Trade-Based Money Laundering

Risk Advisory

Why does Trade-Based Money Laundering (TBML) present such an emergent risk to law enforcement and AML monitoring? This paper aims to provide a clear understanding of trade based money laundering, by providing the history and definitions, discussing the common transaction trends, and explaining how regulatory guidance applies to the financial industry. Additionally, this paper seeks to identify the traceable transaction patterns common to TBML schemes, and suggests additional countermeasures available to AML.

Trade-Based Money Laundering can be defined as "an alternative remittance system that allows illegal organizations the opportunity to earn, move and store proceeds disguised as legitimate trade. Value can be moved through this process by false-invoicing, over-invoicing and under-invoicing commodities that are imported or exported around the world."[1] In essence, criminals are able to use TBML to place and integrate criminal proceeds into the legitimate market. Funds are generated illegally in the US and EU and are then used to purchase household appliances, consumer electronics, liquor, cigarettes, used auto parts, precious metals, footwear and other low-cost, cash-intensive items. These items are shipped legally back to the home jurisdictions of these money launderers, or else sold legally on US markets. The resulting proceeds have a legitimate business relationship, and are effectively laundered.

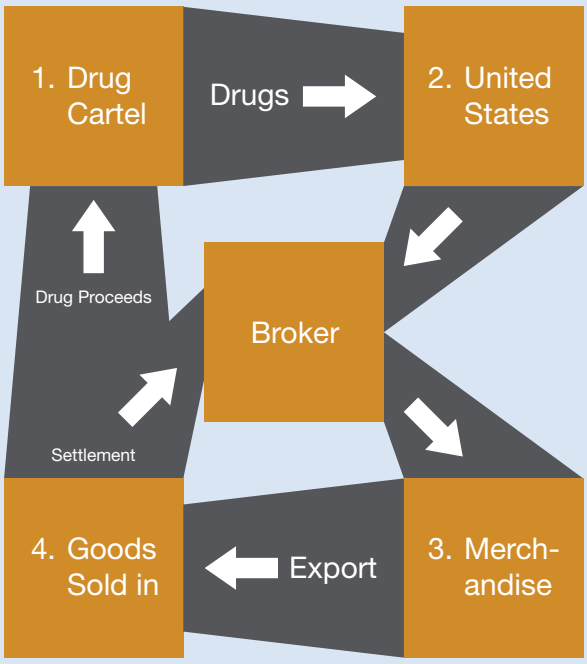
TBML, the Evolution of Informal Value Transfer Systems

Monitoring to prevent criminal enterprise is an endeavor which requires quick adaptation and constant change to internal controls and international laws. In recent years, financial institutions have developed robust AML programs, and have become increasingly successful at monitoring for suspicious activities. A culture of open communication, strong reporting, well-defined know your customer (KYC) policies and robust enhanced due-diligence (EDD) practices, have made it difficult for criminal organizations to stay ahead of investigative networks and regulatory agencies. "International criminal and terrorist organizations have turned to Trade-Based Money Laundering (TBML) to conceal and legitimize their funds, as this is a channel that remains relatively untouched by AML/CFT efforts internationally."[2]

"Trade-based money laundering is not a new [concept]; in fact it has been used globally from Middle East's Hawala system dating back to the medieval period to Colombian cocaine cartels trade-based laundering schemes of the 1980s."[3] Mexican drug cartels, for example, turned to Trade-Based Money Laundering in 2010, after Mexico strengthened its banking regulations to restrict the amount of U.S. currency that could be deposited Mexican banking institutions. The change in legislation came as a response to the bulk cash deposits made in Mexico as part of the Black Market Peso Exchange (BMPE) networks used by Mexican and Columbian drug smugglers.[4] TBML's resurgence was effectively driven by improvements to AML legislation.

The TBML Cycle

TBML takes a variety of different forms. Perpetrators may disguise the true value of an item by under/over invoicing, misrepresenting product values and quantities, and falsifying invoices. The trade networks are used to quickly integrate illicit funds into the trade system, thereby legitimizing the source of funds. The following chart illustrates the basic flow of a TBML cycle.



1. Drug Cartels smuggle drugs across the US Border
2. Drugs are sold in the US
3. An agreement is made with a broker to purchase transferrable goods for a fee.
4. The goods are exported to Mexico using legitimate export documents arranged by the Broker, and subsequently sold on Mexican markets.
5. The Broker Receives his/her fee, and the remaining funds are returned to the Drug Cartel.

So What Is the Risk?

Trade-Based Money Laundering, like other Informal Value Transfer Systems, is designed to obscure the source or destination of funds, or otherwise hide the true purpose of a transaction. Additionally, TBML may present an increased risk of exposure to money laundering and terrorism financing schemes. "TBML may involve not only predicate crimes, such as narcotics trafficking, human trafficking and terrorist financing, but may also disguise the logistical support for terrorist activities, such as the movement of weapons of mass destruction and the materials used to make them."[5] It is estimated that by 2020, as many as 60 million shipping containers will pass through US ports annually.[6] At present, less than one percent of containers passing through US ports receive any significant additional scrutiny.[7] Therefore, trade based transport of illicit goods is currently effectively unmonitored, and presents an essentially unguarded window of opportunity to criminal enterprises and terrorist financiers.

Financial institutions can be held liable for permitting TBML transactions to flow unguarded through their accounts. "American authorities have ratcheted up penalties for banks that assist money-launderers, knowingly or not. In 2012 they reached a $1.9 billion settlement with HSBC after concluding that Latin American drug gangs had taken advantage of lax controls at its Mexican subsidiary. And last year they imposed a $102m forfeiture order on a Lebanese bank implicated in a complex scheme involving the export of used cars to West Africa with the proceeds funneled to Hezbollah, an Islamist group."[8]

Other High Risk Factors

High Risk Geographies

Money Launderers take advantage of jurisdictions with insufficient AML controls. Additionally, because these types of transactions are designed to obscure criminal proceeds or illegal activity, expect to see involvement of jurisdictions known as sources of drug activity, weapons smuggling or terrorism financing. The below table lists some of the regions most widely known for TBML involvement, piracy, terrorism financing and illegal drug trade.[9]

Cuba	Colombia	Iran
Iraq	Libya	Mexico
North Korea	Somalia	Sudan
Syria	Venezuela	Yemen

High Risk Industries

Certain industries present a greater risk. These industries are primarily already identified as high risk following standard NAICS high risk identification. Particular industries to consider are listed below:

- Couriers
- Cargo Services
- Freight Shipping Services
- Import/Export Businesses
- International Shipping
- Money Service Businesses
- Precious Gems Dealers
- Precious Metals Dealers
- Transportation Services
- Used Auto Dealers
- Other High Cash Industries

Red Flags

TBML patterns appear in most jurisdictions with a high risk of money laundering, but a recent improvement in AML programs. Ironically, criminals turn to TBML as a solution once well known, basic Laundering Schemes become ineffective due to improvements in local AML monitoring programs.

Since much of this type of activity occurs outside of normal accounts, it can be extremely difficult to monitor for or track TBML activity. Investigations must therefore focus on the red flags associated with account deposits or transfers of goods. A combination of automated account review software, EDD / KYC programs, and manual review of identified high risk accounts, should yield Patterns of activity that require additional manual review based on identified red flags. Look for the following patterns when performing an investigation or account alert review.[10]

- **Over-invoicing:** The seller acquires surplus value for the goods at point of sale by overstating the price of the goods in the invoice or other documentation.

- **Under-invoicing:** The buyer acquires surplus value for the goods at point of sale by understating the price of the goods in the invoice or other documentation.

- **Multiple invoicing:** The seller can account for several payments by sending several invoices for one and the same trade transaction (either for goods or services).

- **Under-shipment**: The seller sends fewer goods, or goods of inferior quality, than stated in the invoice. The true value of the goods sent is thus lower, so that this method is, in fact, very similar to over-invoicing.

- **Over-shipment:** The seller sends more goods, or goods of superior quality, than stated in the invoice. The true value of the goods sent is thus higher, meaning that this method is, in fact, very similar to under-invoicing.

- **Phantom shipment:** No goods or services are supplied, and all documentation is false.

It should be noted, that capturing these red flags is extremely difficult. Illicit funds are integrated into the international transport industry, an inherently high risk, cash-intensive industry that involves geographical regions with under-developed AML programs. Many of the above red-flags can be missed by investigators, as there is typically limited information included in transaction alerts. Many of these red-flags may be more noticeable to KYC officers and relationship managers, who may have access to invoices and additional account information not available to analysts. Rather than searching for these illusive patterns within all customer transaction records, limiting enhanced monitoring to accounts that appear vulnerable to TBML activity will likely yield more targeted results. Monitoring should be based on the risk profiles developed through strong EDD and KYC policies. Additionally, information involving non-customers should be gathered through research of public records, and inter-bank information sharing through the use of USA PATRIOT Act Section 314(b) inquiries.[11]

It should be mentioned that in a recent effort to crack down on TBML businesses, FinCEN issued a new Geographic targeting Order (GTO) in April, 2015, which seeks to enhance the transparency of business transactions that involve shipments of goods to South America and sold for local currency. As part of the GTO, transaction reporting requirements for such businesses have been lowered from $10,000 to $3,000. Compliance with the new standards is required within 180 days of the order.[12] The goal of such revised reporting will be to make the re-introduction of laundered funds excessively difficult, and improve the abilities of industry monitors and regulatory agencies, to gather useful data, and to better establish profiles on suspect parties.

EDD as a Strong Line of Defense

Bear in mind that the purpose of TBML is to obscure the source or destination of funds, and to remove the majority of the transactions from the customer's account history. Although invoicing irregularities can be used as a strong indicator of TBML or at the least, some attempt at fraud, it is by no means to be considered as the primary or sole indicator of TBML activity. Additionally, monitoring for the above red flags can be difficult for analysts employed in the AML space. Clients

value their privacy, and AML analysts have limited access to invoices, bills of lading, or other documentation involving the suspect transactions.

Transactions in the TBML space tend to vary from the customer's established KYC profile. High volumes of unexpected cash transactions should trigger additional monitoring, and if found to be in conjunction with other pertinent risk factors, should lead to Suspicious Activity Report (SAR) filings. Similarly, uncharacteristic business relationships, reversed flow of funds, incompatible business relationships or industries, and various other deviations from customer profiles should trigger additional monitoring and a review of potentially suspicious activity.

Robust EDD programs, and well defined KYC policies are the financial industry's strongest tools to combat TBML. Since much of the TBML transaction scope occurs outside of account transfers, AML analysts have limited opportunities to monitor customer transactions against this type of money laundering scheme. Therefore, AML analysts must pay special attention to alerted transactions that indicate a deviance from the customer's KYC profile. In fact, "the US Federal Financial Institutions Examinations Council (FFIEC), encourages this approach in its interpretation of the 2001 Patriot Act provisions on money laundering related to trade finance, suggesting that financial institutions take on the task of performing due diligence procedures on their clients' trade activities in addition to monitoring financial activities."[13]

Conclusion

TBML poses a legitimate risk to the international financial community. TBML transactions have the potential to easily obscure the source and legitimacy of funds, making this an attractive process for terrorism financiers and money launderers. Additionally, because TBML involves cash intensive products, it is easy for criminal enterprises to integrate illegitimate funds into the purchasing process without attracting too much attention. Since this process affords few intra account transactions, there are limited resources available to AML analysts to effectively monitor against this form of money laundering. Therefore, good communication between lines of business and between banks using 314(b) inquiries will provide financial institutions with strong tools to mitigate their risks. Effective KYC and EDD policies will further strengthen an institution's ability avoid involvement in TBML activities.

Olivia Greene
Risk Advisory
703.970.0425
olivia.greene@dhgllp.com

1. US Immigration and Customs Enforcement. (n.d.). Investigating Illegal Movement of People and Goods. Retrieved June 17, 2015, from US Immigration and Customs Enforccement: http://www.ice.gov/trade-transparency
2. 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
3. Guzman, D. (2014, September 18). *Trade-based laundering, BMPE becoming in vogue again as traffickers expose longstanding gaps.* Retrieved from Association of Certified Financial Crime Specialists: http://www.acfcs.org/la-raid-on-narco-money-laundering-shows-proliferation-of-tbml-and-black-market-peso-exchange/
4. The Economist. (2014, May 3). Uncontained: Trade is the Weakest Link in the Fight Against Dirty Money. *The Economist.* Retrieved from http://www.economist.com/news/international/21601537-trade-weakest-link-fight-against-dirty-money-uncontained
5. (Delston & Walls, 2009) 87
6. (Delston & Walls, 2009) 99
7. Gouré Ph.D., D. (2015, January 27). *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/
8. The Economist. (2014, September 20). Washing Up: Laundering Mexico's Drug Money. *The Economist.* Retrieved from The Economist Newspaper Limited: http://www.economist.com/news/americas/21618787-drug-kingpins-turn-trade-based-money-laundering-washing-up
9. OFAC. (2015, June 24). *What You Need to Know About U.S. Sanctions*. Retrieved from US Department of the Treasury, Office of Foreign Assets Control: http://www.treasury.gov/resource-center/sanctions/Programs/Documents/terror.pdf
10. Soudijn, M. R. (2014). A Critical Approach to Trade-Based Money Laundering. *Journal of Money Laundering Control*, 17(2), 230-242. doi:10.1108/JMLC-01-2013-0001
11. Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. By registering annually, financial institutions are afforded certain protections under the law, which allow them to share limited customer information with other financial institutions, without violating privacy mandates. (FinCEN, 2013) http://www.fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf
12. FinCEN. (2015, April 21). *FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami*. Retrieved from U.S. Department of the Treasury, Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/nr/html/20150421.html
13. Liao, J., & Acharya, A. (2011). Transshipment and Trade-Based Money Laundering. Journal of Money Laundering Control, 14(1), 79-92. doi:10.1108/1368520111109889, p. 83