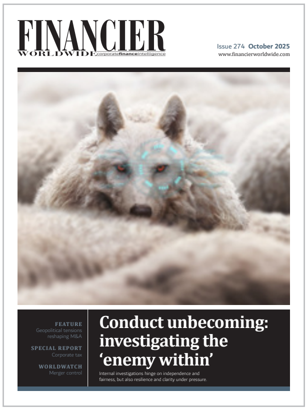

TALKINGPOINT REPRINT October 2025

Trade-based money laundering

FW discusses trade-based money laundering with Alma Angotti and Andrew McCarthy at FTI Consulting, Roberto J. Gonzalez at Paul, Weiss, Rifkind, Wharton & Garrison LLP, and Howard Herndon at Prescentus LLC.

THE PANELLISTS

ALMA ANGOTTI
Senior Managing Director
FTI Consulting
E: alma.angotti@fticonsulting.com

Alma Angotti is a financial crime compliance and sanctions expert with over 25 years of experience in regulatory enforcement and consulting. She held senior roles at the SEC, FinCEN and FINRA, where she led AML enforcement programmes. At FTI Consulting, she advises global financial institutions, fintechs and crypto firms on compliance, risk and investigations. She serves on advisory boards for digital asset initiatives and is approved as an independent compliance monitor by multiple US regulators.

ANDREW MCCARTHY
Senior Managing Director
FTI Consulting
E: andrew.mccarthy@fticonsulting.com

Andrew McCarthy is a financial crime expert with deep knowledge of AML, sanctions, fraud, bribery and corruption across the US, UK, Singapore, Hong Kong and Australia. He has advised clients globally, including in Europe, Asia and the US. Prior to FTI Consulting, he was a partner at Deloitte in Singapore. He also served as a senior economic adviser at the US Department of Defense, supporting global counterterrorism and counter-proliferation efforts.

ROBERTO J. GONZALEZ
Partner
Paul, Weiss, Rifkind, Wharton & Garrison LLP
T: +1 (202) 223 7316
E: rgonzalez@paulweiss.com

Roberto Gonzalez is co-chair of Paul, Weiss's sanctions and AML practice group and was recognised by Legal 500 as a "go-to advisor for financial institutions and technology companies in high-stakes investigations, and regulatory and compliance matters". He has represented clients before the DOJ, Treasury, federal banking agencies and the New York DFS. Previously, he served as deputy general counsel of the Treasury Department, where he supervised the legal offices of OFAC and FinCEN.

HOWARD HERNDON
Co-founder
Prescentus LLC
E: howard.herndon@wbd-us.com

Howard Herndon is a leading expert specialising in artificial intelligence (AI) applications for detecting trade-based money laundering (TBML). His pioneering work developed machine learning algorithms and advanced analytics to identify suspicious patterns in complex trade transaction datasets. Through a groundbreaking proof of concept with Homeland Security Investigations' Trade Transparency Unit, his team demonstrated how AI technologies dramatically improve the speed and accuracy of detecting illicit trade activities, providing crucial support to financial crime prevention efforts.

FW: What are the key characteristics that define trade-based money laundering (TBML)? Approximately what proportion of global illicit financial flows can be attributed to TBML?

Angotti: Trade-based money laundering (TBML) is the process of disguising the origin and movement of illicit funds through trade transactions. The methods used include over- and under-invoicing, multiple invoicing, false shipments and mismatched documentation. TBML is used to launder the proceeds of a variety of criminal activities, including drug and human trafficking, financing terrorism, and evading tariffs and sanctions. TBML accounts for an estimated 87 percent of all global illicit financial flows, which could translate to $800bn to $2 trillion annually. Despite this, court cases have only identified $60bn tied to TBML between 2011 and 2021, indicating widespread underdetection.

McCarthy: TBML is financial hide and seek on a global scale. Criminals exploit the complexity and volume of international trade, hundreds of millions of transactions, murky documentation and cross-border regulations, to disguise illicit funds as legitimate business. Techniques like over- and under-invoicing, duplicate invoicing and phantom shipments are common. And because trade often involves vague or incomplete data, financial institutions (FIs) are left guessing: is this transaction reasonable? Are the counterparties credible? Even regulators joke that detecting TBML is like finding a needle in a stack of needles. Without full transparency or context, it is hard to tell what is real – and that is exactly the point.

FW: How do criminals exploit international trade systems to disguise the movement of illicit funds?

Gonzalez: Criminals use TBML schemes to transfer and conceal illicit proceeds under the guise of legitimate commerce. There are a staggering number of forms these schemes can take. Often, bad actors will use illicit proceeds to buy goods for export – such as electronics or cars – with the subsequent sale of the goods effectively laundering the proceeds. Sometimes, the prices of goods will be significantly higher or lower than market prices, while in other situations there will be no underlying sale of goods at all and the transaction documents will be totally fictional. While TBML may be more difficult to detect than other forms of money laundering, it represents a significant way that criminal organisations launder funds. For example, an April 2025 report by the Financial Crimes Enforcement Network (FinCEN) regarding fentanyl-related suspicious activity reports (SARs) noted that, while TBML SARs accounted for only 2 percent of fentanyl-related SARs in 2024 – they accounted for nearly 42 percent of the aggregate reported amount.

Angotti: Criminals exploit the complexity of international trade and the document-intensive process, by embedding false value or documentation within otherwise legitimate cross-border commerce. For example, launderers can create an invoice that materially overstates or understates the value of the goods which allows for a transfer of value that appears legitimate. These transactions are often routed through intermediaries or low-regulation jurisdictions to evade detection. Importantly, trade finance is only the tip of the money laundering iceberg. The majority of TBML occurs in open account trade and non-financed transactions, where documentation and due diligence requirements are minimal. By leveraging weaknesses in customs oversight, beneficial ownership transparency and cross-border data sharing, these actors move illicit value under the radar of FIs and regulators.

FW: What practical measures can financial institutions (FIs) take to prevent their services from being used for TBML? What are the most common red flags they should monitor?

McCarthy: It all starts with good know your customer (KYC). Knowing your customer, and understanding the nature and purpose of their business, is the strongest line of defence. Are counterparties legitimate? Does their trading pattern make sense compared to others in the same sector? Relationship managers can also be invaluable, offering insights beyond the standard onboarding documents. Red flags include high-risk products, such as scrap metal, mismatched trade routes, odd payment terms or counterparties that do not quite fit. Ultimately, if a business looks off compared to industry norms, that is the cue to dig deeper. Consistency is key because TBML thrives in the gaps.

Gonzalez: Understanding one's customers, including their locations, lines of business and transaction patterns, is crucial to being able to detect unusual activity that may be a flag for TBML. Also, when FIs have access to relevant information, such as in the context of trade finance, they may be able to detect other red flags, such as mismatches between invoice values and market prices or discrepancies between the transactional documents. Sometimes an FI can detect the involvement of a third party in the transaction that seems out of place and could also be a red flag. Bad actors are constantly innovating, and FIs should monitor for new TBML typologies and adjust their controls and training accordingly.

Angotti: FIs can combat TBML by applying a comprehensive, risk-based approach that goes beyond traditional trade finance controls. This begins with strong due diligence, not only on the client, but on their trade counterparties, supply chain partners and logistics providers. Enhanced due diligence is especially critical when dealing with higher-risk goods or jurisdictions with weak anti-money laundering (AML) regulation. Beyond due diligence. Some common red flags include unusual trade invoicing patterns, mismatched or illogical trade routes and counterparties, and discrepancies in shipping and documentation.

Herndon: A compliance programme should implement a multilayered approach combining enhanced due diligence, advanced analytics and staff training. Practical measures include conducting thorough KYC on all trade counterparties, with particular attention to beneficial ownership, implementing pricing analysis tools to identify over- and under-invoicing, establishing relationships with customs authorities and trade databases for shipment verification, and deploying artificial intelligence (AI)-powered transaction monitoring that analyses trade documents holistically rather than in isolation. Key red flags to monitor include significant price discrepancies compared to market rates or similar transactions, mismatches between invoice descriptions and bills of lading, unusual shipping routes or destinations, transactions involving high-risk jurisdictions, customers with limited trade history conducting large transactions, and patterns of round-trip trading or circular transactions. Consider implementing semantic search technologies that can analyse unstructured trade documents alongside structured transaction data, and ensure staff receive regular training on emerging TBML typologies specific to the institution's trade finance products.

A compliance programme should implement a multilayered approach combining enhanced due diligence, advanced analytics and staff training.

HOWARD HERNDON
PRESCENTUS LLC

FW: What makes financial crime compliance particularly difficult for FIs? How can regulators support them in identifying and preventing TBML?

McCarthy: Most FIs only get a narrow view of the transaction, usually a wire between two parties. That means they are working with a few puzzle pieces while regulators might see the whole board. This makes it hard to spot bad actors in real time. Strong KYC and accurate customer risk ratings become the 'north star' for detecting threats.

Regulators can play a huge role by facilitating greater public-private information sharing. If FIs had access to insights across the network, such as counterparties and red flags spotted elsewhere, they would be much more effective. Right now, it is a solo sport that needs to become a team effort.

Gonzalez: TBML crosses multiple sectors, so there are many opportunities for criminals to exploit vulnerabilities in the supply chain and obscure illicit funds. One step regulators can take to support FIs is to provide more detailed guidance on emerging TBML typologies and associated red flags. This might involve more frequent advisories or structured forums for FIs to share insights on TBML detection. More broadly, regulators should issue explicit guidance encouraging FIs to shift resources from lower-risk compliance activities to higher-risk, higher-impact areas like TBML. Because detecting TBML requires significant resources, FIs cannot realistically prioritise it unless regulators and examiners let FIs make those trade-offs.

Bad actors are constantly innovating, and FIs should monitor for new TBML typologies and adjust their controls and training accordingly.

ROBERTO J. GONZALEZ
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

FW: How can advanced technologies help FIs differentiate between legitimate trade and money laundering activities?

McCarthy: AI is shaking things up, but flashy tools do not matter if the data is junk. A strong KYC and customer risk ratings programme are still your foundation. With that in place, AI can analyse transaction patterns, compare them with intelligence databases and flag risks in real time. Agentic AI has helped reduce false positives by refining what actually gets flagged. Optical character recognition has made it possible to scan messy, handwritten shipping documents and pull out usable insights. Even better, AI is taking over many manual review tasks, letting compliance teams focus on complex cases. Smarter tech equals sharper focus.

Herndon: Advanced technologies offer compliance team powerful tools to analyse trade transactions beyond traditional rule-based systems. Retrieval-augmented generation combined with semantic search enables comprehensive analysis by accessing diverse data sources – invoices, bills of lading, customs records and market pricing data – before generating risk assessments. These systems can identify subtle patterns such as pricing anomalies compared to market benchmarks, inconsistencies across multiple trade documents, unusual relationships between trading partners and circular transaction patterns that span multiple jurisdictions. Machine learning (ML) algorithms – using both supervised and unsupervised learning techniques – can build comprehensive networks of customer trading relationships, helping FIs identify shell companies and front businesses. These technologies reduce false positives by providing context-aware analysis rather than simple threshold-based alerts, allowing FIs to focus on genuinely suspicious activities.

Systems continuously learn from the institution's transaction patterns and feedback, improving accuracy over time. Implementation considerations include ensuring data quality, integrating with existing compliance systems and training staff to interpret AI-generated insights effectively.

FW: Could you provide recent examples of FIs being implicated in TBML schemes? What penalties are typically imposed under anti-money laundering (AML) legislation?

Angotti: Several recent cases illustrate how FIs have been unwittingly used to facilitate TBML schemes. In Singapore, five major banks were defrauded of over $95m through trade finance loans based on fictitious invoices tied to luxury goods shipments that never occurred. The shell company behind the scheme had no verifiable logistics footprint yet received financing across multiple institutions due to lack of verifiable trade movement data. In the US, a 2024 federal indictment revealed an alliance between the Sinaloa Cartel and Chinese underground banks. Over $50m in drug proceeds were laundered by purchasing consumer electronics, which were then exported to the Middle East. FIs unknowingly facilitated cross-border payments and trade-related transactions without sufficient scrutiny.

Herndon: The need for a multidisciplined approach is illustrated in a recent case where unusual clusters of trades involving non-industrial diamonds were being shipped from the US to entities in India. The transactions were detected using unsupervised ML and determined to be anomalous based on the frequency and size of the transactions. But it was not until a commodities expert reviewed the trades that their true fraudulent nature was discovered. As it turns out, India is one of the world's largest exporters of non-industrial diamonds and it is highly unlikely that the US would ever be exporting non-industrial diamonds to India in such large quantities.

FW: Looking ahead, how is TBML likely to evolve? And what changes are expected in the strategies used to combat it, with the aim of protecting the integrity of the financial system?

Angotti: TBML is becoming more decentralised, digital and global. As sanctions and tariffs rise, criminals exploit weak jurisdictions, shell companies and digital platforms to obscure illicit flows. Trade in intangible goods, such as intellectual property rights and trade in dual-use items, further complicate detection. Geopolitical shifts and fragmented supply chains increase risks, especially where customs or AML controls are lacking. In response, governments and banks are turning to intelligence-led approaches, using AI, real-time monitoring and cross-border data sharing. Enhanced due diligence, beneficial ownership transparency and collaboration between customs, financial

Ultimately, if a business looks off compared to industry norms, that is the cue to dig deeper. Consistency is key because TBML thrives in the gaps.

ANDREW MCCARTHY
FTI CONSULTING

intelligence units, law enforcement and FIs are essential to disrupting criminal and sanctions-evading trade networks.

> *FIs can combat TBML by applying a comprehensive, risk-based approach that goes beyond traditional trade finance controls. This begins with strong due diligence.*
>
> ALMA ANGOTTI
> FTI CONSULTING

Herndon: Expect TBML schemes to become increasingly sophisticated as criminals adapt to enhanced detection capabilities. Future trends likely include greater use of cryptocurrency integration, more complex layering through multiple jurisdictions and exploitation of emerging trade finance technologies like digital trade platforms. FIs should prepare for evolving compliance strategies that emphasise real-time transaction monitoring integrated with external data sources, advanced analytics combining structured financial data with unstructured trade documents and enhanced information sharing through regulatory frameworks like the proposed Cross-Border Financial Crime Center. Investment priorities should include AI-powered detection systems that can identify complex relationship networks, staff training on emerging digital trade platforms and their associated risks, and partnerships with technology providers specialising in trade finance compliance. Legislative developments suggest increased regulatory focus on cross-border coordination, which may require FIs to adapt reporting systems and information-sharing capabilities. Consider developing pilot programmes with advanced technologies like retrieval-augmented generation to stay ahead of evolving TBML techniques while demonstrating regulatory compliance leadership in the market.

Gonzalez: As with other money laundering typologies, criminal organisations quickly evolve, so it is important for FIs to ensure their compliance programmes are up to date. For instance, FinCEN has recently focused on fentanyl-related illicit finance, which often involves drug cartels and Chinese money laundering organisations and can involve TBML schemes. FinCEN's April 2025 report noted that "cartel-linked TBML schemes appeared to leverage strong consumer demand for electronics, including cellular phones, and vaping/e-cigarette devices" and that "the cartels maintain significant interest in Mexico's vape/e-cigarette market". While TBML can be challenging for FIs to detect, there is a growing set of technological tools, including AI and ML, which can be valuable in analysing large quantities of data for anomalous activity. Compliance professionals should continue to consider how to appropriately integrate these technological advances into their trade compliance programmes. ■