

**TRADE-BASED MONEY LAUNDERING: AN ASYMMETRIC
THREAT WITH TIES TO TERROR AND DRUGS**

BY SENATOR BILL CASSIDY, M.D. (R-LA)

Introduction: Anti-money laundering efforts have made it difficult for illicit organizations to move money through the formal banking system. This makes disguising these transfers as commercial transactions—known as trade-based money laundering—attractive.¹ Terror networks such as Hezbollah are doing just that by using the United States’ banking, trade, and supply chain systems to aid and abet crimes. Drug cartels have also been extremely successful in financing their operations, moving as much as \$100 billion through U.S. financial systems.²

Effective money laundering is crucial to terrorist and criminal organizations. Over the last 15 years, Hezbollah has evolved into a multi-billion dollar transnational organized criminal global enterprise³ with a strong presence in North America and extensive ties with Latin American drug cartels.

Trade-based money laundering is a national security threat. America’s intelligence agencies, law enforcement, U.S. Department of Defense, U.S. Treasury Department, U.S. Department of Homeland Security, U.S. Department of Justice, and the private sector must strategically cooperate to confront terrorist and criminal activity on this new battlefield. There also needs to be a legislative agenda to strengthen national security by countering trade-based money laundering and disrupting drug trafficking, terrorism, adulteration of critical supply chains, and the sale of counterfeit goods.

What is Trade-Based Money Laundering?



Figure 1
Source:
<https://www.acams.org/aml-resources/trade-based-money-laundering/>

Trade-based money laundering (TBML) disguises proceeds of crime by moving value through trade transactions in an attempt to legitimize illicit origins of money or products. This can be done by misrepresenting price, quantity, or quality of imports or exports. TBML techniques vary in complexity and are frequently combined with other money laundering techniques to further obscure the money trail.⁴

Figure 1 illustrates an example of TBML. If one entity is trying to transfer \$1 million to another, they would export \$2 million in goods but only invoice the importer for \$1 million. The importing group could then sell the \$2 million in goods, recovering the initial \$1 million they paid and profiting the additional \$1 million owed by the exporting group.

While transferring the \$1 million through the traditional banking system would raise red flags to authorities, TBML allows transnational criminal organizations (TCOs) to mix large volumes of criminal proceeds with legitimate funds to move illicit proceeds between countries under the guise of licit business transactions.⁵ The transnational nature and complexity of TBML makes detection and investigation exceedingly difficult to achieve, which is attractive to TCOs.⁶

There are certain industries that present a greater risk for TBML, such as couriers, cargo services, freight shipping services, international shipping, and money service businesses. TBML generally appears in jurisdictions with a high risk of traditional money laundering and where authorities have recently improved their traditional anti-money laundering efforts. As a result, criminals are forced to turn to trade to launder money, rather than traditional money laundering schemes.

¹ <https://www.dhg.com/Portals/4/ResourceMedia/publications/Trade-Based-Money-Laundering-Risk-Advisory-DHG-Views.pdf>.

² <https://www.fincen.gov/sites/default/files/advisory/advisu1.pdf>.

³ See e.g., <https://thehill.com/opinion/criminal-justice/411703-department-of-justice-right-to-go-after-hezbollah>.

⁴ <http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html>

⁵ <https://iccwbo.org/media-wall/news-speeches/business-alliance-sheds-light-trade-based-money-laundering-least-understood-financial-crime/>

⁶ *Id.*

Estimates indicate that by 2020, as many as 60 million shipping containers will pass through U.S. ports annually.⁷ DHS is tasked with screening 100 percent of the cargo bound for the U.S., but less than one percent of cargo containers, traveling by ship or plane, is actively inspected.⁸ Identifying TBML is not part of that inspection. These inspections mainly rely on the information provided by party manifests. Our ports and customs agencies do not have the capacity to properly examine this volume which creates a dangerous systemic vulnerability.⁹

TBML negatively impacts a government's finances in two direct ways. First, TBML can result in the decreased collection of customs duties due to undervalued imports and fraudulent cargo manifests entering the commerce of a country.¹⁰ A customs duty is a tariff or tax imposed on goods when transported across international borders.¹¹ The customs duty rate is a percentage determined by the total purchased value of the articles paid at a foreign country.¹² Thus, the duty rate is *not* based on factors such as quality, size, or weight.¹³ As a result, there is an incentive for importers to fraudulently decrease the total reported value of an inbound shipment so as to decrease the duty owed on the shipment.

Second, TBML can decrease tax revenue collected due to the sale of underpriced goods in the marketplace.¹⁴ When imported goods purchased with illicit proceeds are dumped into a market at a low price, governments are robbed of tax revenue that could be collected if the goods were priced in line with the fair market value.¹⁵ This below-market pricing can also put legitimate businesses at a competitive disadvantage, creating a barrier for legitimate economic activity.¹⁶

Colombian cocaine cartels employed TBML in the 1980s. Mexican drug cartels began using TBML in 2010 when Mexico strengthened its banking regulations to restrict the amount of U.S. dollars that could be deposited in Mexican banks as a response to bulk cash smuggling deposits. Recognizing these trends, the Financial Action Task Force (FATF) began studying TBML and terror financing in the 1990s. Congress should thoroughly review FATF's recommendations on combating TBML to determine if they have been implemented and their level of effectiveness.¹⁷

Due to a lack of coordination between agencies, TBML succeeds despite our best efforts. International commercial transaction manifests are tracked by CBP and the Census Bureau. There is no requirement that the information contained in the manifest match the information in the invoice. This lack of manifest and financial invoice information sharing between interested parties, agencies, and financial institutions results in a lack of real-time data tracking necessary to combat TBML. So, if exported goods move from the U.S. to Country 1, but the invoice is routed through Country 2 and the reported value on the invoice is lowered in Country 2 without the knowledge of parties in the U.S. or Country 1, Country 1 will collect fewer duties upon the imported good.

TBML is also one mechanism by which counterfeiters infiltrate supply chains, threatening the quality and safety of consumer, industrial, and possibly military products. Supply chains are the system of organizations, people, activities, information, and resources involved in the initial development of a product to its delivery to the final buyer.¹⁸ This includes the transformation of raw materials, components, and intellectual property to create the product as well as

⁷ <https://www.dhg.com/Portals/4/ResourceMedia/publications/Trade-Based-Money-Laundering-Risk-Advisory-DHG-Views.pdf> (quoting Delston, R. S., & Walls, S. C. (2009). *Reaching Beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside the Financial Sector*. The Case Western Reserve Journal of International Law, 41, p. 85).

⁸ *Id.* (quoting Gouré Ph.D., D. (January 27, 2015). *Terrorism 3.0 and the Need for 100 Percent Cargo Scanning*. Retrieved from The Lexington Institute: <http://lexingtoninstitute.org/terrorism-3-0-and-the-need-for-100-percent-cargo-scanning/>).

⁹ *Id.*

¹⁰ See U.S. Department of the Treasury, National Money Laundering Risk Assessment, June 12, 2015, p. 29, at <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf>.

¹¹ See <https://www.cbp.gov/travel/international-visitors/kbyg/customs-duty-info>

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf>

¹⁶ *Id.*

¹⁷ <http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html>

¹⁸ See Chris Nissen et al., The MITRE Corporation, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, Pg. 7 (Aug. 2018).

necessary coordination with suppliers, intermediaries, and third-party service providers to deliver the correct raw materials, components, and final products.¹⁹

A supply chain is exposed to multiple threats and is vulnerable to adversary insertion of counterfeit parts that pass ordinary inspection but fail operationally.²⁰ TBML is intimately tied to breaches that exist throughout the entire commercial supply chain.²¹ As a result, a TBML scheme can introduce counterfeit products, components, or raw materials into the supply chain that are potentially dangerous to consumers. In addition, these adversaries seek to infiltrate areas of U.S. military dominance and to challenge U.S. interests in cyber domains via supply chains upon which our government, industries, and the public rely.

Effectively addressing this complex issue requires all-source information intelligence to generate actionable data for law enforcement, military, political, diplomatic, and international priorities. The private sector will be an important ally in combating TBML. To address TBML, the U.S. must:

- I. Develop an appropriate methodology and system to integrate necessary trade data and intelligence data;
- II. Direct existing federal agencies to prioritize combating TBML through interagency and private sector cooperation;
- III. Enhance cooperation with trading partners to identify, prosecute, and curtail TBML.

I. Develop an appropriate methodology and system to integrate necessary trade data and intelligence data

There needs to be real-time coordination and reviewable connections between the agency handling the manifest information and the agency handling corresponding financial information within the U.S. and between the U.S. and our trading partners. This could be accomplished through a public distributed ledger system. This system would allow all parties to simultaneously follow the transaction and track any changes made to the documents uploaded to the system. The connection with the manifest allows correlation with the shipped goods.

The private sector also must be involved. The Department of State recently testified before the Senate Caucus on International Narcotics Control that the private sector largely controls the tools of commerce upon which traffickers operate, and is therefore vital to addressing illicit trade.²² Counterfeit goods are a major issue for private industry which therefore has a vested interest in addressing TBML. The private sector is beginning to employ distributed ledger systems. It follows that government agencies should partner with the private sector to promote this effort.

Congress can enable this by acting in the following way: First, Congress should charge the appropriate agencies developing systems to track and correlate shipping manifest and financial information from the public and private sectors in real-time. This consideration would include, but not be limited to, a public distributed ledger. Next, the appropriate agencies should review the efficacy of existing systems. Congress should then commission a public-private partnership through the appropriate agency to develop a scalable system which integrates existing information and reporting requirements to allow real-time analysis of trade transactions. It is important to include private industry so they can assess the impacts in terms of responsibilities, controls, costs, etc. Adapting anti-money laundering and counter-terrorist financing regulation from the financial sector and applying it to the trade sector, without a detailed analysis of the private sector, could be costly and/or ineffective.²³

Using an existing Federally Funded Research and Development Center (FFRDC) is a possible means to develop these systems. Finally, this system can be implemented with a small trading partner. As lessons are learned and data is collected, the solution(s) can be scaled up.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² See Statement of Kristen Madison, Assistant Secretary of State for International Narcotics and Law Enforcement Affairs, Hearing before the Senate Caucus on International Narcotics Control, "Stopping the Poison Pills: Combating the Trafficking of Illegal Fentanyl from China", October 2, 2018.

²³ <http://classic.austlii.edu.au/au/journals/DeakinLawRw/2010/2.html>

II. Direct existing federal agencies to prioritize the combating of TBML through interagency and private sector cooperation

The deaths associated with drug trafficking, the financing of Hezbollah, and the adulteration of supply chains with counterfeit goods showcase the danger TBML poses to our country. The U.S. has confronted similar national security challenges by unifying law enforcement, civilian, and intelligence agencies through a whole of government approach. The abuse of licit trade channels requires business intelligence from the private sector to combat TBML. The National Counterterrorism Center, created after 9/11 under President Bush, is an example of such an effort. A joint interagency task force to focus on illicit trade transactions and protecting our national interests, trade channels, and supply chain is necessary. It will analyze commercial transactions, identify TBML, collect and share information, consolidate classified and unclassified data, and identify all parties involved in a transaction. It would detect sales and distribution of counterfeit goods and identify those using trade to disguise drug proceeds or support terrorist or other threat networks. In addition, detailed, standardized invoices and bills of lading would be required. The shipping data should be properly analyzed to discover anomalies and be coupled with informed statistical sampling. Further, the joint interagency task force will aim to protect supply chains from risk, interruption, and exploitation of vulnerabilities. In doing so, we will address weaknesses in international commerce. To accomplish this, Congress must do the following:

1. Determine the joint interagency task force leadership, membership, authorities inherent to the members, and what new authorities are needed for the group.
2. Create a forum for the private sector to cooperate in detecting and reporting counterfeit goods and supply chain breaches. As discussed above, one option is through a Federally Funded Research and Development Center (FFRDC).

This new task force would provide agencies with the proper tools to analyze financial information on exports and imports and the correlation between manifests and financial invoices. It would also set up mechanisms that allow agencies to identify all involved parties such as originators, transporters, financiers, facilitators, and those who are sending and receiving the goods. In addition, the task force would also engage in capacity building, detecting red flags, and identifying new typologies to assist agents in identifying TBML risks. Further, it would create the necessary communications channels to improve data and information sharing. The ultimate goal is for these action items to extend internationally.

In regards to public-private partnerships, it is important to ensure effective data sharing amongst the private and public sectors. The private sector can share business intelligence and best practices with the government in exchange for data and analysis from the government that they can use to identify, detect, and prevent illicit trade and protect their industries. It is in everyone's best interest to ensure that effective data sharing makes trade more transparent.

III. Enhance cooperation with our trading partners to identify TBML, through trade agreements and Memorandums of Understanding

TBML undermines national security and the rule of law in other countries where it takes place. This is particularly an issue in Mexico and Central and South America where, in addition to corruption, there are weak institutions and a strong presence of drug traffickers. These countries have informal economies, so it is easy to distribute counterfeit goods and sell products without paying the appropriate taxes. It is also important to engage in other regions of the world, particularly those countries with informal economies and corruption in ports. The United States must also engage with China given the number of counterfeit goods produced in the country.

Congress should direct the use of U.S. foreign aid funds to increase the capacities of foreign customs and financial authorities to detect and investigate TBML cases. Congress should also urge the executive branch to negotiate the proper incentives and language into trade agreements and bilateral investment treaties to ensure that our trading partners

cooperate with anti-TBML efforts. The executive branch must ensure enhanced capacity building, robust information sharing, and support in the acquisition of improved systems to scan and inspect packages.

Trade Transparency Units (TTUs)²⁴ must also be extended to additional countries and must not remain exclusively bilateral strategies. The goal should be a global network of TTUs. Congress should coordinate and support the appropriate agencies in the creation of a pilot TTU unit that integrates more than two countries. Congress must ensure that TTUs receive adequate funding and personnel, and require all TTUs to report their progress to Congress. Congress should direct the executive branch to increase existing cooperation on TBML tracking with Mexico and Central and South America and other regions of the world through memorandums of understanding (MOUs). These MOUs would focus on enhancing port collaboration and training of authorities to increase transparency and professionalize foreign customs agents.

Conclusion: There is a direct connection between different illicit activities through the use of licit trade. Our nation is facing a drug use crisis and a supply chain infiltrated by counterfeit goods. The presence of drug traffickers in our region and their intrinsic connection to international threat networks, as well as the use of licit trade to further their motives, is a national security concern. For the United States, TBML is more than just mis-invoicing, mis-labeling, or distribution of counterfeit goods. It includes tax evasion, disruption of markets, profit loss for business, corruption of government officials, and a persistent threat to our economy and security. Threat networks, terror groups, and drug traffickers are often linked through social relationships and common facilitators, which means that despite different objectives, they share the same assets for shipping illicit goods, funneling money, and bribing officials. Those assets form part of a supply chain in which licit trade takes place. This makes TBML one of the most profitable and safe mechanisms to launder money, and it is imperative that Congress act. Until we prioritize TBML as a national security concern, corrupt actors will continue to use licit trade to fund illicit activities. We will only be effective in our efforts if we combat threat networks through the cooperation of our military, law enforcement, intelligence community, private industry, non-government affiliated organizations, partner nations, and our citizens.²⁵

²⁴ TTUs were established to identify global TBML trends and conduct ongoing analysis of trade data. See e.g., <https://www.ice.gov/trade-transparency>

²⁵ Colonel Joshua J. Potter, USSOCOM, Countering Threat Networks: A Primer.