TYPOLOGIES OF MONEY LAUNDERING & TERRORIST FINANCING THROUGH TRADE AND MONEY SERVICES BUSINESS (MSB) IN UNITED ARAB EMIRATES.

PREPARED BY: - ALTAF SHAIKH
Table of contents:

1. Executive Summary---------------------------------------------------------------3

2. Background---------------------------------------------------------------------3

3. Introduction---------------------------------------------------------------------5

4. Typologies of Money Laundering through TBML and MSB------------------------8
   a) Trade-based Money Laundering
   b) Money services businesses (MSB)

5. Red flags-----------------------------------------------------------------------13

6. Case Study-----------------------------------------------------------------------18

7. Imposed AML fines due to common and recurring activities---------------------20

8. Regulatory Requirement--------------------------------------------------------23

9. Examples of fines imposed on Financial Institution-------------------------------23

10. Risk mitigation factors of Money Laundering/Terrorist financing------------27

11. Conclusion----------------------------------------------------------------------30

12. References-----------------------------------------------------------------------34
1. **Executive Summary:**

Money laundering is an evolving activity, driven by the need for criminals to legitimize the proceeds of crime. In recent years, global and regional regulators have implemented stringent measures pertaining to Anti-Money Laundering & Terrorist Financing, which has made it difficult to launder money through the traditional channels. Due to the same, money launderers are using more sophisticated methods like TBML especially since it is very difficult to set red flags for detection of illicit funds. This can be supported by a report from International Narcotics Control Strategy Report (INCSR) of 2017 which states billions of dollars are laundered annually by way of Trade-Based Money Laundering (TBML).

Anti-money laundering and countering the financing of terrorism (“AML/CFT”) controls for trade finance and Money Service Business (MSB) as areas where there could be scope for improvement. Robust controls in these areas enable banks to better prevent and detect the risks associated with trade based money laundering, proliferation financing and other sanctions compliance related issues. This paper aims to provide guidance on the AML/CFT controls in trade finance and MSB, assist them in their benchmarking against industry norms and in the implementation of sound risk management practices, and identification of control gaps.

The purpose of this white paper is to illustrate that money laundering & terrorist financing through medium of Trade and MSB are persistent problem in UAE due to which huge fines are imposed on financial institutions.

The sharing of sound practices is intended to help further strengthen their controls and risk management. The guidance should be applied in a risk-based and proportionate manner, taking into account the risks posed by the customers, and the nature and complexity of the trade finance and MSB activities.

2. **Background:**

Money laundering and crime are complement to each other. One cannot survive without the other. Crime generates dirty money and money laundering washes that dirt to make it look clean. People always want a safer place to keep their legal or illegal earnings at a secured and lower tax jurisdiction. Recently a huge leak of documents from a Panamanian law firm, Mossack Fonseca, has thrown new light on how the rich and powerful hide their wealth. They show how the company has helped clients launder money, dodge sanctions and evade tax.

Money laundering is a problem for UAE, despite the steps country has taken to combat financial, organized, and terrorist crimes. The UAE maintains a strong Anti-Money Laundering (AML) system in
an effort to protect against the possibility of money laundering and terrorist financing. There is an increase in risk awareness to dealing with Middle East financial institutions.

The regulator for AML controls in the UAE is the Central Bank (CBUAE); in the Dubai International Financial Centre (DIFC) free-zone, it is the DFSA. The CBUAE regulates all banks, moneychangers, finance companies, and other financial institutions operating in the United Arab Emirates while the DFSA regulates authorized firms, which include banks, insurance companies, investment banks, asset managers, and fund administrators, providing financial services in the DIFC. Both regulators require financial institutions to have extensive customer due diligence (CDD) policies as part of their AML/CTF programs.

AML related rules and regulations have also been issued by both the UAE Central Bank and the Dubai International Financial Centre (DIFC). The survey reveals the growing importance of AML globally and in the region, with regulatory fines now running into billions of dollars, regulatory action becoming genuinely license threatening and increased threats of criminal prosecution against banks and individuals. The financial services industry worldwide and in the UAE, is making significant changes in response to regulatory action and increasingly far-reaching global AML regulations, changing the AML scene from a standalone function under compliance, to a complex and overarching function cutting across legal, risk, operations and tax.

The UAE Federal National Council (FNC) had included four activities that were considered criminal offences – transferring, depositing, transmitting or replacing money with the purpose of hiding or disguising its illicit origin. The FNC has also added two more offences: saving or investing in illegal money.

In the recent past, the Governor of Central Bank of the UAE and Chairman of the National Anti-Money Laundering Committee (NAMLC) inaugurated an annual specialized seminar for the NAMLC at the Central Bank's Head Office in Abu Dhabi. The core areas of discussions were AML/CFT training programs, supervision and examination methodology on AML/CFT, the AML and Suspicious Cases Unit's online STR System and Suspicious cases analysis methodology including international cooperation.

Financial institutions are moving forward in aligning themselves with international best practices, their respective compliance units will have to ensure full understanding of their obligations and support at every level of the organizational hierarchy. Effective financial crime compliance, will require enhanced communication both internally with senior management and externally with regulators.
3. Introduction:

United Arab Emirates (UAE) is a regional hub for transportation, trade, and financial activity. Dubai especially is a major international banking and trading center that has aggressively sought to expand its financial services business.

The United Arab Emirates is the 29th largest export economy in the world and the 31st most complex economy according to the Economic Complexity Index (ECI). In 2016, the United Arab Emirates exported $98.8B and imported $184B, resulting in a negative trade balance of $86B. In 2016 the GDP of the United Arab Emirates was $348B and its GDP per capita was $72.4k.

The top exports of the United Arab Emirates are Gold ($15.8B), Diamonds ($12.3B), Jewellery ($11.8B), Cars ($4.5B) and Raw Aluminium ($4.22B).

Its top imports are Gold ($31.9B), Diamonds ($12.5B), Cars ($11.6B), Broadcasting Equipment ($8.77B) and Planes, Helicopters, and/or Spacecraft ($8.5B).

The top exports destinations of the United Arab Emirates are India ($11.3B), Iran ($ 8.81B) Switzerland ($7.42B), Iraq ($ 5.36B) and Oman ($ 5.15B). The top import origins are China ($ 30.1B), India ($30B), the United States ($22.4B), Germany ($16.3B) and the United Kingdom ($ 9.1B).

<table>
<thead>
<tr>
<th>Foreign Trade Indicators</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imports of Goods (million USD)</td>
<td>226,000</td>
<td>239,000</td>
<td>250,000</td>
<td>230,000</td>
<td>225,000</td>
</tr>
<tr>
<td>Exports of Goods (million USD)</td>
<td>349,000</td>
<td>379,000</td>
<td>375,000</td>
<td>265,000</td>
<td>265,900</td>
</tr>
<tr>
<td>Foreign Trade Indicators</td>
<td>2012</td>
<td>2013</td>
<td>2014</td>
<td>2015</td>
<td>2016</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Imports of Services (million USD)</td>
<td>62,301</td>
<td>61,157</td>
<td>63,744</td>
<td>65,650</td>
<td>83,213</td>
</tr>
<tr>
<td>Exports of Services (million USD)</td>
<td>15,276</td>
<td>20,422</td>
<td>22,982</td>
<td>26,358</td>
<td>63,417</td>
</tr>
</tbody>
</table>

Source: WTO – World Trade organization; World Bank, Latest Available Data

The country also has an extensive offshore financial center, with 37 free trade zones (FTZs) and two financial free zones. There are over 5,000 multinational companies located in the FTZs and thousands more individual trading companies. Companies located in the FTZs are considered offshore or foreign entities for legal purposes. UAE law prohibits the establishment of shell companies and trusts; however, the operation of financial entities in FTZs not identified, regulated, or supervised for financial activity presents a gap in regulatory oversight. Therefore, there is significant opportunity for illicit money launderers to engage in regulatory arbitrage and avoid the controls and supervision put in place by the Central Bank of the UAE (CBUAE) and FTZ regulators of the two financial free zones.

The UAE is particularly susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; its expanding trade ties with the countries of the former Soviet Union; and lack of transparency in its corporate environment. The United Arab Emirates (UAE) is an independent sovereign state bordered by Saudi Arabia and Oman and sharing maritime borders with Qatar, Iraq, and Iran. It is located in the Arabian Gulf with access to the strategic Straits of Hormuz. The total area of the country is 83,600 square kilometers. The federation, which was established on December 2, 1971 (with its capital in the city of Abu Dhabi), is composed of seven emirates: Abu Dhabi, Dubai, Sharjah, Ajman, Umm Al-Quwain, Ras Al-Khaimah, and Fujairah.

United Arab Emirates (UAE) serves as an important regional center for international commerce and banking and has therefore taken vigorous steps to protect the integrity of its economy from terrorist financing. In addition to increased scrutiny of the formal banking sector, exchange houses, hawaladars and trading companies in the UAE have received increased attention. With immigrants comprising over 80 percent of the population, money remittance is a key pillar of the local economy in the Emirates. Since formal financial services are limited in many guest workers home countries, hawaladars are prevalent in the UAE. According to the State Department, there are some indications that trade-based money laundering occurs in the UAE — including through commodities used as counter-valuation in hawala transactions or through trading companies.
To oversee hawalas (alternative remittance systems), the UAE Central Bank issued new regulations in July 2012, making hawala registration mandatory, extending customer due diligence and suspicious transaction reporting obligations to hawaladars and instituting sanctions for noncompliance. The Anti-Money Laundering Suspicious Cases Unit (AMLSCU), the financial intelligence unit (FIU), issued cautionary notes to the public regarding dealing with unlicensed charitable associations and investment companies.

In efforts to combat ISIL, the U.S. and UAE established a new joint financial counterterrorism task force in October 2014 that will be focused on combating extremist fundraising and financial networks in the region. This initiative reflects increased U.S. efforts to stem the flow of money to ISIL from individual supporters, its oil profits, and its access to the international banking system. “The task force was created specifically to target terror finance in the region.” The Gulf and Turkey are the two regions U.S. counterterrorism officials say are key to degrading ISIL’s finances, outside of Iraq and Syria.

The Gulf is a hub of private fund-raising and is also home to a banking infrastructure that offers the potential for money laundering and access to the international financial system.

Gulf countries had enhanced their efforts to combat the financing of terrorism with the following measures:

• Dedicate more financial, human and technological resources to government agencies like financial intelligence units which are responsible for investigating and prosecuting terrorist financing and other financial crimes.

• Enhance the exchange of information and intelligence between government and private sector entities and among partner nations to better combat terrorist financing.

• Raise public awareness of how charitable donations can be used to fund terrorism.

• Identify, pursue, and prosecute terrorist financiers and their facilitators.

As terrorist groups like ISIL and other Al Qaeda affiliates evolve, they seek out ways to circumvent government counterterrorism efforts to realize their brutal agendas. With financial advances in raising and moving money, terror groups can be expected to adopt new methods of acquiring economic resources, and governments must keep up with these innovations. Since financing is the most critical enabler for terrorist groups to recruit, train, arm, and sustain their members and commit acts of violence, combating the financing of terrorism has become an integral part of the fight against terrorism. Given the Gulf region’s geography, economy, and vulnerability to terrorist financing, Gulf countries continue their efforts to stem the flow of funding to terrorist groups and safeguard their financial system.
4. **Typologies of Money Laundering through TBML and MSB:**

A. **Trade Based money laundering (TBML):**

“Trade Based Money Laundering” (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.

There is a growing concern on how the rapid growth in the global economy has made international trade an increasingly attractive avenue to move illicit funds through financial transactions associated with the trade in goods and services. TBML is a complex phenomenon since its constituent elements cut across not only sectoral boundaries but also national borders. The dynamic environment of international trade allows TBML to take multiple forms.

Most of that illegal money comes through various mechanism of TBML. Although there are legitimate ways of using tax heavens, most of what has been going on is about hiding the true owners of money and avoiding paying tax on the money.

We know that within the scope of “trade finance” a Financial Institution (FI) provides services, such as • Bank guarantees • Documentary collections • Financing under open account transactions • Forfeiting and risk participation • Import/export loans • Packing loans • Pre-shipment loans • Structured trade financing • Trust receipts • Warehouse financing • Import/export invoice discounting • Letters of credit (“L/C”) • Financing for transactions under L/Cs and so on.

There are some indications trade-based money laundering occurs in the UAE, TBML is hard to detect because on paper it can look like ‘business as usual’ including through commodities used as counter-valuation in hawala transactions or through General trading companies and such activity might support sanctions-evasion networks and terrorist groups in Afghanistan, Pakistan, Iran, Iraq, Syria, Yemen, and Somalia. Activities associated with terrorist and extremist groups include both fundraising and transferring funds. Bulk cash smuggling is also a significant problem.

1. **Over-invoicing or Under-invoicing.**

A mismatch in the invoice value and the fair market price.

**Over-invoicing:** By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer, as the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market.

**Under-invoicing:** By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer, as the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market.
II. **Over-shipping or Short-shipping**.

A mismatch in the invoiced quantity of goods and the quantity of goods in fact shipped. By over or under-shipping, the invoiced quantity of the goods, the buyer or seller (as the case may be) gains excess value when the payment is made.

III. **Fictitious Trades**.

Also known as “ghost shipping” or “phantom shipping”. A seller may not ship any goods at all, but simply collude with a buyer to ensure that all shipping and customs documents associated with the trade.

IV. **Use of Shell or Fictitious Companies**.

A shell corporation is a non-traded corporation without any active business operations. They can be set up in a matter of days with minimal time and paperwork. They typically have little or no revenue and very few assets, and many of them don’t even have a physical location. Shell companies are often the vehicle behind tax evasion, money laundering, bankruptcy fraud, market manipulation, and other various operational schemes. They typically leave no paper trail because they have no tangible assets and can sometimes get away with submitting very little legal paperwork. The process of transforming money obtained from crime into money that appears to have come from legitimate sources. For example, a drug trafficker can launder dirty money through a shell company by declaring illegal drug proceeds as legal income through his or her “business,” which is actually a shell company with no real operations.

V. **Multiple Invoicing of Goods and Services**.

Issuing more than one invoice for the same trade transaction. By invoicing the same goods or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services.

VI. **Black Market Trades**.

Also, commonly referred to as “black market peso exchange arrangements” (or similar), this usually involves the domestic transfer of funds (that need laundering) to pay for goods on behalf of a foreign importer. A typical black-market trade may involve, for example:

- Money launderer selling funds at a discount to a foreign money broker;
- Money broker integrating these funds into the financial system, often via smaller bank accounts to avoid raising suspicion also known as “smurfing”;
- Money broker paying for goods on behalf of a foreign buyer; and
• Foreign buyer selling the goods to repay the money broker. In such instances, there may not be any fraudulent documents involved.

VII. **Alternative Remittance System.**

Alternative Remittance System i.e. “Hundi” or “Hawala” is a way to transfer funds through informal channels. Hundi means “trust” and hawala means “transfer related to money”. These are also often referred to as “underground banking system” or “parallel banking system” or “informal money transfer system”. Alternative remittance systems are financial services, traditionally operating outside the conventional financial sector, where value or funds are moved from one geographic location to another.

Under-invoicing / over invoicing of goods and services are used in TBML to move funds across the borders not only to disguise its illicit origin but also to evade taxes and duties as well as get undue export incentives. To settle such over or under payments in international trade transactions, Hundi or Hawala mechanisms are used.

Hawala Operators (Hawaldars) or Hundi Dealers operate their business under a global network which helps them to do their business worldwide. Generally, Hawala Operators or Hundi Dealers have other formal businesses, like exchange houses, travel agencies, import/export or shipping companies, grocery stores, gold and jewellery shops, textile or apparel shops and many other business establishments. Often these operators arrange fund transfers for a large number of migrant workers and immigrants, who send back their savings to the home jurisdiction. The popularity of their business lies in certainty, convenience and cheap.

The transactions ensure that remittance reaches the beneficiary at an assigned address in definite time period, for a charge which is less than the transfer charges of formal system. Moreover, the accounts among the Alternative Remittance System operators are settled by making compensatory payments in local currency to persons in the home jurisdiction who have been assigned by the partner hawala operator located abroad. Since such hawala transactions remain largely unreported, there is no reliable data available on hawala / hundi / other alternative remittance systems. The significance of this trade finance mechanism as means to fill up the gap arising out of difference in actual trade value being exchanged and the amount transferred through formal mechanisms call-for larger awareness and focused training on the subject of Alternative Remittance System.

VIII. **Third party payment.**

A third party is introduced preferably in a third jurisdiction, in the payment channel between two trading partners. Such third party may be a notifying party between consignor and consignee. It can also be a facilitator who acts as an intermediary for trade transaction as well as for trade finance mechanism. In still other situations such third party may either be a factoring or forfaiting entity. The technique involves making the process of due diligence to be conducted by domestic financial institutions more difficult to succeed.
B. Money services businesses (MSB)

MSB serve a critical role in the financial world by providing access to money transfer services. The ease, efficiency, and cost-effective access to these services without having to open an account or experience long waiting periods attracts millions of customers each year. Because customers do not have to go through a formal onboarding process or typically collect Know Your Customer (KYC) data to use MSB, customers are largely anonymous. As such, MSBs are traditionally been perceived as high risk and targets for money laundering, terrorist financing, and other suspicious activity.

MSB are non-bank institutions that provide financial services such as money transmission, currency exchange, or check cashing, often with much lower fees than traditional banking institutions and without the requirement to maintain a formal account. However, limited and varying levels of regulatory oversight, as well as challenges to conducting customer due diligence (CDD) in many recipient payout locations and jurisdictions, have raised concerns about AML/CFT vulnerabilities. Even if MSBs are in full compliance with the sending jurisdictions’ regulations, transactions are often perceived as risky when the recipient jurisdiction lacks adequate AML/CFT frameworks or borders jurisdictions that are subject to sanctions, have limited governance capacities, or are experiencing conflict.

Additionally, MSB operators in sending locations often pool funds from several individual transactions to deposit in one lump sum, which obscures information about the original source of the funds. These funds are then transferred to clearinghouses, which often reside in “conduit states,” such as Jordan, Turkey, and the UAE. This additional stopover of funds adds a layer of suspicion and complexity, particularly when conduit states are perceived to have lax AML/CFT controls.

### Distribution of Moneychangers operating in the UAE as at 30/9/2014

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Emirate / City</th>
<th>Head Office</th>
<th>Branches</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Abu Dhabi</td>
<td>30</td>
<td>192</td>
<td>222</td>
</tr>
<tr>
<td>2</td>
<td>Dubai</td>
<td>90</td>
<td>385</td>
<td>475</td>
</tr>
<tr>
<td>3</td>
<td>Sharjah</td>
<td>11</td>
<td>133</td>
<td>144</td>
</tr>
<tr>
<td>4</td>
<td>Ajman</td>
<td>2</td>
<td>31</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>Umm Al Quwain</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Ras Al Khaimah</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>7</td>
<td>Fujairah</td>
<td>1</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>8</td>
<td>Al Ain</td>
<td>5</td>
<td>41</td>
<td>46</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>139</strong></td>
<td><strong>835</strong></td>
<td><strong>974</strong></td>
</tr>
</tbody>
</table>

Source: UAE Central Bank website.

Objective is to identify methods used to channel proceeds of crime through the Money Remittance and Currency Exchange service sectors and mechanisms to prevent and mitigate money laundering and terrorism financing risks in these sectors.
Need to identify red flag or indicators for detection of suspicious ML/TF transactions relating to money or value transfer and currency exchange service providers.

Primary reasons that make the sector vulnerable to ML activities:

- Inadequate and poor implementation of controls for remittances such as “gifts” of significant amounts in absence of sufficient CDD.
- Failure to conduct adequate CDD in establishing source and ultimate beneficiary; reporting entities not being able to effectively determine the relationship or the link between the transfers of funds and the person that sends or receives the funds.
- Unstable currencies and emerging black market which makes the hoarding of foreign currency attractive.
- Failure to strictly adhere to the KYC requirements in fear of losing clients;
- The speed in transfer for international and local remittances, and low commission associated with local Money Value Transfer (MVT) services makes it an attractive option for anyone wishing to remit money.

Below are the Money Laundering techniques and mechanisms said to be used to launder funds through the Money Value Transfer/Currency Exchange sectors:

I. **Disguising the purpose of remittance:**
- Regular transfer of funds in the form of gifts, living allowances, medical expenses, advance payments etc. by the same client to the same recipient in the absence of any relationship;
- The use of third parties to transfer funds to known high risk persons in certain jurisdictions;
- The customer is unwilling to provide routine information when requested; or, the information provided is insufficient or false

II. **Structuring/smurfing:**
- Sending multiple transactions through different Money or Value transfer (MVT) service providers to conceal the value of total funds being remitted to circumvent set thresholds;
- Sending/Receiving to/from different sources/beneficiaries (with indications of relations between the various receivers);
- Money transfers from one account to numerous unrelated accounts;
- Series of foreign exchange transactions structured just below the threshold;
- Frequent exchange of cash into other currencies;

III. **Huge deposits or sudden inflows that are quickly remitted:**
- Money transfers from one account to numerous unrelated accounts.
- The immediate remittance or transfer of funds once they are deposited into an account.
IV. **Others Money Laundering indicators in MVT/CE Sectors:**

- Large or frequent transfers of money from several unrelated individuals in different areas;
- Transferring funds without any apparent economic reason and carrying out transactions which do not make economic sense;
- Money transfers to high risk jurisdictions without reasonable explanation, which are not consistent with the customer’s usual foreign business dealings;
- Multiple senders toward a single individual;
- Using numerous individuals to purchase forex using preloaded visa cards/cash passports and cashing the funds in a neighboring country;
- Customers walking in MVT outlets/premises with huge volumes of currency for exchange;
- Bringing into a country forex from unknown sources which some may be from criminal activities, which may end up being put into formal financial circulation;
- Accounts (especially in remote areas) in receipt of regular large deposits.

5. **Red flags of Trade Based Money Laundering:**

TBML paper published by the Financial Action Task Force (FATF) has a list of red flag indicators that can be used proactively by bank trade finance departments to combat TBML.

The following is a non-exhaustive list of red flags that could highlight trade-based money laundering. These should be considered for implementation by Financial Institutions (FI’s) on a risk-based approach, having regard to the nature and scale of their business and particular scenarios. In relation to suggested red flags that refer to particular percentages or other thresholds, each FI’s should consider the most appropriate percentages or other threshold that addresses the relevant trade-based money laundering risk, based on the FI’s internal risk assessment for that product type, transaction or customer.

I. **Red Flags relating to Trade Finance:**

The transaction involves receipt of cash (or other payments like wire transfers, checks, bank drafts or postal money orders) from unrelated third-party entities or an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods. This may be done to obscure the true origin of the funds (e.g. wires where no apparent business relationship appears to exist between the originator and the beneficiary);

- The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or for reasons like changes of the beneficiary or location of payment;
• A customer’s inability to produce appropriate documentation (e.g. invoice or any other document) to support a requested financial transaction or bank finds double invoicing or a Customer fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer;

• The method of payment appears inconsistent with the risk characteristics of the transaction; (For example, the use of an advance payment for a shipment from a new supplier in a high-risk country or Frequent transactions involving rounding or whole dollar amounts).

• Phantom shipping – no goods are shipped and all documentation is completely falsified to move funds in the guise of trade.

II. **Unusual deposits occurring in combination with one or more of the following indicators:**

• Multiple deposits occurring in various locations when the account owner resides elsewhere, for example, deposits made in various cities when the account owner resides in a different city.

• Multiple bank accounts held by a customer individually or along with closely related family members. These accounts may be held at one or more financial institutions. Such accounts may be used to facilitate the placement and layering of illicit funds.

• Checking accounts receiving cash deposits in amounts under $1,000 as frequently as several times per month. These deposits may be followed by ATM withdrawals in foreign countries. This method, sometimes referred to as micro-structuring, is used by “smurfs” to deposit cash which may then be used to purchase goods.

III. **Red Flags relating to Jurisdictions:**

• Commodity is shipped to (or from) a jurisdiction designated as “high risk” for ML activities;

• Commodity is transshipped through one or more jurisdictions for no apparent economic reason.

• Customers conducting business in high-risk jurisdictions. Although not specifically identified by the authority handling AML work or FATF; FTZs may be added to the list of high-risk jurisdictions given that there is an argument that FTZs exacerbate the risk

• Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.

• Unusual shipping routes or trans-shipment points.

• Funds transferred into a country’s domestic accounts that are subsequently transferred out of the account in the same or nearly the same amounts. Origination and destination locations are frequently high-risk jurisdictions.
IV. **Red Flags relating to Goods:**

- Significant discrepancies between the goods description on the transport document (i.e., bill of lading), the invoice, or other documents (i.e., certificate of origin, packing list, etc.).

- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value;

- The size of the shipment appears inconsistent with the scale of the exporter or importer’s regular business activities;

- The type of commodity being shipped is designated as “high risk” for ML activities; [e.g. high-value, low-volume goods (e.g. consumer electronics, diamonds), which have high turnover rates and which present valuation difficulties].

- Shipment locations or description of goods that are inconsistent with the letter of credit

- Documentation showing a higher or lower value or cost of merchandise than that which was declared to Customs or paid by the importer (i.e. commodity over-valuation or undervaluation)

- Customers involved in potentially high-risk activities, including those subject to export/import restrictions such as equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil

- A shipment that does not make economic sense (e.g. the use of a forty-foot container to transport a small amount of relatively low value merchandise)

- The type of commodity being traded appears inconsistent with the exporter or importer’s usual business activities (e.g. a steel company that starts dealing in paper products, or an information technology company that suddenly starts dealing in bulk pharmaceuticals)

V. **Red Flags related to Customer:**

- Uncommon transaction structure or overly complex transaction structure without a clear and legitimate commercial purpose or some reasonable justification.

- Transaction is not commensurate with known customer profile, structure or business strategy. In a trade-based money laundering context, this may be where the nature or type of goods shipped is not in line with the business nature of the customer

- Customer significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or merchandise) with dubious pricing of goods and services.
• Customer or parties have suspicious addresses. For example, different transacting businesses may share the same address or the businesses only provide a registered agent’s address.

• Customer reacts aggressively to know your customer questions or tries to force the financial institutions to take CDD shortcuts by citing time pressures.

• Customer refuses any form of contact or communication, without a valid reason for that refusal.

• Customer is overly keen to waive discrepancies.

• Customer offers to pay unusually high fees.

• The bank is approached by a previously unknown party whose identity is not clear, who seems evasive about its identity or connections, or whose references are not convincing, or payment instructions are changed at the last minute.

VI. Red Flags related to Documentary:

• The shipment locations of the goods, shipping terms, or descriptions of goods are inconsistent with the L/C. This may include changes in shipment locations to high risk countries or changes in the quality of the goods shipped.

• Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.

• There are substantial discrepancies in merchandise descriptions, e.g. quantities, weights.

• Obvious over or underpricing of goods (that is, significant discrepancies appear between the value of the goods reported on the invoice and the known fair market value of the goods). In a trade context, where goods are highly overvalued, the importer could be moving funds out of their country. Conversely, where the goods are highly undervalued, the exporter could be moving funds out of its country.

• Obvious misrepresentation of the quantity of goods shipped. The contract value is unusually high for a party

• Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

• Transaction involves the use of repeatedly amended or frequently extended L/C.

• The beneficiary or applicant refuses to provide documents to prove shipment of goods (indicates possible phantom shipping or multiple invoicing).
• There are other dubious indicators such as unusual codes, markings or stamps on the monetary instruments (e.g. drafts or bills of exchange, or future dated bills of lading, and transaction under L/C without proper transport document or document evidencing shipment / delivery of goods).

• There are indications that the descriptions of the goods are coded or disguised.

• The customer requests (a) an L/C without calling for a transport documents or documents evidencing shipment or delivery of goods; or (b) an amendment to a L/C removing the transport document or document evidencing shipment or delivery of goods as required in the original terms.

• The transaction is without transport documents evidencing movement of goods.

• The bill of lading describes containerized cargo but without container numbers or with sequential container numbers.

• There are indications that documents have been re-used.

• There are indications of double invoicing.

• Invoice shows “Other/Undefined” charges as an unreasonably high percentage of total transaction value.

• An L/C is dated later than its date of presentation.

• The description of goods on the transport documents (if any) cannot be linked to the document terms and / or the actual invoice.

• Customer re-submits a document rejected earlier as a result of financial crime risk concerns.

• The documentation appears illogical, fraudulent and/or improperly modified from its original content, or certain documentation is absent that would be expected given the nature of the transaction.

In addition, any of these red-flag indicators, in conjunction with shipments to duty-free zones of high dollar merchandise such as electronics, auto parts, precious metals and the like could be an indication of trade-based money laundering or BMPE activity.

It is important to remember that no activity by itself is a clear indication of trade-based money laundering. Due to some similarities with legitimate financial activities, financial institutions should evaluate indicators of potential trade-based money laundering in combination with other red flags and expected transaction activity for its customer before making determinations of suspiciousness. Additional investigation and analysis may be necessary to determine if the activity is suspicious, based on information available to the financial institution.
6. Example and Case Study:

Iranian exporters of oil, dates, textiles and other goods are able to ship their goods overseas but face difficulties when invoicing their customers. They must often employ middlemen throughout the Middle East and often Asia to front for their transactions. Avoiding USD is key, as the strongest proponent of Iranian economic sanctions is the United States. Other countries that issue hard currency including Canada, Australia and the European Union place restrictions on Iranian financial institutions, individuals and corporations dealing in their respective currencies. International financial institutions based in these countries offering correspondent banking services to respondent banks around the world are very curious about their respondent banks dealing with Iranian entities directly or entities covertly representing sanctioned Iranian individuals, corporations or financial institutions. A tremendous amount of time and effort is expended by major correspondent banks to ensure they don’t become unwitting conduits for sanctioned entities via their respondent banks.

The Iranian export transaction is constructed so that the buyer’s funds are directed to a trading company in an offshore financial haven, such as Dubai or Hong Kong.

Case Study 1

XYZ General Trading LLC and ABC General Trading LLC hold accounts with Good Bank. The owner of both these companies is the same Individual (Mr. X). The account activity of XYZ General trading LLC involves frequent cheque deposits and internal transfer of funds within own companies accounts.

XYZ General trading LLC is also holding account with Bank in sanction country. Funds are being transferred from their account with Bank in sanction country to Good Bank account through cheques. Funds are again internally transferred from XYZ General Trading LLC to ABC General Trading LLC within Good Bank. Later outward TT remittances are done to ABC General Trading LLC account which is held with other bank in UAE.

Red flag:

1) Frequent inward remittance/internal transfer from own company account with other bank followed by frequent outward remittance outside the country.

2) Transfer of funds within own Group Companies accounts without any business rational.

3) In the above case we are not aware the exact source of funds which are being brought from their account with Bank in sanction country.

4) Multiple general trading companies owned by same beneficial owners.

Risk:
Layering of funds by executing multiple transactions within Group Company accounts of the same ultimate beneficial owners and wiring out the funds from the country after consolidating the funds.

Risk Mitigation:

Business should be aware their customer line of business and transaction activity. On random basis checks should be performed for high value transactions along with supporting documents to validate the transaction. Proper justification should be obtained from the customer for such transactions behavior which does not appear to be done for any appropriate business rationale.

Case Study 2

LOP PROJECTS LIMITED was registered in a free zone. There were 2 beneficial owners of this company Mr. X and Mrs. Y. The stated business activity was providing services to corporates on gift and promotional items and logistics services. LOP PROJECTS LIMITED maintained USD and AED accounts with Good Bank. When transactions were reviewed in the USD account it was observed that small frequent inward remittances were being received from an entity KAT LIMITED which was located in a high risk offshore location with weak banking supervision and regulations. The purpose of receiving these inward remittances as mentioned by the owner Mr. X was for providing business consultancy services to KAT LIMITED. When a public domain search was conducted on KAT LIMITED it was observed that it was fully owned by Mrs. Y who was 50 % owner of LOP PROJECTS LIMITED. More ever KAT LIMITED had links with several other counterparties which were involved in money laundering scams as per information available on public media.

Red flag:

1) Frequent inward remittance/internal transfer from KAT LIMITED which was owned by Mr. Y.

2) Source of funds and line of business of KAT LIMITED was not cleared.

3) KAT LIMITED was located in a high risk offshore location with weak banking supervision and regulations.

4) KAT LIMITED had links with several other counterparties which were involved in money laundering scams as per information available on public media.

Risk:

Layering of funds by executing multiple cross border transactions and source of funds was not cleared; funds are transferred from high risk offshore location.

Risk Mitigation:
Business should be aware their customer line of business and transaction activity. On random basis checks should be performed for high value transactions along with supporting documents to validate the transaction. Proper justification should be obtained from the customer for such transactions behavior which does not appear to be done for any appropriate business rationale.

7. **Imposed AML fines due to common and recurring activities:**

   I. **Business Strategy, Culture of Compliance and Senior Management Oversight**
   
   - Willful Blindness.
   - Misled regulators
     
     - Extensive efforts over the years to evade regulatory oversight (local and Overseas regulators).
     - Falsifying business records.
     - Significant AML program deficiencies remained pervasive and systemic.
     - Management was aware of failure but did not take action.
     - Remedial measures for the firm’s due diligence policies and procedures were either not implemented or implemented inadequately, even after the adverse findings and formal action by the regulator.
     - Failed to correct previously identified systemic weaknesses.
     - Failure to comply with previous regulatory actions and/or agreements (e.g., consent order).
     - Knowingly facilitating transactions on behalf of third-party money launderers acting on behalf of transnational criminal organizations.
     - Compliance Officer often ignored the AML program.

   II. **AML Governance:**
   
   - Resources.
     
     - Unqualified and/or inadequate staff in compliance.
     - The AML and Compliance officers held other full-time positions within the firm, did not have experience with or training in AML requirements, and spent minimal time dealing with AML matters.
     - The AML officer did not attend meetings with regulators to discuss examination findings, nor was the AML officer provided copies of examination reports detailing AML deficiencies.
     - Management failed to hire knowledgeable and experienced personnel to fill critical roles despite repeat criticisms by the regulator.
     - Branches did not relay concern to the head office about complex structures and transactions.
III. **Policies and Procedures:**

- Disregarded the most basic AML requirements.
- Failure to maintain a compliance program reasonably.
- Failure to have and/or implement procedures for Information Sharing.
- Deficient due diligence policies and procedures for assessing customer risk.
- Failure to have group-wide policies and procedures.

IV. **Risk Assessment Methodology:**

- Failure to have an overall adequate risk assessment.
- Failure to assess its risk exposure within the context of products, services, customers, transaction types or geographical reach of the institution.
- Ineffective Risk rating process. Lack of understanding of basic AML requirements resulted in the failure to identify, evaluate and risk rate dozens of higher risk accounts to mitigate potential AML risks.
- Failure to periodically review risk rating process to ensure that all high-risk customers were identified.

V. **Due Diligence:**

- Customer profiles were missing altogether, or provided too little information to ascertain a customer’s potential risk.
- Review of high-risk accounts was inadequate and often not performed within a reasonable period of time.
- Blindly relied on a third-party vendor to conduct due diligence for all customers.

VI. **Transaction Monitoring:**

- Inadequate automated transaction monitoring systems to support the volume, scope, and nature of international money transfer transactions conducted.
- Failure to adequately audit its high-risk areas and the transactions conducted in those areas.
- Wire transfer monitoring
- Did not address identification of repeat customers, repeat payer’s, or other potentially suspicious trends and patterns.
- Cash deposits activity in all account.

VII. **Suspicious Activity Report:**

- Failure not only to file a few reports but not at all with no AML program in place.
Did not adequately identify, research, report, and monitor suspicious activities occurring through the Branch’s funds transfers, demand draft services, and correspondent relationships, and did not adequately audit and independently test such activities.

Failure to monitor accounts for suspicious activity, relative to the types of products and services, volume of business and nature of customers at the bank.

Despite evidence of nested accounts, failed to detect and review “nested” accounts for suspicious transactions.

Request for Information (RFI): AML Operations / AML Investigations frequently had difficulties getting responses to requests for information generated in connection with automated transaction monitoring “alerts.” Because RFIs went unanswered for considerable period of time without SARs being filed, alerts were often closed without any response to the pending request. As a result of these deficiencies, the firm cleared numerous AML “alerts” based on its own perfunctory internet searches and searches of public source databases but without ever receiving responses to its requests for information.

VIII. Training:

- Nonexistent training.
- Did not have formalized ongoing AML training for all employees. In fact, the training was limited to showing a videotape and circulating memos to certain employees. The training was not job specific or documented.

IX. Record Keeping and Reporting:

- Violations of the Currency Transaction Reporting Requirements.
- Failure to maintain accurate books and records.

X. Sanctions:

- Sanctions violations.
- Firm used non-transparent payment messages, known as cover payments, to conceal the involvement of sanctioned entities.
- Removed information identifying sanctioned entities from payment messages, in transactions processed through financial institutions in the United States.

XI. USA PATRIOT Act:

- Failed to comply with Section 314(a) of the USA PATRIOT Act, a program requiring financial institutions to search their records to locate accounts and transactions of persons that may be involved in terrorism or money laundering.
8. Regulatory Requirement:

The Financial Action Task Force ("FATF"), the Wolfsberg Group and the Joint Money Laundering Steering Group ("JMLSG") have all drawn attention to the vulnerabilities of international trade to money laundering, terrorist financing and sanction breaches, otherwise called Trade Based Money Laundering or TBML. FATF recognizes trade finance as being one of the three main methods used for money laundering. The reports from FATF, Wolfsberg and JMLSG noted that the TBML methods varied in typology from the most basic, such as over- and under-invoicing or double invoicing, to very complex schemes.

The United Arab Emirates is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). It is also a member of the Gulf Co-operation Council, which is a member of the Financial Action Task Force (FATF).

The UAE has recently brought its anti-money laundering (AML) and combating terrorism financing (CTF) legal arrangements into closer alignment with the OECD's Financial Action Task Force's Recommendations (FATF Recommendations) by implementing significant changes and enhancements to the law.

Given the importance of trade finance to the economy and to the future success of the DIFC, the Dubai Financial Services Authority11 ("DFSA") has an important role to ensure this activity is conducted safely and in a manner that properly manages and mitigates the risk of TBML and financial crime. Whilst we fully support the role that trade finance has in the DIFC, we recognize that such activities come with higher TBML and reputational risks that need to be carefully managed by Firms. As part of this effort, we launched a trade finance related thematic review in 2015 ("the Review"). The Review aimed to assess the quality of systems and controls being utilized by Firms to conduct trade finance activities in or from the DIFC and particularly to mitigate TBML risks.

Legislative changes:

The UAE first AML legislation, Federal Law No. 4 of 2002 concerning the Criminalization of Money Laundering (Old AML Law) has been amended by Federal Law No.9 of 2014 (AML Amendment Law), including changing its name from the law "concerning the Criminalisation of Money Laundering" to the law "concerning Combating Money Laundering and Terrorism Financing Crimes". This reflects the addition of CTF to the Old AML Law. A separate law to combat terrorism crimes, Federal Law No. 7 of 2014 (CTC Law), has been enacted. In this briefing, we refer to the Old AML Law, as amended by the AML Amendment Law, as the New AML Law.

Institutional changes:

A comprehensive set of regulatory arrangements for AML/CFT in the UAE, set out in Cabinet Resolution No. 38 of 2014 concerning the Executive Regulation of Federal Law No.4 of 2002
Concerning Anti-Money Laundering and Combating Terrorism Financing (Cabinet Resolution), has been implemented.

9. **Examples of fines imposed on Financial Institution**

- Standard Chartered paid $667 million. In August 2014, Standard Chartered was fined again by $300 million, among other penalties, for negligence in its anti-money laundering mechanisms since the 2012 settlements.

- HSBC Holdings Plc., one of the largest banking and financial services organizations in the world with operations in over 80 countries, settled to pay $1.9 billion to resolve an investigation regarding violation of sanctions and allegations of being exploited by Mexican drug gangs for money laundering in 2012.

- Royal Bank of Scotland has been fined $100m by US regulators for violating US sanctions against Iran, Sudan, Burma, and Cuba. The violations took place between 2005-09, RBS found that bank procedures removed location information on payments made to US financial institutions from countries such as Iran and Cuba.

- Since 2009, over six foreign banks have settled lawsuits with US authorities for violating sanctions, mostly against Iran. Recently, BNP, the fourth largest bank in the world, arranged to pay a record $8.9 billion after pleading guilty to falsifying business records and conspiracy, having violated US sanctions against Cuba, Iran, and Sudan.

- ZTE Corp, China’s largest listed telecommunications equipment supplier, has agreed to pay a total of US$1.2 billion in penalties to the US government to settle its violation of long-standing trade sanctions on Iran and North Korea. The US government has stated that between January 2010 and April 2016, ZTE conspired to evade the long-standing and widely known embargo against Iran to obtain contracts with and related sales from Iranian entities to supply, build, operate and service large-scale telecommunications networks in Iran made out of equipment and software from the US.

- Western Union pays nearly $600 million over failures in AML, fraud & agent oversight: The world’s largest money transmitter will pay nearly $600 million to U.S. authorities, the largest compliance-related penalty ever against a money services business, for enabling a range of frauds and financial crimes, failures in agent oversight, and not filing thousands of suspicious activity reports.

- Deutsche Bank AG has been fined nearly $630 million by regulators in the UK and US over suspicious ‘mirror’ trades that enabled an estimated $10 billion to flow out of Russia through London and New York, and for “significant deficiencies” throughout its AML control framework.
• Habib Bank, Pakistan’s largest lender, and its New York branch will pay a fine of $225m to the New York Department of Financial Services for “repeated breakdowns” in the bank’s AML and sanctions compliance programmes before it exits from the US, the regulator announced on 7 September [2017].

• The Commonwealth Bank of Australia faces civil penalty proceedings in federal court after AUSTRAC, Australia’s financial intelligence unit and AML/CFT regulator, accused it of “serious and systematic non-compliance” with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

• ABN Amro Group NV, the Dutch state-owned lender, has been fined more than $1.3 million in total by regulators in the Netherlands and Dubai for AML systems and controls failures at its private bank in Dubai, notably for the period 1 January 2013 to 31 December 2014.

![Bank Penalties](chart.png)
Which crimes are most commonly correlated with money laundering?

- Fraud: 36%
- Narcotics Trafficking: 31%
- Conspiracy & Collusion: 29%
- Organised Crime: 27%
- Theft & Embezzlement: 18%
- Bribery & Corruption: 11%
- Tax & Customs Violation: 10%
- Forgery: 9%
- Cybercrime: 7%
- Extortion: 5%
- Regulatory Enforcement: 5%
- Frozen & Seized Assets: 5%
- Unlawful Arms & Ammunition Possession: 4%
- Public Office Abuse: 3%

FINES FOR BANKS THAT BREACHED U.S. SANCTIONS

<table>
<thead>
<tr>
<th>Year</th>
<th>Bank</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>US</td>
<td>$100 million</td>
</tr>
<tr>
<td>2005</td>
<td>ANH/Abbasi Bank</td>
<td>$80 million</td>
</tr>
<tr>
<td>2006</td>
<td>National Australia Bank</td>
<td>$400,000</td>
</tr>
<tr>
<td>2007</td>
<td>Royal Bank of Scotland</td>
<td>$500 million</td>
</tr>
<tr>
<td>2008</td>
<td>HSBC</td>
<td>$11.8 million</td>
</tr>
<tr>
<td>2009</td>
<td>Chase</td>
<td>$100 million</td>
</tr>
<tr>
<td>2010</td>
<td>BNP Paribas</td>
<td>$8.9 million</td>
</tr>
<tr>
<td>2011</td>
<td>HSBC</td>
<td>$1.9 billion</td>
</tr>
<tr>
<td>2012</td>
<td>Bank of America</td>
<td>$1 billion</td>
</tr>
<tr>
<td>2013</td>
<td>JPMorgan Chase</td>
<td>$100 million</td>
</tr>
<tr>
<td>2014</td>
<td>Commerzbank</td>
<td>$1.45 billion</td>
</tr>
<tr>
<td>2015</td>
<td>Credit Suisse</td>
<td>$5 million</td>
</tr>
</tbody>
</table>

KEY
- Bank Location
- Sanctioned Country/Entity
- Bank Fine
- United Nations Sanctions

- Australia
- Italy
- Switzerland
- Bahamas
- Japan
- United Arab Emirates
- France
- Netherlands
- United Kingdom
- Germany
- Russia
- United States of America

- National Bank of Abu Dhabi
- Emirates Bank
- Deutsche Bank
- Mitsubishi UFJ Financial Group
- National Bank of Pakistan
10. Risk mitigation factors of Money Laundering/Terrorist financing:

These are suggestions only, and should be considered for implementation by individual financial institution on a risk based approach, having regard to the nature and scale of their business and particular scenarios. Need to consider that there are many legitimate trade transactions that involve, for example, complex shipping routes involving multiple jurisdictions or complex payment mechanisms. Understanding the commercial purpose of any transaction is a key requirement. Ultimately, trade based money laundering typically involves the use of trade to disguise the proceeds of crime and move value. Conversely, greater transparency in a customer’s affairs reduces the risk that the customer is linked to trade-based money laundering.

I. **Trade Controls:**

- Implementing Trade Controls that provide specific guidance on AML/CFT matters in the context of trade.
- Ensuring Trade Controls contain appropriate procedures for handling exception reports and red flags, as well as a procedure for escalating such reports, setting out clear lines of escalation.
- Considering ML/TF risks specific to their trade-related activities and identifying the customers and transactions that present higher risk at various stages of relevant trade transactions.
- Requiring relevant staff to undertake appropriate CDD (see suggested practices under “CDD Procedures” below) and make use of CDD information to assess whether the trade transactions are commensurate with the customer’s background.
- Implementing reports and systems (such as exception reports and detection scenarios) that capture the transaction pattern or activities of customers, such as the following examples: Transactions involving high-risk jurisdictions
- Requiring relevant staff to conduct appropriate screening (see suggested practices under “Screening Techniques” below).
- Ensuring that red flags are regularly updated and easily accessible to staff.

II. **CDD Procedures:**

- Documenting an internal assessment framework to assess who is a “customer” for the purposes of the AMLO in a given trade transaction or another trade-related scenario.
- In addition to the assessment of customer’s trade-based money laundering risk upon establishment of the relationship, assessing, on a case-by-case basis or in relation to a particular category of trade transactions.
- Assessing customer’s trade-based money laundering risk based on their anticipated trade-related activities, upon application for relevant services. Examples of factors for consideration may include types of goods, trade volumes, counterparties and shipment methods.
- Documenting a formal consideration of trade-based money laundering risk in applicable Trade Controls for particular types of trade transactions and categories of customers.
- Obtaining and reviewing underlying trade documentation wherever possible.
• Where reasonably practicable, obtaining and using reliable and up-to-date pricing information for relevant commodities and perform price checks on a sampling basis. FIs may have regard to publicly available sources of pricing information for commodity-related transactions. Given the difficulty in obtaining market prices for certain other goods, such as garments and household items, FIs should simply make further enquiries where the pricing of the goods appears to be manifestly unusual, or there are other ML/TF risks, such as red flags. By way of example, the pricing of a t-shirt could be seen as “manifestly unusual” and warrant further enquiries where the invoice states the unit cost is USD 100, where the normal unit cost would be in the order of USD 10. FIs may wish to consider establishing acceptable price variance thresholds (which could accommodate different thresholds for different types of underlying goods/commodities) and escalation procedures when the thresholds are exceeded.
• Ensuring trade processing staff keep up-to-date with emerging trade-based money laundering risks.
• Requiring processing teams to escalate suspicions for investigation as soon as possible, having regard to internal escalation procedures.

III. Screening Techniques:
• Identifying and screening all relevant parties to a transaction and other information contained within trade documents against applicable sanctions lists.
• Screening for and recording in relevant systems information on all relevant fields to a transaction, such as, for example:
  • Counterparty names and locations
  • Counterparty banks, their capacity in the transaction, and locations
  • Customer names including individuals and companies
  • Carrier / charter / agent
  • Consignee
  • Country of origin
  • Description of goods / commodities
  • Freight forwarders and shipping companies
  • Originating and recipient entities of the goods (i.e. importer and exporter)
  • Shipper, consignee and notification party on transport documents
  • Shipping route (such as the port of loading, port of discharge, port of transhipment, etc.)
  • Vessel names and Flag of vessel
• Investigating hits before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made.
• Using reliable third-party data sources where appropriate to verify the information given in trade documentation, such as Letter of credits and bills for collection, and in circumstances where credit lines are provided, or otherwise facilitated through open account trades, such as invoice financing, pre-shipment financing, inventory financing.
• Appropriately prioritizing the review of certain types of potential matches following analysis of previous sanctions alerts.
• Validating key information where possible, such as shipping container numbers.
• Ensuring new or amended information about a transaction is captured and screened.
• Re-screening for potential sanctions matches when appropriate – for example, at the key stages of a transaction.

IV. Expertise, Training and Awareness:

• Employing staff involved in CDD, screening and review in relation to trade transactions (‘Level 1’ trade processors) with good knowledge of international trade and customers’ expected activities and a sound understanding of trade-based money laundering risks.
• Employing staff responsible for reviewing escalated transactions with substantial knowledge of trade-based money laundering risks.
• Making available detailed guidance for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags.
• Providing tailored training that raises staff awareness and understanding of trade based money laundering and sanctions risks. Such training utilizes appropriate guidance from regulators and industry bodies like the Wolfsberg Group, APG, etc.
• Making use of relevant FATF, regulatory and industry publications to raise awareness of emerging risks amongst relevant staff.

V. Assurance:

• Ensuring regular, periodic quality assurance work is conducted by suitably qualified and experienced staff who assess the judgments made in relation to trade-based money laundering risk and potentially suspicious transactions.
• Where possible, conducting a review to ensure that all red flag controls at the preprocessing stage are working effectively.
• Expertise in trade-based money laundering also being held in a department outside of the trade finance business (e.g. compliance) so that independent decisions can be made in relation to further investigations.
11. Conclusion:

The importance of having and implementing an effective AML program is not just about meeting the regulatory obligations. It also very much impacts the personal lives of many innocent people; these assessments as we all know in general is one or all of the following – Consent orders, fines, criminal charges, prison sentence, closure of business, removal of license to operate as an individual or business and damage to reputation.

The AMLSCU needs to enhance its financial information sharing capability to support cooperative efforts with counterpart FIUs. Law enforcement and customs officials should conduct more thorough inquiries into large declared and undeclared cash imports into the country, as well as enforce outbound declarations of cash and gold utilizing existing smuggling laws.

It is recommended that banks follow a “3 layers of defense approach” that encompasses business operations, oversight, and audit controls, to appropriately cover a multitude of TBML risks:

The first line of defence is described by the Basel Committee on Banking Supervision as the business line management and staff who are generally responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which they are accountable.

The second line of defence is generally limited to independent challenge of the business function’s inputs to, and outputs from, the risk and compliance management framework for identifying, managing, measuring and reporting risks.

Internal audit function as the responsible party for the third line of defence which review the trade finance related activities to a certain extent, usually as part of their overall credit processes. However, internal audit reviews that specifically test the effectiveness of internal controls for managing TBML risks are not typically carried out.

Solution must be some comprehensive analytics and reporting that enables views of concentrated risk across entire, or components of, trade portfolios. It should be a monitoring solution that highlights potentially suspicious activity at the individual deal or transaction level.

A platform is required to monitor, screen and provide analytics which enable financial institutions to:

- Alert stakeholders when problems arise
- Improve financial crimes risk management across the program
- Automate flagging of unusual activity against Trade AML typologies
- Standardize programs with affiliates and correspondents
- Identify sanctions risks (including seaports) beyond customary screening systems
- Avail International Maritime Bureau (IMB) report, to know the genuineness of the trade transaction.
- Establish a global bank-wide repository of all critical issues to both improve your business and compliance
- Internal systems to capture past and usual behaviour and therefore be alerted to unusual customer behaviour
- Communication between operations and front office, or those in the FI’s who have the most complete understanding of the customer’s expected behaviour.
- Provide the ability to screen SWIFT messages from four different perspectives: a) Sanctions Screening, b) Non-standard clauses, c) Mismatching with key Trade Parties and d) Non-Trade related SWIFT messages
- Interface with the institution’s existing Case Management Tool
- Improve customer due diligence and Identifies trade activity out of pattern with existing KYC customer profiles

Investigator can review Violation Rules Vigilance (VRV) alerts on system and take appropriate action to mitigate money laundering risk such as approach to International Maritime Bureau (IMB) report, to know the genuineness of the trade transaction and senior management should understand the need to interface with the institution’s case management system.

An approach must realize the necessity of random sampling, and to provide reports and dashboards reporting for investigators for further.

A robust solution is needed to recognize the importance of key fields in monitoring and screening high-risk trade activities, such as set some rules (scenarios) in system for trade finance transactions which can cover high risk transactions and amendments.

**The Use of Data Analytics to Identify TBML:**

Financial institutions have been leveraging a range of traditional analytical techniques to identify potential money laundering activities. These existing techniques can be applied to monitor TBML specific typologies and Funnel Accounts:

**Rules Engines:** These are used to execute algorithms built as business rules to check volume, velocity, and variance in transactions. Such business rules can also be executed in-line with more advanced modeling techniques such as customer profiling, account profiling, peer comparison, and text analysis to detect behavioral anomalies.

**Profile and Trend Analysis:** These statistical tools can be used to accumulate transaction data into a predictive profile, established to serve as the baseline behavior of a customer and/or accounts, historical transactions and seasonal trends into a condensed, easily accessible profile to identify changes in transaction patterns, customer relationships, deviation from expected behavior and many more.
**Sequence Mining:** A form of data mining where the system is looking for a defined sequence of events, which can indicate wrong-doing (such as the sequence described in flow through of funds typology). For the detection of TBML, such sequence analysis is expected to expand to cover new typologies and identify new sequences, i.e. multiple shipment requests from a single customer or address, etc.

**Link Analysis:** A technique used to identify hidden relationships between seemingly unrelated parties by detecting common links in both static (reference) or transaction data.

Some of the newer analytical techniques used in the analysis of semi-structured or unstructured datasets include:

**Text Analytics and Text Mining:** This method involves the use of natural language processing combined with statistical and machine learning techniques to model and structure information from textual sources to derive high quality information.

**Big Data Analytics:** Big Data is usually characterized by one or more of the following: high volume, high velocity, or high variety data. Given that Trade Finance data comes from a variety of internal and external sources in multiple formats, and given the unstructured format of that data, big data analytics brings versatility to the data consumption process.

**Enhancing Reference Databases:** Gaining access to a library of industries, products, channels, vessel names, dual use goods, high-risk countries, ports, etc. will bring greater accuracy to monitoring and efficiency to analysis of the money laundering activity. These lists can be bought from external list consolidators and can also be managed internally by leveraging advanced tools to enhance data availability and versatility.

**Advanced Statistical Analytics:** A process of quantitatively describing the main features in a dataset, which can, through mathematical models, be compared against global or regional benchmarks for congruence (or lack thereof).

**Predictive Analytics:** Advanced statistical models can help banks anticipate possible future outcomes and the likelihood of wrongdoing based on the detection of indicative parameters or a specific pattern.

**Web Analytics:** Web crawling software can be used to download relevant web pages matching specific search terms and criteria, (i.e. container details, negative news, etc.) to indicate TBML acts. Such techniques can also be used to gather social media data to be later used for the purpose of link-analysis and the detection of networks and related parties.
**Image Analytics:** Converting hardcopy documents to consumable formats to reduce the effort of gathering and structuring data

Financial institutions are encouraged to take incremental steps towards automation, through progressive enhancement of each of the key areas discussed in this article – from improving KYC and CDD processes through enhancement of screening tools, list management capabilities, the availability of data, advanced analytics, and obviously investment in training of the FI’s last line of defense – it is human capital, front and middle office employees.

Financial institution should consider itself at the Leading Phase of the maturity spectrum only when it has completed trade finance related data consolidation within its financial crimes data-mart across the enterprise, allowing it to run predictive analytics capabilities and screening both pre and post-transaction as well as across the entire trade finance lifecycle. The different systems used for TBML and AML monitoring are capable of sharing ‘trigger events’ seamlessly.

Finally, banks at this maturity level have a specialized TBML team in place, able to appropriately review any exception report generated and truly understand the business reasoning behind business agreements and import/export engagements. A bank at this stage has successfully optimized the balance between people, processes, and technology.

No matter which phase the financial institution is in, countering TBML risks with a consolidated and sophisticated detection system is the key to success. Predictive analysis and machine learning are no longer ‘techniques of the future’ – innovative institutions are implementing these techniques today to stay ahead of the competition... and the criminals.
12. References:

2. https://atlas.media.mit.edu/en/profile/country/are/
6. https://www.moneylaunderingbulletin.com/legalandregulatory/cases/?pageNo=2
15. https://www.interpol.int/