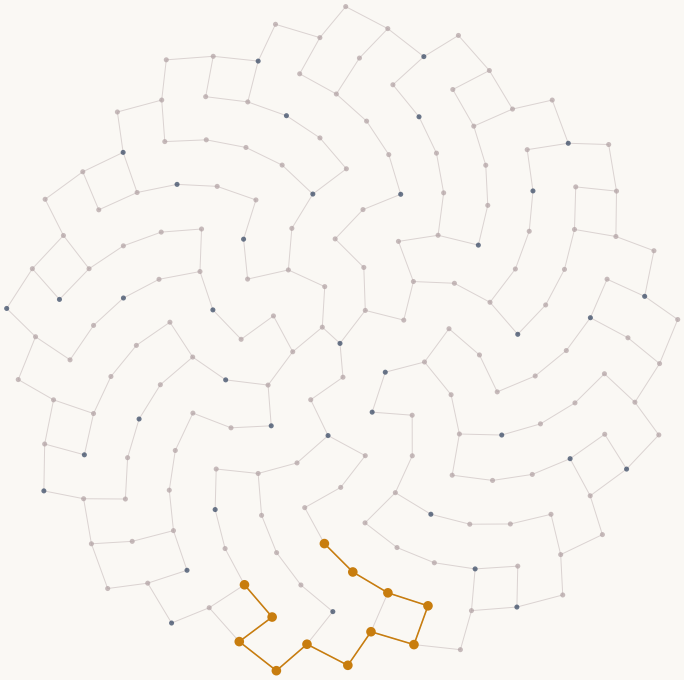
A SAYARI FINANCIAL CRIME BLOG . MAY 2025 . SAYARI ANALYST TEAM



TBML Through Electronics: Why Corporate Data Closes the Gap

Electronics are the preferred vehicle for trade-based money laundering.

FATF's corporate structure approach - not just trade document review - is what modern TBML detection requires.

By Sayari Analyst Team . Published May 2025 . sayari.com

FINANCIAL CRIME

TBML Through Electronics: Why Corporate Data Closes the Gap

By Sayari Analyst Team · Published May 2025

Electronics are the preferred vehicle for trade-based money laundering. FATF's corporate structure approach - not just trade document review - is what modern TBML detection requires.

Trade-based money laundering (TBML) was once treated as an emerging risk. FATF's 2020 guidance and Egmont Group reports formalized a new enforcement reality: TBML is not secondary to cash schemes-it is a preferred primary channel for moving illicit proceeds at scale. A 2025 federal indictment of defendants who laundered drug proceeds through electronics shipments to China and the Middle East demonstrates the shift. The volume-estimated at $1.6 trillion laundered annually through trade globally-explains why regulators moved TBML to the center of AML strategy.

Electronics, particularly smartphones, have become the vehicle of choice for this activity. The category combines three structural advantages for launderers: exceptionally high unit value (permitting large sums in compact shipments), global demand with established supply chains, and pricing ambiguity. That last point is critical. Unlike commodities with transparent spot prices, electronics lack a singular "fair market value"-a smartphone shipped from Southeast Asia to Dubai might legitimately cost anywhere from $400 to $1,200 depending on condition, origin, warranty, and route. Launderers exploit that band. Over-invoicing a shipment of used phones at $1,200 per unit when market rate is $600 allows them to justify why illicit cash entered the trade. Under-invoicing the same goods creates parallel justification for moving the cash out. The practice is elegant in its simplicity and opaque by design.

The challenge for compliance teams: traditional trade-based money laundering detection-reviewing invoices for suspicious descriptions, flagging mismatched quantities, or cross-referencing shipment docs-catches only the surface layer. Sophisticated TBML networks now operate behind legitimate-looking paperwork. The invoices are credible. The commodity descriptions are plausible. The payment terms align with market norms. What those

documents do not reveal-and what trade document review alone cannot expose-is the corporate structure underneath.

Why Electronics Are Structurally Ideal for TBML

Electronics sit at the apex of TBML vehicle selection because the market allows price opacity while demanding legitimacy. A kilogram of cocoa has a London spot price. A barrel of crude oil trades on the NYMEX. But a shipment of refurbished iPhones, or surplus smartphone components, or last-season inventory-these lack standardized pricing mechanisms. A trader can justify almost any valuation with plausible market reasoning.

That opacity combines with two market realities. First, electronics move in established global supply chains. Shipments from Shenzhen to Lagos or Taipei to São Paulo are routine and raise no flags simply by routing. Second, electronics carry unit value high enough to move significant sums in compact shipments. A 40-foot container of smartphones might be worth $2-4 million depending on model and condition, making electronics the preferred medium for launderers moving substantial criminal proceeds without logistical awkwardness.

The method scales. A criminal network might establish a legitimate electronics trading company, purchase real inventory, and then layer additional shipments-either real goods at inflated prices or phantom invoices-to move laundered money. The real trading company provides cover. The price opacity provides justification. The scale provides efficiency.

The Four TBML Techniques and Why Trade Document Review Catches Only Some

Launderers deploy four primary techniques exploiting different points in the trade workflow.

All four techniques embed within plausible trade documents. Trade document review catches sloppy operators. It misses careful ones.

The FATF/Egmont Corporate Structure Shift: From Transaction to Network

The enforcement community's response, formalized by FATF's 2020 guidance and Egmont Group typology reports, represents a conceptual shift. Detection cannot rest on transaction-level scrutiny alone. It must extend to the network.

The new framework asks: who are the parties? What does the corporate registry reveal about their true ownership? Are they real operating entities or vehicles created for a single transaction? Do they share directors, addresses, or bank accounts? Is a newly formed company suddenly handling large volumes, then dormant? These questions point to patterns that trade documents never disclose.

A shipment from Company A to Company B, supported by seemingly legitimate invoices, tells an incomplete story. But when corporate registry data reveals that both companies share a director, registered at the same address, with a third entity at that address receiving beneficial ownership changes in the weeks before-the picture crystallizes. The trade documents are theater. The network reveals motive.

Launderers can falsify invoices, but registering shell companies requires engagement with government systems. That engagement, aggregated across multiple jurisdictions, leaves traces. A corporate ownership network spanning 250+ jurisdictions becomes visible when primary-source corporate registries reveal overlapping directors, layered ownership structures, and shell company patterns.

What a Defensible TBML Detection Program Requires

A defensible program must operate on two levels simultaneously.

The first is the familiar layer: transaction monitoring tied to trade documents. Compliance teams need capacity to flag mismatched invoices, identify suspicious pricing variance, and cross-reference shipments against declared business activity. This layer catches obvious outliers and sends signals to the second tier.

The second layer-where modern TBML schemes hide-is network analysis at the corporate level. Who are these trading entities? What does the corporate ownership network reveal? Are the same directors appearing across multiple trade lanes? Are entities registering, conducting a single major transaction, then dormant? Are shared addresses clustering around regions known for TBML?

Programs operating only on the first layer detect outliers but miss embedded networks. Programs adding the second layer-querying corporate registries, mapping beneficial ownership, analyzing network clustering-add a detection mechanism launderers cannot easily defeat with better forged documents, because detection works from source corporate data, not from paperwork they control.

This is not a replacement for sanctions screening or other AML fundamentals. It addresses the specific vulnerability TBML exploits: the gap between what trade documents communicate and what corporate structures reveal.

The $1.6 trillion in annual TBML activity will continue as long as trade remains viable. Launderers will adapt as detection improves. But the enforcement consensus is clear: detection requires corporate structure analysis alongside transaction monitoring.

For AML teams and trade finance units, this means audit-ready access to corporate registry data across jurisdictions where counterparties operate.

Sayari's corporate and trade data platform is built for this task. With primary-source corporate records from 250+ jurisdictions and visibility into 4 billion trade transactions, compliance teams can move from transaction-level to network-level detection.

Request a demo to see how corporate network analysis changes detection capability, or visit Sayari's financial crime use case.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.