

## HOW DOES GLOBAL TRADE AND RECEIVABLES FINANCE MITIGATE AGAINST PROLIFERATION FINANCING?

### POLICY STATEMENT

**Key message:**

1. The identification of proliferation risk and the shipment of dual use goods for nefarious purposes is extremely challenging for Financial Institutions.
2. Financial Institutions do not have sufficient information and expertise to identify proliferation risk in a single transaction.
3. Co-operation with governments and law enforcement on proliferation typologies is more likely to yield results in identifying this activity.

Implementation: This paper is for industry information and guidance and designed to supplement the ICC/BAFT/Wolfsberg Trade Finance Principles.

Document review: The document will be held under watching brief of the ICC Financial Crime & Policy Group and updated as required.

## How Does Global Trade and Receivables Finance Mitigate against Proliferation Financing?

### Introduction

This paper will consider the application of a risk-based approach to assist Financial Institutions (FIs) in identifying high risk customers and transactions in relation to Proliferation Finance (PF) of Weapons of Mass Destruction (WMD); this includes the consideration of dual use goods (goods that may have both civilian and military purposes). It should be noted that publicly available information about what constitutes the financing of proliferation is limited; much of the research that is available discusses PF indicators which are generic and overlap with other types of financial crime, such as trade based money laundering and terrorist financing; the amount of information that is “actionable” is therefore limited.

Furthermore, whilst trade financed products allow for stronger risk assessments due to its documentary nature, as opposed to clean payments, this will only be at an individual transactional level. FIs rarely have oversight of the entire route of goods, as well as the entire transaction chain and network. As a result, the ultimate end-user is often unknown and assessment related to PF is therefore limited.

This paper has considered information from a number of reliable sources, including the Financial Action task force (FATF), and a table of Proliferation Finance Indicators has been devised (see Annex A<sup>1</sup>). The consideration of the inadvertent financing by FIs of WMD, specifically in relation to terrorist acts, is not within the scope of this paper.

### 1. Background

In the absence of a universally recognised definition of financing of proliferation, this paper has adopted FATF’s 2008<sup>2</sup> definition:

“Proliferation financing refers to: the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations<sup>3</sup>”.

As noted in the above definition, dual use goods (DUGs), which “are items that have commercial and military or proliferation applications”<sup>4</sup>, are important as they are a characteristic of proliferation networks. However, DUGs make it difficult to identify PF due to their ‘dual’ nature. Furthermore, according to FATF, DUGs destined for proliferation use are difficult to identify even when detailed information on a particular good is available, due to specialist knowledge required for the assessment. Due to these complexities involved in identifying DUGs, context is important, such as quantities shipped, counterparty and

<sup>1</sup> Please note that these indicators are not intended as to be utilised as ‘red flags’ by FIs; they support the theoretical content of this paper.

<sup>2</sup> FATF, 2008: Proliferation Financing Report

<sup>3</sup> FATF, 2008: Proliferation Financing Report

<sup>4</sup> The Wolfsberg Group, ICC and BAFT, 2017: Trade Finance Principles

associated entities, and the ultimate end user of goods. The end user of goods is particularly important to highlight as this is something the FI's very rarely have sight of, adding another layer of complexity associated with the identification of DUGs used for proliferation in international trade.

DUGs are a subset of Export Control Lists<sup>5</sup> and there is currently no regulatory requirement or industry standard for Financial Institutions to undertake screening or any form of identification of DUGs. There is also no standard or comprehensive list for DUGs screening. Although there are limited regulatory and industry standards for FI's to undertake screening, it is nevertheless regarded as good practice by the Financial Conduct Authority (FCA), Monetary Authority of Singapore (MAS), and Hong Kong Monetary Authority (HKMA), in terms of financial crime controls for Trade Finance. Interestingly, although HKMA makes specific reference to in flight screening for DUGs, they also state that the assessment of DUGs may require specialist knowledge. Similarly, MAS states that the interpretation of 'dual use' is not practical for a L1 check<sup>6</sup>, as a level of technical knowledge may be required.

Consistent with this, the UK Joint Money Laundering Steering Group states that the "...evaluation of the goods involved in a transaction very often requires a large amount of technical knowledge only available to export controls experts and/or exporters. Goods lists pose a tremendous challenge even for export control enforcement and certainly a greater one for real time screening than entity lists. Furthermore, firms in general lack the expertise to discriminate between legitimate and proliferation-sensitive goods. Goods lists, in themselves, should not be used as a basis for transaction screening, as their limited effectiveness, and greater difficulty, make them an inefficient safeguard"<sup>7</sup>.

These contradictory elements in some regulatory guidance are considered to be more of a hindrance for banks than support as these regulators do not provide a clear path for banks to follow in order to achieve that 'good practice', nor do they clearly define which goods should be considered 'dual use'. This lack of clarity or detailed guidance makes it nearly impossible for banks in these countries to properly address the potential regulatory risks involved. The more so, as they are neither considered nor able to be experts in this extremely complex area.

It is also unclear what exactly the role of regulators in this area is supposed to be, as the enforcement of export control regulations generally falls within the remit of Customs authorities, who have much better oversight over the physical movement of goods in and out of their jurisdictions.

Some Financial Institutions will have some sort of 'DUG' list in place, containing goods descriptions which may indicate dual use goods, which are used by usually Operations staff to assess against the goods descriptions provided with some trade finance transactions (as

---

<sup>5</sup> Export controls are regulations which are "designed to support national and international measures aimed at preventing the proliferation of weapons of mass destruction". This control puts an obligation on the exporter to obtain a license for their goods depending on: 1. Nature of goods due to be exported 2. Destination concerned 3. Ultimate end use of the goods 4. Licensability of trade activities. <https://www2.deloitte.com/uk/en/pages/tax/solutions/export-controls-for-indirect-tax.html>  
<https://www.gov.uk/guidance/beginners-guide-to-export-controls>

<sup>6</sup> A L1 check is the initial review of documents in relation to a trade transaction where an assessment is made based on 'red flags'; any concerns will be escalated onwards (for example, to L2).

<sup>7</sup> [file:///C:/Users/43846014/Downloads/Trade\\_finance%20\(18\).pdf](file:///C:/Users/43846014/Downloads/Trade_finance%20(18).pdf)

is commonly known, most open account trade transactions do not contain any kind of goods descriptions, so mostly we will be referring here to so-called documentary trade transactions, involving either Documentary Letters of Credit or Documentary Collections). Following assessment of a screening 'match', a decision to discount the alert or escalate it to another team is then made. However, this type of list based screening is insufficient to identify true DUGs, including proliferation related activity, primarily due to:

1. The tendency of those involved in this illegal activity to hide, change or otherwise make impossible to identify the actual description of the goods.
2. Heavy reliance on the available goods description, which is problematic as a single good can be described in a number of ways.
3. Extremely high numbers of false positive matches, making the process challenging and time consuming.
4. Requirement of technical expertise to decipher DUG's, knowledge which is often not held by staff in Financial Institutions.

In line with this, Brewer (2018a)<sup>8</sup> notes that identifying PF on the basis of goods or materials involved is not always reliable. According to data compiled by the U.N. Sanctions panel on Iran prior to implementation of the Joint Comprehensive Plan of Action (JCPOA), only circa 10 per cent of shipments to Iran's nuclear or missile programs involved goods listed by multilateral export control regimes as items of specific use in WMD programs<sup>9</sup>. The remainder consisted largely of standard industrial items, where the activity was proliferation-related, but the trade appeared legitimate.

Although FATF (2008) concluded that it was not possible to identify any single financial pattern uniquely associated with proliferation financing, they published a list of 20 indicators of *possible* proliferation financing following an analysis of 25 case studies. These indicators largely reflect evasion techniques which also overlaps with other types of financial crime risk indicators. For example, "customer vague/incomplete on information it provides, resistant to providing additional information when queried", could also be indicative of money laundering and/or terrorist financing, sanctions evasion or fraud.

Following FATF's publication, Brewer (2017) conducted an analysis of 60 case studies involving North Korea, Iran, Syria, and Pakistan, and modified this list, categorising the indicators into one of three categories: 1. Potentially highly indicative 2. Potentially moderately indicative 2. Potentially poorly indicative. Brewer also identified additional indicators which included the involvement of small trading or intermediary companies, non-specific description of goods or materials, and fake or fraudulent documentation. These additional indicators highlight the nature of their overlap with other types of financial crime and their generic nature.

### **Current Threats<sup>10</sup>**

The **Democratic People's Republic of Korea (DPRK)** currently poses the most significant proliferation challenge. It continues to carry out procurement to develop an increasingly advanced nuclear weapons capability. According to RUSI (2017)<sup>11</sup>, DPRK continues to

<sup>8</sup> Brewer, 2018a: The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation

<sup>9</sup> United Nations Panel of Experts, 2014: Final report of the Panel Experts established pursuant to resolution 1929

<sup>10</sup> The threats discussed are current at the time of publication.

<sup>11</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

access the financial system globally via the use of front companies<sup>12</sup>, joint ventures with foreign firms, and especially Chinese financial institutions. They also continue to carry out activities such as trafficking of sanctioned commodities, in order to make resources available for their nuclear programme. These activities are dependent upon complex networks of businesses, which include middle men, and complex ownership structures designed to dilute any links back to DPRK<sup>13</sup>. It should also be noted that designated companies often operate under new identities within 6-12 months of designation, reinforcing the inadequacies of screening measures<sup>14</sup>.

Following the negotiation of the JCPOA, the majority of **Iran's** International Sanctions were terminated. RUSI (2017) point out that this termination does not indicate that Iran no longer poses a nuclear proliferation threat. Financial institutions should therefore bear in mind that "Iran is still prohibited from pursuing an illicit nuclear and missile programme outside the agreed-upon procurement and licensing framework established under the JPOCA"<sup>15</sup>. Additionally, a number of Iranian entities and individuals remain designated under UN Sanctions, due to their involvement with Iran's ballistic missile program<sup>16</sup>.

To this end, FinCEN (2018) issued an advisory<sup>17</sup> on the Iranian regime's exploitation of financial institutions worldwide. Within this advisory it is stated that dual-use goods for Iran's ballistic missile programs have been previously procured through intermediary companies that obfuscated the final recipient of the goods, such as networks of China-based brokers and their companies. Front and shell companies<sup>18</sup> are also used to evade sanctions. For example, German-based front companies were used previously to print counterfeit bank notes.

Front companies have also been used as a procurement method by **Syria**. The Syrian Scientific Studies and Research Centre (SSRC) was thought to be the key entity developing Syria's chemical weapons and ballistic missile programme; they conducted procurement (before 2011) by ordering goods from foreign suppliers via front companies<sup>19</sup>. These front companies made corresponding payments separately which were funded by wire payments from the SSRC, through companies based in tax havens and offshore financial centres<sup>20</sup>. Once U.S. and EU sanctions had been enforced on many of these front companies, the SSRC utilised Syrian businessmen who were funded in cash to carry out procurement on behalf of SSRC. Brewer (2018a) notes that following further international sanctions in 2014 and 2015, the SSRC disguised its activity by directing Syrian businessmen to evade sanctions by extending overseas business networks, particularly to exploit Chinese suppliers.

---

<sup>12</sup> Front companies are fully functioning companies with the characteristics of a legitimate business, which aim to disguise and obscure illicit financial activity.

<sup>13</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

<sup>14</sup> 2018: RUSI and Dechert LLP Roundtable event: Supply Chain Risk and DPRK Sanctions

<sup>15</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

<sup>16</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

<sup>17</sup> FinCEN Advisory 2018: Advisory on the Iranian Regime's Illicit and Malign Activities and attempts to Exploit the Financial System

<sup>18</sup> Shell companies are incorporated companies with no independent operations, significant assets, ongoing business activities, or employees.

<sup>19</sup> Brewer, 2018a: The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation

<sup>20</sup> Brewer, 2018a: The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation

Reports published earlier this year suggest that DPRK has been shipping supplies to the Syrian government that could be used in the production of weapons<sup>21</sup>. The supplies include acid resistant tiles, valves and thermometers, according to a report by the UN. This highlights the dangers of trade between the two countries, with DPRK gaining funding for its nuclear and missile programme by providing goods to Syria to maintain its chemical weapons.

Data on networks that finance the **Indian** and **Pakistani** WMD programs are highly limited in comparison with those of DPRK and Iran; Brewer (2018a) concludes that this suggests that the networks supporting these programs are relatively simple and funding is likely to be largely self-sufficient. According to data that is available, relatively few front companies have been involved, and there are no examples of companies acting as money remittance businesses<sup>22</sup>. Given that these countries are not subject to sanctions, these characteristics may reflect that complex methods are simply not required.

## 2. Typologies of Procurement of Goods

Understanding of the underlying procurement of goods is critical as it is more likely for individual goods and **component parts** to be shipped rather than finished off-the-shelf weapons (although Brewer (2018b)<sup>23</sup> notes that this should not be ruled out). This is highlighted by a recent case study<sup>24</sup> which involved a couple in the UK who unwittingly supplied prohibited aircraft parts and “nuts and bolts”, which could have been used in Iran’s nuclear weapons program. These goods were exported by a Dutch shipping company and onto Iran through a network of companies in Malaysia; the individual who owned these companies acted as a broker between the couple and the Iranian buyers. This individual is alleged to have held contracts to source and supply Iranian aviation firms with parts and components for planes and helicopters.

According to RUSI<sup>25</sup>, proliferators are becoming more proficient at upgrading the technology locally and have become more skilled at manufacturing many component’s locally. Analysis of previous cases shows that procurement of goods is a complex process, often involving several entities starting from manufacturing through to transport and end use. For example, according to the UN Security Council, foreign traders involved in violations of the coal ban operated through numerous **front companies** registered in various jurisdictions whilst being physically based in another. This indicates that activity often involves entities well beyond those that may be listed on Sanctions lists.

The use of front companies is not specific to DPRK; FATF (2008) reports that front companies are commonly established by proliferators and used to conduct transactions that mimic legitimate business, and there will also be a false end-user which is located in a country not linked to proliferation. These front companies may be similar to those established by money launderers. In some cases, these companies may not engage in any legal activity as there may be multiple names for the same front company. Additionally, they may arrange the routing or re-routing of goods acquired by the importer or its intermediary.

<sup>21</sup> <https://www.nytimes.com/2018/02/27/world/asia/north-korea-syria-chemical-weapons-sanctions.html>

<sup>22</sup> Brewer, 2018a: The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation

<sup>23</sup> Brewer, 2018b: The Financing of WMD Proliferation

<sup>24</sup> <https://www.dailymail.co.uk/news/article-6328725/Very-naive-couple-60s-groomed-supplying-parts-Irans-nuclear-programme.html>

<sup>25</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

This activity also involves networks of proliferators which utilise **middle men** and agents located overseas to procure materials. In order to obscure involvement with DPRK, the link between these middle men is far removed, and the movement of goods makes use of several transshipment points<sup>26</sup>. This is a point at which goods can be relabeled which complicates the delivery route, making tracking of their origin and final destination more difficult.

According to Brewer (2018a), **DPRK shipping companies** play a significant role in the circumvention of sanctions. Major ports from South East Asia and beyond are used by these shipping companies to transport prohibited materials on behalf of DPRK nuclear and other WMD programs, and they also serve as a source of income. Due to financial sanctions, they have relied greatly on foreign companies acting as bankers on their behalf. Interestingly, Brewer also suggests that proliferators may now make less use of trade finance than they once did. This is based on a comparison of the case studies in FATF's (2008) and Brewer's (2017) research. Whilst more than half of the case studies evaluated by FATF involved letters of credit, only a small minority of cases did so in Brewer's analysis, and none of these were related to DPRK case studies (it was Iran's proliferation program that used documentary trade finance).

Collectively, these methods illustrate that a strategy beyond list-based screening is required to counter PF. Additionally, Brewer (2018b) suggests that a comprehensive approach towards combatting PF also requires public-private sector collaboration, especially due to the global nature and complexities of PF. This includes the sharing of sensitive intelligence by Government organisations (which can be declassified) with the private sector.

This view is supported by a recent press release by the US Department of State<sup>27</sup>, following a meeting with industry leaders from maritime insurance companies, commodity traders, and other relevant parties. Attendees at this meeting aimed to discuss mechanisms to enhance cooperation between the private sector, governments, and the UN, and proactive measures that could be taken by the private sector to prevent evasion activities used by DPRK. This highlights the need for a collaborative approach between public and private sectors.

### 3. Distinguishing PF from other Financial Crimes

Brewer (2017) concludes that one of the "the most difficult aspects of identifying PF is that the goods and materials involved are often industrial items that, if not clearly identified as subject to some sort of controls, may appear innocuous to those involved in the supply chain and those assessing transactions in FIs". Moreover, as noted earlier, many of the indicators identified by FATF and Brewer are not uniquely associated with PF and overlap with other types of financial crime (See Annex B for the PF indicators which also overlap with other types of financial crime).

The source of funds for WMD proliferation can be legal or illegal<sup>28</sup>. As a result, longstanding risk indicators for money laundering may be relevant in cases where the source of funds is illegal. However, according to FATF, PF is more likely to involve cases where the source of

<sup>26</sup> RUSI, 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions

<sup>27</sup> <https://www.state.gov/r/pa/prs/ps/2018/11/287401.htm>

<sup>28</sup> FATF 2008: Proliferation Financing Report

funds are legal but the end use or type of goods involved is intentionally obscured. These structural differences should be noted when considering the indicators in Annex A and B.

#### **4. RECOMMENDATIONS**

Based on the above research and considering that screening measures are not proportionate or sufficiently targeted to mitigate risk, the following recommendations are proposed:

##### **Public / Private Partnership**

A collaborative approach between public and private sectors is recommended for a comprehensive approach to countering PF; this requires taking proactive measures to enhance communication between the two sectors. Brewer (2018b) and the US Department of State (2018) have both recently stressed this requirement, highlighting the global nature and complexities associated with PF and the need for Government to share desensitised intelligence with the private sector. Without this, crucial intelligence to better detect and mitigate against PF related activities will be missing.

##### **Post transactional AML monitoring**

To enhance risk coverage, a typology relating to DPRK PF may be considered within post transactional AML monitoring (i.e. trade surveillance) where such systems exist in FIs, or focused reviews of trade data where they don't. The typology/review should consider a *combination* of risk indicators which can be fine-tuned into a rule (for post-transaction AML monitoring solutions). The alternative approach, focused reviews of trade data, could be conducted by an investigations team whereby specific corridors could be investigated on a thematic basis.

The analyst should also consider the additional indicators in Annex A and B for a more comprehensive review of the client from a PF perspective.

##### **Education**

Increase awareness and knowledge of up-to-date PF indicators for Investigators, as well relevant KYC teams, trade finance staff, and Relationship Managers, so they are better informed when assessing potential PF related cases.

#### **5. Conclusion**

This paper has outlined the challenges in identifying true cases of PF as the typology is complex and multifaceted, in a similar way to that of trade based money laundering typologies. It should also be noted that PF is not exclusive to trade finance products and that financed trade makes up circa 20 per cent of international trade (the remaining is conducted using open account). Although the documentary nature of trade finance products allows a stronger risk assessment to be undertaken as opposed to open accounts transactions, this will only be at an individual transaction level. FIs rarely have oversight of the entire route of goods, as well as the entire transaction chain and network. As a result, the ultimate end-user is often unknown and assessment related to PF is therefore limited.

Screening goods against a list of DUGs at individual transactional level has proved ineffective; however, by undertaking targeted customer analysis across key corridors



combined with customer data outside of the trade finance department, FIs could work towards aiming to mitigate against proliferation financing. Information sharing between private and public sectors is imperative to build a stronger and collaborative regime to counter PF, for any of these solutions to work.

Acknowledgements:

This paper was written for the ICC Financial Crime Risk and Policy (FCRP) Group by Nita Patel, Graham Finding & Dr. Graham Baldock.

With special thanks to editorial contributions from members of the ICC FCP Group.

**Annex A**

RUSI suggests that Financial Institutions should not only consider the procurement of goods by DPRK to facilitate its programme, but also DPRK’s capability to export sensitive goods to buyers, such as Syria and Egypt. To this end, the indicators listed in Annex A have considered both the buying and selling parts of the trade cycle. Please note that these indicators are not intended as to be utilised as ‘red flags’ by FIs; they support the theoretical content of this paper.

**DPRK Proliferation Finance and Trade of Dual-Use Goods Indicators**

Risk Number	Risk/Indicator	Summary	Source
1	CB accounts held with Chinese banks	North Korea has particularly used correspondent accounts held with Chinese banks to facilitate its international financial transfers. Some Chinese branches also maintain offices or branches within NK.	UN Report, March 2018
2	Kholmsk (Russia) port used for transporting coal from DPRK	Kholmsk, Russian Federation – this was identified by the UN as a new route to a port rarely visited previously by NK. Tracking data showed at least 4 vessels calling at this port, all of which were said to be transporting NK coal. Other vessels are believed to have berthed here, and coal may have been transshipped using false origin documents.	UN Report, March 2018
3	Export Controls	Customer is a manufacturer/dealer in products which are subject to export controls	Brewer, 2017
4	Other	Involvement of individuals or entities in foreign country of proliferation concern; may be dealing with complex equipment for which he/she lacks technical background	Brewer, 2017 FATF, 2008
5	Other	Parties conduct trade in export controlled products	Brewer, 2017
6	Other	Parties maintain links to a university in a proliferating country	Brewer, 2017
7	Other	Personal accounts are used to purchase industrial items	Brewer, 2017
8	Other	Trade finance transaction involves shipment through country with weak export control laws	Brewer, 2017

9	Other	Parties are located in countries with weak export control laws	Brewer, 2017
10	Other	Individuals or entities involved, or their details (such as addresses or telephone numbers), are similar to, or may be connected to, parties listed under the WMD-related sanctions or export-controls regime, or they have a history of involvement in export control contraventions	Brewer, 2017 FATF, 2008
11	Jilin and Liaoning in China	NK takes advantage of trading companies in border provinces such as Jilin and Liaoning in China to keep its assets offshore in accounts that conceal NK ownership and facilitate international sanctions	RUSI, 2017
12	Spare Parts	NK is known to have a penchant for identifying military-related goods it sells overseas (including missile related products) as 'spare parts' for construction machinery	RUSI, 2017
13	Freight Forwarding	Freight forwarding company listed as consignee.	RUSI, 2017

## Annex B

These indicators have been extracted from research completed by FATF, Brewer, and RUSI which based their work on proliferation programs of DPRK Syria, Iran, Pakistan and India. Please note that these indicators are not intended as to be utilised as 'red flags' by FIs; they support the theoretical content of this paper.

Generic Indicators			
Risk Number	Risk/Indicator	Summary	Source
1	Other	Parties conduct business activity inconsistent with their profile	Brewer, 2017 FATF, 2008
2	Other	End-user not identified	Brewer, 2017
3	Other	Goods ordered from third countries	Brewer, 2017
4	Other	Cash used in transactions for industrial items	Brewer, 2017
5	Other	Highly technical goods shipped to countries with low levels of technology	Brewer, 2017
6	Other	Commercial business is acting as a money-remittance business	Brewer, 2017
7	Other	Links identified between parties involved in a given transaction (for example, common ownership)	Brewer, 2017
8	Other	Parties provide trading documentation with non-specific or misleading description of goods	Brewer, 2017
9	Other	Parties provide documents which are fake or fraudulent	Brewer, 2017
10	Other	Parties conduct business with financial institutions with weak financial crime controls; or in countries with weak export laws	Brewer, 2017
11	Other	Parties use circular routes of shipments or circular routes of financial transactions	Brewer, 2017
12	Other	Shipment of goods in inconsistent with normal trade patterns	Brewer, 2017
13	Other	Declared value of shipment is obviously undervalued	Brewer, 2017
14	Other	Customer provides inconsistent and/or incomplete information in trade documents and financial flows	Brewer, 2017

15	Other	Customer conducts unusual pattern of wire transfer for no apparent reason	Brewer, 2017
16	Other	New customer requests letter of credit while waiting approval of new account	Brewer, 2017
17	Other	Payments connected with parties not identified on letter of credit or other documentation	Brewer, 2017
18	Other	An order for goods is placed by company or individual from foreign countries other than the country of the stated or suspected end-user	Brewer, 2017
19	Other	Transaction involves shipment of goods inconsistent with normal geographic trade patterns	FATF, 2008
20	Other	Involvement of a small trading, brokering or intermediary company (may be carrying out business inconsistent with their normal business)	Brewer, 2017
21	Other	Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, etc.	FATF, 2008
22	Middle Men	The use of middle men and agents located overseas to procure materials; illicit trade is often mixed with legal trade	RUSI, 2017



## About The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC) is the world's largest business organization representing more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

[www.iccwbo.org](http://www.iccwbo.org)

Follow us on Twitter: [@iccwbo](https://twitter.com/iccwbo)

### **INTERNATIONAL CHAMBER OF COMMERCE**

33-43 avenue du Président Wilson, 75116 Paris, France

T +33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59

E [icc@iccwbo.org](mailto:icc@iccwbo.org) [www.iccwbo.org](http://www.iccwbo.org)