مصرف البحرين المركزي
Central Bank of Bahrain

TRADE BASED MONEY LAUNDERING

GUIDANCE FOR FINANCIAL INSTITUTIONS

FEBRUARY 2023

Contents

I. PURPOSE, SCOPE, AND APPLICABILITY

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. Using the cover of trade is an attractive method for money laundering and terrorist financing due to the sheer size of the trade mechanisms worldwide and the continuing introduction of new products to reduce supply line costs.

This guidance paper issued by the Central Bank of Bahrain ("CBB") should be read in conjunction with local regulations and international standards. The guidance included in this paper applies to all licensees regulated and supervised by the CBB.

This paper aims to provide guidance to assist financial institutions in understanding trade-based money laundering and the means of identifying suspicious activity associated with trade-based money laundering.

This guidance paper was developed by consolidating relevant information applicable to financial institutions included in guidance papers and typologies, including:

- MENA FCCG and the Global Coalition to Fight Financial Crime (GCFFC) MENA Chapter - **'Trade Based Financial Crime (TBFC) Reference Guide'** issued in October 2022
- Financial Action Task Force **- 'Trade Based Money Laundering – Risk Indicators'** issued in March 2021;
- Financial Action Task Force - **'Trade Based Money Laundering – Trends and Developments'** issued in December 2020;
- Financial Action Task Force - **'APG Typology Report on Trade Based Money Laundering'** issued in July 2012; and
- Financial Action Task Force - **'Trade-Based Money Laundering'** – issued in June 2006.

In summary, this paper outlines the process, trends and challenges of trade-based money laundering and touches on Trade-Based Terrorist Financing and services-based money laundering. The paper also includes risk indicators to help financial institutions identify potential suspicious activity associated with trade-based money laundering. Additionally, the paper covers measures and best practices to counter trade-based money laundering.

II. UNDERSTANDING TRADE-BASED MONEY LAUNDERING

- The Financial Action Task Force (FATF) recognised the misuse of the trade system as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. This method of money laundering (ML) is based upon abuse of trade transactions and their financing. As the anti-money laundering (AML) and counter-terrorist financing (CFT) standards that have been applied to other money laundering techniques (i.e., misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling)) have become increasingly effective, such abuse of trade finance and the trade system has become progressively attractive to money launderers and terrorist financiers.

- The term **trade finance** refers to the financial component of an international trade transaction (i.e., managing the payment for goods and related services being imported or exported). Trade finance activities may involve, among other things, managing payments for open account trading, or issuing letters of credit, standby letters of credit and guarantees.

- **Trade-Based Money Laundering (TBML)** is defined as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities".

- In summary, the primary aim of any TBML scheme is the deliberate movement of illicit proceeds through the exploitation of trade transactions. In doing so, criminals may engage in a range of other potentially unlawful activities through the misrepresentation of the price, quantity or quality of imports or exports by methods such as preparing false invoices, mischaracterizing goods to circumvent controls, and other customs and tax violations. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail. But the aim of TBML – unlike trade-related predicate offences – is not the movement of goods, but rather the movement of money, which the trade transactions facilitate.

- Another key distinction of TBML schemes is the involvement of Professional Money Launderers (PMLs). Whereas criminals perpetrating trade-related predicate offences are usually the ultimate beneficiaries of those illicit proceeds, PMLs offer specialist expertise using a range of ML techniques (e.g. TBML) to diversify their risk exposure. These PMLs take receipt of the criminal proceeds on behalf of the Organised Criminal Groups (OCGs) and transfer or convert those proceeds, including via TBML schemes, before passing them back to the OCG, minus the payment of their fee or commission.

III. THE TRADE FINANCE ENVIRONMENT

- 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.

- The vast number of trade transactions produces a high level of 'noise' about the level of legitimate trade, and the increased flexibility of the processes masks the criminal ML activity. In order to better understand how TBML operates, it is necessary to understand the environment in which it operates. By understanding this environment, the financial institution (FI) can better recognise the 'red flags' that help peel away the layer considered paramount by money launderers and terrorist financiers in achieving their goals as a result of all the 'noise' of legitimate trade.

- International trade involves a range of risks for the parties involved, which leads to uncertainty over the timing of payments between the exporter and importer. This creates tension along the supply chain, which can have negative consequences for both the importer and exporter. Trade processes and financing have adapted to address this tension, while still supporting the growth of the global marketplace.

- There are a variety of trade financing instruments used, including open accounts, documentary collections and letters of credit (which are summarised below) as well as consignment and cash in advance. It is important to note that this is by no means an exhaustive list but is provided to ensure a basic level of understanding. As such, research has noted that open account and documentary collections are the most prominent methods of payment for international transactions that have been used for TBML.[1]

  - ***Open Account:***

    The United Nation's Trade Facilitation Implementation Guide notes that an "open account transaction is a sale where the goods are shipped and delivered before payment is due". Payment is usually made by a set time period, anywhere between 30 and 90 days after receipt of the goods or services. TBML schemes frequently involve this method because FIs have a reduced role, meaning less oversight than for the documentary collection process. FIs can struggle to accurately or consistently assess the legitimacy of the customer's operations, whether through automated or manual transaction monitoring.

    Such a payment method creates a disconnect between the trade movement and the funds used to finance such a trade. This disconnect is then exploited by OCGs, PMLs or terrorist

[1] https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

financiers, using specific loopholes or gaps, in a compartmentalised fashion, mitigating their risk exposure. Further complexity can be added by using third-party intermediaries in multiple jurisdictions to frustrate law enforcement or FI detection and disruption.

- ***Documentary Collections:***

  In a Documentary Collections transaction, the exporter's and the importer's banks facilitate the export sale by exchanging shipping documents for payment. More specifically, the exporter requests payment by presenting shipping and collection documents for the traded goods to its FI. The FI then forwards these documents to the importer's FI, who then transfers the funds to the exporter's FI, who will subsequently credit those funds to the exporter.

  Documents are not always standardised, increasing the risk of TBML exploitation through fictitious or false invoicing. However, when these documents can be checked and assured, certain data points can be used to spot TBML, including:

  - Use of a personal email address in lieu of a legitimate business email;
  - Subject to an FI's data storage capabilities, the obvious recycling of previous documentation with few or no edits, including something as basic as the date; and
  - The complete lack of any trading presence of the exporter, following research by the FI. This included the use of residential rather than business premises for exporters providing significant quantities of goods.

(For further TBML red flag indicators, refer to Section VI: Risk Indicators)

- ***Letters of Credit:***

  A letter of credit (LC) is a precise document whereby the importer's bank extends credit to the importer and assumes responsibility in paying the exporter. More specifically, the importer's bank, at the request of importer, pays a named beneficiary a specified amount of money upon presentation of specified documents set out in the terms and conditions of the letter of credit.

  The documentary credit arrangement offers an internationally recognised and used method of attaining a commercially acceptable undertaking by providing for payment to be made against presentation of documentation representing the goods, making possible the transfer of title to those goods. However, even in this simple form the true value of goods transferred between countries can be masked through misrepresentation of price, quantity and quality. Letters of Credit may be generated to create a veneer. The

documentation generated in the process leaves a paper trail which money launderer may rely upon to disguise illegal proceeds.

IV. TRENDS AND DEVELOPMENTS OF TRADE-BASED MONEY LAUNDERING

- Criminals exploit sectors, products, or businesses prone to gaps in, or the inconsistent application of, customer due diligence and know your customer processes across jurisdictions, which can be aggravated by a limited understanding of TBML risk. This section discusses the trends regarding the economic sectors, products and businesses that are more likely to be vulnerable to TBML activity. This should not be considered as a definitive list and is primarily provided to give an overview of the current risk and the diversity of the sectors and products exploited.

I. Types of Economic Sectors and Products

- A wide range of economic sectors are vulnerable to TBML, meaning both high-value, low-volume sectors or products (such as precious metals) and low-value, high-volume sectors or products (such as second-hand textiles) can be exploited by criminals to launder the proceeds of crime. Despite this variety in sectors, a handful of common themes conducive to TBML exploitation were identified:

  - Goods with wide pricing margins;
  - Goods with extended trade cycles (i.e., shipping across multiple jurisdictions); and
  - Goods which are difficult for customs authorities to examine.

- Supply chains moving lower-value goods are most at risk to end-to end ownership by a criminal organisation or PML network. The set-up costs can be considerably lower than supply chains moving higher-value goods and may not attract the same level of scrutiny by authorities across the supply chain. An additional benefit of exploiting these products is the scope for supplying multiple markets across different jurisdictions[23]. This also helps mitigate the risk of alerting authorities or regulated firms to any suspicions of market saturation – e.g. it wouldn't necessarily be suspicious if a particular lower-value product, such as clothing, is repeatedly shipped to the same destination. These factors create a suitable environment for the continued use of common TBML techniques. For example, a criminal organisation may execute legitimate shipments of cosmetic goods, creating enough valid documentation to allow for subsequent phantom shipments and misuse of that previous documentation. In some

[22] These products are also usually in high demand – for example, cheap clothing – which can create the veneer of legitimacy for a TBML network.

[3] [3] https://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

instances, the transactions remained entirely legitimate (so none of the common TBML techniques were used), but the product shipped had almost no value as a saleable good and is literally dumped once it arrived – e.g. second-hand textiles *(For further examples, refer to Section III. Common Trade-Based Money Laundering Techniques).*

- When OCGs or PMLs exploit higher-value products, they are more likely to do so through the penetration and subsequent misuse of established supply chains. OCGs or PMLs may leverage an existing company struggling with a cash flow problem, they buy their way in as a 'silent partner' and use the business and its supply chain contacts to launder the proceeds of crime. This infiltration of legitimate businesses is covered in further detail below.

Gold, precious metals, and minerals

- The exploitation of gold and other precious metals and minerals is often a factor in TBML schemes, including the use of gold as an alternative form of value within the ML process – i.e., not just a commodity to exploit in moving value, but also a proxy for cash. The association with illegal mining activity creates additional issues such as systematic breaches of health and safety standards, other forms of worker exploitation, and substantial environmental problems.

Auto parts and vehicles

- Numerous TBML schemes describe the exploitation of auto parts or vehicles, including trade in second-hand cars or luxury vehicles. One scheme included the transportation of damaged cars from one jurisdiction to another, with a legitimate market in place for onward sale, following repair of the vehicle. The OCGs were appropriately declaring the right price at the point of export but were declaring a considerably lower-value at transshipment points. This was despite the market for damaged cars being relatively transparent and the sale of vehicles close to their undamaged price. To further frustrate law enforcement authorities, the OCG routed payments through an entirely different network of companies located in alternate jurisdictions.

Agricultural products and foodstuffs

- TBML schemes also noted the exploitation of agricultural products, including the abuse of food supply chains involving highly perishable items such as fresh fruit and vegetables. These are good examples of low-value, high-volume products that are not necessarily affected by market saturation given their perishability. OCGs and PMLs penetrate these legitimate supply chains and use them as a means of introducing illicit cash into the financial system. They do not use any of the common TBML techniques, instead they exploit these legitimate supply chains to move their criminal proceeds to different jurisdictions.

Clothing and second-hand textiles

- As with foodstuffs, clothing and second-hand textiles are a compelling example of a low-value, high-volume product that allows for an extended supply chain, making them attractive for exploitation in TBML schemes. The extreme price variability also makes it attractive in terms of mis-description of the price to support the laundering activity.

Portable electronics

- Portable or handheld electronics (mobile phones, laptops, etc.) are also attractive in TBML schemes as they can be deliberately misrepresented and incorrectly valued, increasing the opportunity to move significant criminal proceeds.

- In addition to the sectors and products mentioned above, TBML exploitation also occurs in the following sectors: construction materials (lumber), plant machinery, scrap metal dealers, fuel and energy products, and alcoholic or soft drinks.

II. Types of Businesses

- As with sectors and products, the types of businesses at risk of TBML exploitation are varied. Small or medium-sized businesses are often featured in multiple TBML schemes, but previous international investigations involved large multinational companies, often through overseas subsidiaries that have more fluid trading relationships in distributing products into newer markets. The below paragraph provides insight into how shell and front companies are commonly used by criminals as a tool in TBML schemes.

Shell and front companies

- The exploitation of shell and front companies has become a key feature of many different types of ML activity, as well as facilitating a significant number of predicate offences. While there is often a significant intersection between TBML/TF schemes and the exploitation of shell or front companies, they do not feature in all TBML/TF schemes, particularly those involving exploitation of legitimate supply chains. However, some OCGs, PMLs and terrorist financiers do construct their TBML scheme around shell companies or involve them as part of the financial settlement process, anonymising the ultimate beneficial owner to maximum effect. In turn, front companies offer convenient opportunities to integrate physical cash into a business and then exploit its banking relationships to move the cash across jurisdictions.

III. Common Trade-Based Money Laundering Techniques

- **Over- and under- invoicing of goods and services:** The key element of this technique is the misrepresentation of the price of the goods or services, in order to transfer value. In this type of arrangement, the critical enabling aspect is that the importer and exporter are complicit in the misrepresentation.

- **Over- and under- shipment of goods and services:** As above, this involves the misrepresentation of the quantity of goods or services, including 'phantom shipments' where no product is moved at all. Again, it relies on collusion between the importer and exporter.

- **Multiple invoicing of goods and services:** This doesn't require the misrepresentation of the price; rather it centres on the reuse of existing documentation to justify multiple payments for the same shipment of goods or delivery of services. Criminals or terrorist financiers exploit this further by reusing these documents across multiple FIs, making it difficult for one institution to identify it.

- **Falsely described goods and services:** This involves the misrepresentation of the quality or type of a goods or services, such as the shipment of a relatively inexpensive good, which is described as a more expensive item, or an entirely different item, to justify value movement.

- While these techniques are listed independently, in practice criminals can mix these methods in one scheme, further complicating the transaction chain. For example, more sophisticated ML networks may use phantom shipping in conjunction with multiple invoices. One shipment may involve the movement of actual goods to create a veneer of legitimacy, or to test customs compliance processes, with subsequent trading may use multiple invoices for phantom shipments, serving as a cover for the transfer of funds.

- These techniques are still prevalent today. However, other trends are emerging, including the exploitation of legitimate supply chains that operate without the collusion between importer and exporter, or the introduction of criminal cash into trade transactions, including the growth of surrogate shopping.

IV. Common Trade-Based Money Laundering Methods of Financial Settlement

A. Illicit cash integration

- ***Exploitation of other types of FIs:*** While a substantial amount of TBML cash integration involved banks, OCGs and PMLs can also exploit other types of FIs, including money value transfer services (MVTS). For example, conspirators involved in a false invoicing TBML scheme have used MVTS to facilitate payment for the

goods, rather than attempt payment via a bank. The OCGs or PMLs perceive the MVTS sector to have a less developed understanding of TBML, so the MVTS would not question why it is facilitating a business payment of a significant amount rather than the payee using a more appropriate method.

- ***Surrogate shopping networks:*** Surrogate shopping networks involve individuals or networks of shoppers purchasing desired goods on behalf of wealthier individuals, ostensibly to circumvent customs controls or other forms of tariff restrictions. Some shoppers may also make purchases on behalf of OCGs to distance them from the asset, suggesting the surrogate shopper has at least some knowledge that what they are doing is on behalf of an OCG. This type of activity has been exploited as part of TBML schemes internationally, whereby OCGs or PMLs provide local currency (the proceeds of crime) to these surrogate shoppers, who pay for desirable goods that are transported to another jurisdiction and passed to the OCG or PML.

  An adaptation of this scheme involves the surrogate shopper paying for the requested goods using credit cards, and the OCG or PML settling their debt using the proceeds of crime. For example, students were making multiple purchases of portable electronics, such as smart phones and tablets. Their credit card balances were subsequently settled via electronic funds from companies suspected of laundering the proceeds of drug trafficking. Not only did this allow for the laundering of criminal proceeds, but the electronics were suspected of being sent for onward sale into grey markets in Asia and the Middle East. This process can be used with the traditional TBML techniques, including the misrepresentation of the goods purchased, to increase the margins of the proceeds of crime transferred as payment.

- ***Infiltration of legitimate supply chains:*** In this case, an OCG or PML purchases a stake in a legitimate business, which may or may not be struggling financially, and continues using its supply chain as a method of integrating illicit cash into the financial system. The OCGs or PMLs do not attempt to change the business practices of the company they've invested in, nor do they necessarily introduce any of the common TBML techniques referenced previously. Instead, their aim is a slow and steady increase of introducing illicit cash into the business, while maintaining those existing supply chain relationships.

B. Third-party intermediaries facilitating invoice settlement

- Third-party intermediaries often appear as part of the invoice settlement process and are often associated with the exploitation of open account trading, because of the lack of oversight by FIs. They can serve a dual purpose, depending on where in the chain the OCG or PML is involved. For example, in penetrating legitimate supply chains

and sourcing goods without any misrepresentation, the OCG may pay for those goods by involving a previously unknown third-party (usually the company responsible for integrating criminal cash) into the transaction.

C. Trade-based terrorist financing

- What made TBML schemes attractive in moving value, offered the same opportunities to terrorist financiers. Trade-Based Terrorist Financing (TBTF) uses the same trade processes as TBML but has a significant and fundamental difference – proceeds or value moved can come from both legitimate and illegitimate sources, increasing the complexity in detecting and disrupting TBTF. As such, TBTF is defined as "disguising the movement of value through the use of trade transactions in an attempt to finance terrorism, whether from legitimate or illegitimate sources". In practice, TBTF schemes can and do rely on common TBML techniques. They can also feature legitimate firms and transactions right through the supply chain, until the funds are eventually diverted to terrorist organisations.

D. Services-based money laundering

- Services-based money laundering (SBML) is not TBML, however it is included here for reference as it is recognised as an increasing risk. The fundamental difference between the two is that SBML schemes rely on exploiting the trade in services or other intangibles to disguise and justify the movement of illicit proceeds. The schemes can create further complexity for FIs to successfully detect and disrupt ML. The following services and sectors were identified as vulnerable to SBML:

  - Gambling, particularly online gambling service providers;
  - Software providers, including gaming and business software, such as electronic point of sale services;
  - Financial services, including virtual asset wealth management;
  - Consultancy and advisory services; and
  - Trademarks and similar intangible items such as intellectual property rights.

V. CHALLENGES OF TRADE-BASED MONEY LAUNDERING

- TBML is a particularly complex form of ML that causes various difficulties at each stage of the investigative and detection processes. These difficulties have led to a relatively low number of successful TBML investigations across the globe so far.

- Lack of understanding and awareness of TBML is one of the biggest challenges of trade-based money laundering. As knowledge of TBML increases globally, criminals are constantly seeking new opportunities to legitimise criminal proceeds through the misuse of the international trade system. One of the factors underlying these challenges is the relative complexity of TBML schemes. They can involve a multitude of sectors and commodities exploited as a means of moving value, from second-hand cars to flowers, meaning no one scheme is like another. A growing number of online business opportunities has opened new horizons for international trade. At the same time, it has also created additional challenges to the understanding of TBML methods. New technologies and the digitalisation of trade allow for an increased speed of trade operations, which in turn requires FIs to develop knowledge and analyse data in order to identify suspicious trade and financial transactions among the thousands of legitimate transactions in a timely manner.

- FIs are often on the forefront of the fight against ML, since they are involved in moving value (e.g. by executing transactions on behalf of their clients). At the same time, being on the front lines against ML and TF creates significant challenges for FIs, as criminals constantly improve their ML methods and FIs must keep pace. It also should be noted that most trade and production chain companies do not have similar reporting obligations under the FATF Recommendations (unless they fall within the scope of business activities such as dealers in precious metals or stones), nor do they typically fall under the domestic legal framework of many jurisdictions, which places the duty on FIs to detect potential instances of such activities and appropriately advise the relevant competent authorities in a timely manner.

- TBML is highly adaptive and can exploit any sector or commodity, making it difficult for FIs to prioritise resources and translate the latest insights into the business rules and compliance systems. In practice, TBML schemes can consist of a large number of front companies, with funds transmitted between several banks, meaning each of the involved FIs can see only a small part of the network. This fragmentation of TBML schemes makes it inevitably difficult for FIs to identify potential TBML schemes based on the analysis of the whole chain, and in many cases limits their ability to detect discrepancies in supplementary documentation and customer profiles.

- Another challenge faced by FIs is the verification of information provided by their non-resident customers. This can be an issue for all types of ML, when a lack of a public registry can present difficulties for FIs trying to verify an address, income, or other client-related data. TBML schemes only exacerbate these challenges. During the due diligence process for a trade transaction, for example, a client might submit a copy of the invoice, contract, or other supplemental documents to the bank to justify the transfer of funds from one jurisdiction to another. If the bank has problems accessing customs data, it will not be able to promptly verify, amongst other things, the authenticity of the documents, whether the goods have been actually shipped, and whether their quantity and description match the contract.

- Many TBML techniques require both the buyer and the seller to be complicit, sometimes meaning that the same person or a group of persons execute control over the different parties of a transaction. In this case, obtaining information about the beneficial owners of the customer's counterparties may assist the FI in detecting TBML. However, such information may not be available, for example if the counterparty has never been a customer of that FI or if there is no public registry of beneficial owner information available. The counterparty may also be incorporated in a jurisdiction other than the one in which the FI executing payment is registered, further complicating the FI's efforts to collect this information.

- Another re-occurring challenge faced by FIs in identifying TBML schemes is estimating the "fair price" of a traded commodity. This challenge is particularly relevant for TBML schemes using the over-/and under-pricing technique. FIs often have only a vague description of the traded good, and establishing a "fair price" can require significant resources and may be based solely on open source information. In addition, some of the commodities used by criminals are not traded in public markets and there are accordingly no benchmark prices available.

- Moreover, because TBML involves international trade, the documentation provided to FIs is often in different formats and languages, meaning that verification will likely be done manually. This requires FIs to devote additional time and resources, including hiring highly qualified staff, what may be more difficult for smaller FIs with more limited compliance budgets. In this context, paying methods like letters of credit or documentary collection require customers to provide the FI with more documentation than open-account trade. Thus, money launderers may see open account trade as more attractive because the FI has very limited oversight of the transaction. At the same time, even when an FI suspects its customer being involved in TBML and terminates relationships with them, the customer may still be able to open a new account in another bank.

VI. RISK INDICATORS

- A risk indicator demonstrates or suggests the likelihood of the occurrence of unusual or suspicious activity. The risk indicators detailed below are designed to enhance the ability of FIs to identify suspicious activity associated with this form of money laundering. By no means is this a conclusive list. The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of TBML, nor will the indicator necessarily provide a clear indication of such activity, but it could prompt further monitoring and examination, as appropriate. Similarly, the occurrence of several indicators could also warrant closer examination. TBML indicators are also dependent on the business lines, products or services that an FI offers; how it interacts with its customers; and on the FI's human and technological resources.

I. Structural Risk Indicators

- The corporate structure of a trade entity appears unusually complex and illogical, such as the involvement of shell companies or companies registered in high-risk jurisdictions.
- A trade entity is registered or has offices in a jurisdiction with weak AML/CFT compliance.
- A trade entity is registered at an address that is likely to be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.[4]
- The business activity of a trade entity does not appear to be appropriate for the stated address, (e.g. a trade entity appears to use residential properties, without having a commercial or industrial space, with no reasonable explanation).
- A trade entity lacks an online presence, or the online presence suggests business activity inconsistent with the stated line of business, e.g. the website of a trade entity contains mainly standardised material taken from other websites or the website indicates a lack of knowledge regarding the particular product or industry in which the entity is trading.
- A trade entity displays a notable lack of typical business activities, e.g. it lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances.
- Owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners, e.g. they lack experience in business management or lack knowledge of transaction details, or they manage multiple companies.
- A trade entity, or its owners or senior managers, appear in negative news, e.g. past money laundering schemes, fraud, tax evasion, other criminal activities, or ongoing or past investigations or convictions.

[4] This may also include the address of a trust and company service provider that manages a number of shell companies on behalf of its customers

- A trade entity maintains a minimal number of working staff, inconsistent with its volume of traded commodities.
- The name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it, potentially in an effort to appear as part of the corporation, even though it is not actually connected to it.
- A trade entity has unexplained periods of dormancy.
- An entity is not compliant with regular business obligations, such as filing VAT returns.

II. Trade Activity Risk Indicators

- Trade activity is inconsistent with the stated line of business of the entities involved, e.g., a car dealer is exporting clothing, or a precious metals dealer is importing seafood.
- A trade entity engages in complex trade deals involving numerous third-party intermediaries in incongruent lines of business.
- A trade entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
- A trade entity makes unconventional or overly complex use of financial products, e.g. use of letters of credit for unusually long or frequently extended periods without any apparent reason, intermingling of different types of trade finance products for different segments of trade transactions.
- A trade entity consistently displays unreasonably low profit margins in its trade transactions, e.g. importing wholesale commodities at or above retail value, or reselling commodities at the same or below purchase price.
- A trade entity purchases commodities, allegedly on its own account, but the purchases clearly exceed the economic capabilities of the entity, e.g. the transactions are financed through sudden influxes of cash deposits or third-party transfers to the entity's accounts.
- A newly formed or recently re-activated trade entity engages in high-volume and high-value trade activity, e.g. an unknown entity suddenly appears and engages in trade activities in sectors with high barriers to market entry.

III. Trade Document and Commodity Risk Indicators

- Inconsistencies across contracts, invoices or other trade documents, e.g. contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.
- Contracts, invoices, or other trade documents display fees or prices that do not seem to be in line with commercial considerations, are inconsistent with market value, or significantly fluctuate from previous comparable transactions.

- Contracts, invoices, or other trade documents have vague descriptions of the traded commodities, e.g. the subject of the contract is only described generically or non-specifically.
- Trade or customs documents supporting the transaction are missing, appear to be counterfeits, include false or misleading information, are a resubmission of previously rejected documents, or are frequently modified or amended.
- Contracts supporting complex or regular trade transactions appear to be unusually simple, e.g. they follow a "sample contract" structure available on the Internet.
- Shipments of commodities are routed through a number of jurisdictions without economic or commercial justification.

IV. Account and Transaction Activity Risk Indicators

- A trade entity makes very late changes to payment arrangements for the transaction, e.g. the entity redirects payment to a previously unknown entity at the very last moment, or the entity requests changes to the scheduled payment date or payment amount.
- An account displays an unexpectedly high number or value of transactions that are inconsistent with the stated business activity of the client.
- An account of a trade entity appears to be a "pay-through" or "transit" account with a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons, including:
  - An account displays frequent deposits in cash which are subsequently transferred to persons or entities in free trade zones or offshore jurisdictions without a business relationship to the account holder.
  - Incoming wire transfers to a trade-related account are split and forwarded to nonrelated multiple accounts that have little or no connection to commercial activity.
- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g. by a shell or front company not involved in the trade transaction.
- Transaction activity associated with a trade entity increases in volume quickly and significantly, and then goes dormant after a short period of time.
- Payments are sent or received in large round amounts for trade in sectors where this is deemed as unusual.
- Payments are routed in a circle – funds are sent out from one country and received back in the same country, after passing through another country or countries.

- It is important to note that if a customer meets one or more of the above risk indicators it does not mean it is being used in a TBML scheme. Further analysis is recommended to offset the risk of false positives.

VII. BEST PRACTICES

- The MENA FCCG, in collaboration with the Global Coalition to Fight Financial Crime (GCFFC) MENA Chapter, issued a paper in October 2022: 'Trade Based Financial Crime - Middle East and North Africa: A reference guide for the anti-financial crime community'[5], which detailed recommended responses by FIs to fight against Trade Based Financial Crime (TBFC).

- There are a number of measures Financial Institutions can take to enhance their control framework which will assist in the identification and mitigation of TBFC. As per the reference guide, a number of these are outlined below.

I. Risk Assessments

- There are several ways to carry out a risk assessment with the "convention/standard methodology" being the most widely used approach. The risk assessment should cover the entire financial institution's business, though it may be conducted in sections or as part of a continuous exercise, with a focus on separate lines of business, sub sets of products, geographies and/or legal entities. *(For more detailed guidance, refer to the Section VI: Risk Indicators, and the Guidance Paper: Risk Assessments, published by the CBB in October 2021).*

II. Customer Due Diligence

- A key control to mitigate against TBFC is the customer due diligence (CDD), or know your customer (KYC), process. An understanding of the customer and their expected activity enables Financial Institutions to not only service their customers better but also enables them to undertake comprehensive monitoring with a view of identifying TBFC.

- While a financial institution is not expected to do due diligence on the customer of a customer, there are situations where a financial institution must undertake a degree of due diligence regarding a party that is neither its customer nor a correspondent bank. Typically, such situations arise where the financial institution is affecting a transaction and it is appropriate in that context that the financial institution obtains information on the correspondent bank's customer. Due diligence of a customer's customer is also common in supply chain finance and with receivables finance counterparties. A common level of diligence for such parties would be a customer identification program analysis and a negative news check.

5 https://www.gcffc.org/wp-content/uploads/2022/10/English-Trade-Based-Financial-Crime-in-the-Middle-East-and-North-Africa_.pdf

III. Sanction Screening

- The industry standard to mitigate sanctions risk is to undertake screening of the details available to the financial institution, whether at the time of on-boarding of customers, at the time of transfer of funds, or on an ongoing basis. This control, whether manual or automated, should be designed in such a way as to assist with the identification of sanctioned individuals and organisations. When automated, the process requires proper governance and appropriate list management, supported by meaningful information and ongoing validation, testing and tuning.

- Sanction screening is the comparison of customers and transactions against government-issued lists of names; these lists are often supplied and maintained through external vendors. Through their own assessment and research, Financial Institutions may also augment these with additional criteria that are relevant to sanctions, including terms and phrases.

IV. Transaction Monitoring

- Transactions are usually monitored through automated systems that examine transactions periodically or in real time according to the nature of the transactions or inherent risks against a suite of scenarios that assess each transaction against a set of parameters or thresholds; there also may be scenarios that aggregate the payment data to make an assessment. Along with the expectation for Financial Institutions to mitigate TBFC, there is a regulatory requirement to report suspicious transactions that may indicate crimes such as money laundering, terrorist financing, and tax evasion to the relevant authorities, in line with local laws and regulations.

- A financial institution must continuously fine-tune the full suite of scenarios based on its own risk appetite, which may differ between their customer portfolios. This form of transaction monitoring—assessing each transaction on a per-transaction basis—does not assess the holistic activity of a client, and therefore can result in the generation of numerous false positive alerts that require resources to clear.

- Different customer sets or types require different monitoring; for example, retail customers should have a different set of scenarios and thresholds than corporate customers, as their pattern of activity and transaction values differ. In terms of specific transactions, wire payments can pose additional challenges when they carry minimal information about the actual transaction.

- Trade finance transaction monitoring may also be undertaken through automation or manually. The information contained within each trade finance document may be assessed against a number of red flags, a process known as "document checking". From a trade finance perspective, a financial institute will be aware that a buyer and supplier have entered into a trade contract. Therefore, if there are discrepancies in a transaction which, having been escalated, have been determined should be rejected and the documents returned, the goods

may still be in transit which will ultimately require payment from the buyer. The financial institute should have controls in place that monitor for open account payments that maybe used to settle the trade transaction.

V. Unusual Transactions

- What constitutes an unusual transaction can vary from client to client, sector to sector, or jurisdiction to jurisdiction. However, transactions that are inconsistent with the client's business strategy or profile (e.g. a construction company that starts purchasing large quantities of luxury cars) or transactions which do not make economic sense (e.g. a customer paying multiple times the market rate for an item) can be unusual transactions that require review and assessment.

- The goal of any business is to generate a profit. Therefore, businesses have an incentive to conduct their trade transactions in the simplest and most efficient way possible to minimise the costs of the transactions, in terms of both time and money, while maximising the benefits. It therefore follows that a transaction designed in an inefficient manner or way that makes little economic sense should face further scrutiny to determine the transaction's structure, if there has been an error, or more importantly, whether the transaction is serving as a vehicle for TBFC.

- When a customer attempts to make a transaction using trade finance products that, based on the documents presented, appears to have discrepancies or does not make economic sense, the financial institution should follow up to assess the validity of the transaction, by way of undertaking a holistic assessment of the activity and, if needed, requesting further information from the customer.