



**GLOBAL COALITION
TO FIGHT
FINANCIAL CRIME**

Trade-Based Financial Crime - Middle East and North Africa

A reference guide for the anti-financial crime community

GCFCC MENA Chapter

There has been a lot of industry focus on trade-based money laundering (TBML), however, as this document outlines, trade is an adept vehicle for many types of financial crime. Goods can be over or under-invoiced, counterfeit goods can be traded, goods can be misrepresented on invoices to avoid detection, and documents can be presented for fictitious shipping. These are only a few of the ways in which the trade system can be used to mask criminal activity. The term trade-based financial crime (TBFC) will be used throughout this document to encompass the various trade-related scenarios which can constitute a crime or illegal activity.

TBFC can be complex, involving many parties, with actors employing a variety of schemes in an attempt to circumvent laws, regulations, systems and controls to ensure their scheme is successful. There is no single solution to prevent TBFC or the impact it may have; only by working together, through public-private partnerships (PPPs) and cross-sector cooperation to internal team collaboration, will those charged with mitigating TBFC have a chance of effectively combatting it.

This document has been put together by the Trade-Based Financial Crime Working Group of the Global Coalition to Fight Financial Crime MENA Chapter, a public-private coalition that aims to enhancing the fight against financial crime globally. It provides a high-level overview of TBFC, outlining what it is, how it can occur, different roles within the trade cycle, financial services products that assist trading, and steps that can be achieved in identifying and mitigating TBFC. It is designed for all parties who wish to gain a better insight into how illicit funds, goods or services can be moved through trade flows. The authors drew on their decades of combined expertise as well as the wealth of published information on the subject to compile this reference guide.

GCFFC MENA Chapter

Trade-Based Financial Crime - Middle East and North Africa

A reference guide for the anti-financial crime community



Foreword

Financial crime crosses borders and betrays communities and ecosystems; it steals trillions of dollars from people all over the world, usually from those most in need, and endangers precious, finite resources. Addressing the true human and environmental impact and societal costs of criminal activity is a challenge that requires constant and collective action.

Criminal organisations rely on an interconnected and international financial system to support their illegal schemes; they exploit various means to move their ill-gotten gains without detection, enjoying the proceeds once they have been laundered and layered beyond traceability. The global trade system, which UNCTAD reported as having reached a record volume of USD 28.5 trillion in 2021, is an especially attractive tool for criminals, as it provides a ceaseless network of commercial activity, transporting goods and money around the world.

The complexity and extensiveness of the global trade system makes it not only vulnerable to use as a conduit for illicit funds, but also particularly challenging to protect from criminal abuse. In any given trade transaction, there may be multiple parties, each providing a different service or playing a different role, and each link in the chain carries its own exposure to trade-based financial crime. Although industry attention is typically diverted towards trade-based money laundering risks, there are a plethora of other means by which financial crimes can be committed through the trade system, defrauding investors, circumventing sanctions, or evading tax. Practitioners operating in every part of the defensive system, across the public and private sectors, need to be aware of how this manifests as suspicious activity, and how it can be effectively dealt with once it has been successfully detected.

This comprehensive **“Trade-Based Financial Crime - Middle East and North Africa”** reference guide was compiled by the Global Coalition to Fight Financial Crime (GCFFC) MENA Chapter for the benefit of all professionals based in the region, concerned with protecting the integrity of the regional economy. In line with the Chapter’s mission to enhance local regional expertise and bridge public and private sector efforts, this reference text was created by world-leading experts with a specific focus on how TBFC methodologies are experienced in the MENA region. It aims to provide a single, accessible source of knowledge and instruction for compliance professionals, customs officials, and law enforcement agencies alike, to create aligned understanding of how the trade system is abused, what methods are available to detect these abuses, and how that information can be deployed by the authorities to prevent further occurrences of trade-based financial crime. By producing the guide in bilingual format, it is immediately more accessible to regional practitioners, and reflects the MENA-specific focus that lies at the heart of the Chapter’s mandate.

Special recognition and thanks are owed to the experts who donated their considerable knowledge and insights to this reference guide. Their expertise is matched only by their generosity in devoting so much time and effort to this initiative, and their shared dedication to improving defences against illegal trade.



Ibtissem Lassoued
Chair, **GCFFC MENA Chapter**
and Partner, Financial Crime,
Al Tamimi & Company



Michael Matossian
Vice Chair, **GCFFC MENA Chapter**,
Deputy Chair, **MENA FCCG**
and EVP & Chief Compliance Officer,
Arab Bank Group

Letter from Co-Sponsors

TBFC Project

Financial crime continues to be a significant challenge for policy makers, governments, law enforcement, regulators and Financial Institutions given the impact it has on the public, irrespective of whether they are directly or indirectly affected. The cause and impact of financial crime has no borders and criminals, by definition, do not respect laws of countries and states; in fact, they prey on the differences in laws and regulations to further their heinous activities.

As we all know, the proceeds of crime can emanate from number of approaches such as organised crime, corruption, human and wildlife trafficking, tax evasion, cyber-crime, terrorism, drugs, sanctions evasion etc. A key common factor connecting the bad actors seeking to launder the proceeds of crime or evade sanctions, is the misuse of the global trade network.

Trade is an attractive way to launder the proceeds of crime, or evade sanctions, due to several of its fundamental features; its international and cross-border nature, the involvement of multiple parties in a typical trade transaction (thereby limiting the ability to fully understand end to end transaction chain), the variety of goods involved, and, importantly, the use of open account trade (where traditional trade documentation such as Letters of Credits are not sought).

The MENA region harbours a long tradition of trade. As such, it shares trade-based financial crime typologies with other global trading hubs, but also exhibits its own specific typologies that reflect the unique risks that transit this geography. Countries that are large facilitators of trade with a thriving business market and mature financial infrastructure are more vulnerable to the threat of trade-based financial crime. The Middle East epitomises the concept of a trade hub, connecting the East, West and Africa with its prime geographic location, advanced economies and, long and rich history of trade.

It is in this context that GCFFC MENA Chapter prioritised focus on creating a compendium of knowledge to help improve awareness of Trade Based Financial Crime ("TBFC") as a reference guide for anyone involved in the trade ecosystem. This guide focuses significantly on parts of trade where transfer of value (or money) is involved and is therefore particularly relevant to Financial Institutions. We have, however, taken a conscious effort to strike the right balance between high-level concepts and details, with a view to making this document accessible and useful for the non- Financial Institution stakeholders involved in trade.

This project was a collective effort from a team of experts that have volunteered their personal time to pool their vast knowledge for this project. We would like to thank each for their efforts over the course of the project.

Amjad Batayneh (Author) is a Manager at the Special Investigations Unit at Group Regulatory Compliance, Arab Bank. He has more than 18 years of compliance experience in banking and previously held numerous senior positions specialised in Sanctions, AML Investigations and Trade Finance among different local and international banks in Jordan. Amjad holds several international certificates including CAMS, CGSS, and several LIBF (London Institute for Banking and Finance, UK) certificates including CTFC, CDCS, CSDG, CITF and QTFS.

Amjad holds a masters degree in Financial Management from Arab Academy for Banking and is an authorised trainer for ACAMS and the Institute of Banking Studies in Jordan.

Channing Mavrellis (Lead Editor) is Global Financial Integrity's Illicit Trade Director, focusing on the intersection of illicit financial flows (IFFs), transnational crime, and international trade. Channing has over a decade of experience working on issues related to AML/CFT, and specialises in conducting data-driven analysis of illicit trade and trade-related IFFs. In addition, she has strong experience providing policy advice and training to US and foreign government officials on illicit trade. She has testified before Congress as well as delivered remarks on illicit trade, customs fraud, and IFFs at events organised by the OECD, UNDP, US Customs and Border Protection, US Department of State, and US Department of Defense, among other organisations.

Fahad Haque (Author) is the Regional Head of Sanctions for MENAT at HSBC. He has been part of the HSBC Group for over 8 years covering AML and Sanctions across several jurisdictions including London, Milan and Dubai. Earlier, Fahad worked with the UK financial services regulator, the Financial Conduct Authority and holds ICA diploma in Governance, Risk and Compliance.

Graham Baldock (Author) has over 17 years of compliance experience having held senior level roles in Financial Institutions in the UK. Prior to moving to the UAE, Graham was the Global Head of Financial Crime Compliance for the Trade Finance department in HSBC. He is a member of the UAE ICC Banking Commission and MENA TBML Working Group for the Global Coalition to Fight Financial Crime. He holds a Professional Doctorate in Criminal Justice from Portsmouth University, UK, along with several international certificates including Certified Global Sanctions Specialist (CGSS), and Advanced Risk Management (CAMS-RM).

Jonathan Brewer (Author) is a Visiting Professor at King's College, London, conducting research on financing of WMD proliferation. He was the financial expert of the UNSC resolution 1929 Panel on Iran. Formerly with the UK Diplomatic Service, Jonathan worked in British Embassies in Luanda, Mexico City and Moscow. He holds a PhD in Geophysics from Cornell University, USA, and a BA in Geology from Oxford University, UK.

Nishanth Nottath (Project Lead) is the Executive Vice President – Head AML, ABC and RegTech at Mashreq Bank UAE. Prior to this role he was the Global Head of Transaction Monitoring at HSBC and held a number of leadership roles in anti-financial crime covering the Middle East and Africa at HSBC, Standard Chartered Bank and KPMG. Nish is a Chartered Accountant (India), Chartered Management Accountant (UK), and PGP holder in Data Science / Business Analytics from University of Texas, Austin, US.

We hope that this reference guide will improve awareness around this complex topic and support the efforts of the anti-financial crime community.



Collin Lobo
Co-Sponsor – TBFC Project,
GCCFC MENA Chapter
Regional Head of Compliance,
HSBC MENAT



Scott Ramsay
Co-Sponsor – TBFC Project,
GCCFC MENA Chapter
SEVP, Group Head of
Compliance, **Mashreq Bank**

FOREWORD	5
LETTER	6
GLOSSARY OF TERMS, ABBREVIATIONS, AND ACRONYMS	10
PREFACE	13
INTRODUCTION TO TRADE	16
Parties to a Trade Transaction	16
Agreements Involving Trade and Trade Finance	18
Delivery of Goods	19
Payment for Goods	22
TRADE-BASED FINANCIAL CRIME	30
Money Laundering	31
Trade Mis-invoicing	33
Service Based Money Laundering (SBML)	35
Terrorism Financing	36
Proliferation Financing	38
Tax Crimes	44
Sanctions Evasion	46
Illegal Wildlife Trade	47
Additional Considerations	50
TYPOLOGIES	58
Risks Associated with Documentation	58
Switch Bill of Lading	58
Blank Endorsed Bill of Lading	58
Fraudulent Bills of Lading and Other Falsified Documents	58
Back-to-Back Letters of Credit	59
Misuse of Standby Letter of Credit	59
Risks Associated with Goods	60
Evasion through Consolidation of Goods	61
High Risk Goods	62
Risks Associated with Actors	63
Freight forwarders and customs brokers	63
Front and Shell Companies	63
Risks Associated with Transport	65
Transshipment	65
Concealing the Final Destination of Goods	65
International and National Responses to TBFC	67
United Nations	67
Financial Action Task Force	67
Risk-Based Approach to Money Laundering	68
Dual-Use and Sensitive Goods	69
Export Controls	71

FINANCIAL INSTITUTIONAL AND TBFC: VULNERABILITIES AND RESPONSES	74
Vulnerabilities	74
Responses	75
Risk Assessments	75
Customer Due Diligence	76
Sanction Screening	77
Transaction Monitoring	77
Unusual Transactions	78
DIGITALISATION OF TRADE	82
TBFC and Technology	82
Network Analytics	83
Digitalisation	83
Data	84
Innovation	84
Distributed Ledger Technologies	84
Risks	86
The future of DLT adoption	87
CONCLUSION	89
BIBLIOGRAPHY	90
APPENDICES	94
Appendix I: Recommended Resources	94
Appendix II: Additional Information on Payment Messages / Trade SWIFT messages	95
Appendix III: Harmonised System Codes	96
Appendix IV: TBFC Red Flags and Risk Indicators	97
Appendix V: Trade Finance Check Lists	105
Appendix VI: Proliferation Financing Indicators	108
Appendix VII. Indicators of Laundering the Proceeds for Illegal Wildlife Trade	110
TBFC PROJECT TEAM, GCFFC MENA CHAPTER	112



Table of Contents

Glossary of Terms, Abbreviations, and Acronyms

Term/Abbreviation/Acronym	Definition
AML	Anti-money laundering
B/L	Bill of lading
CBI	Central Bank of Iran
CDD	Customer due diligence
CFT	Combatting the financing of terrorism
COD	Cash on delivery or collect on delivery
DC	Documentary collection
DLT	Distributed ledger technology
DPRK	Democratic People's Republic of Korea (North Korea)
EU	European Union
Eurostat	European Statistical Office
FATCA	Foreign Account Tax Compliance Act (United States)
FATF	Financial Action Task Force
FCA	Financial Conduct Authority (United Kingdom)
FCL	Full container load
FI	Financial institution
FIU	Financial Intelligence Unit
FTZ	Free trade zone
GAAR	General anti-avoidance rule
GCFFC	Global Coalition to Fight Financial Crime
HS	Harmonised system
ICA	International Compliance Association
ICC	International Chamber of Commerce
IFF	Illicit financial flow
IIBLP	Institute of International Banking Law & Practice
Incoterms	International Commercial Terms
IRGC	Iranian Revolutionary Guard Corps
ISBP 745	International Standard Banking Practice Publication (745)

ISP98	International Standby Practices, 1998 edition
JCPOA	Joint Comprehensive Plan of Action
KYC	Know your customer
LC	Letter of credit
LCL	Less than container load; also known as "groupage"
LG	Letter of guarantee
MENA	Middle East and North Africa
ML	Money laundering
MT103	Single Customer Credit Transfer
MT700	Issue of a Documentary Credit
MT760	Issue of a Guarantee
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control (United States)
PF	Proliferation financing
PPP	Public-private partnership
SBLC	Standby letter of credit
SBML	Service-based money laundering
SDN	Specially Designated Nationals
STR	Suspicious Transaction Reports
TBFC	Trade-based financial crime
TBML	Trade-based money laundering
TF / TBTF	Terrorist financing / Trade Based Terrorism Financing
UCP600	Uniform Customs and Practice for Documentary Credits
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
URDG758	Uniform Rules for Demand Guarantees
WMD	Weapons of mass destruction
IWT	Illegal Wildlife Trade



Preface

“If you are filled with pride, then you will have no room for wisdom” (African proverb)

Fighting financial crime is a complicated process involving professional bodies, practitioners, legislators, regulators, and educators. If criminal activity is left unchecked, and if criminals are not held accountable, lives would be lost, careers would be shattered, and the wellbeing of generations would be compromised.

From an educational perspective, we are genuinely interested -particularly in the MENA region- in understanding why some people do the right thing while others choose otherwise. We are interested in deciphering the reasons why sometimes good people commit humungous errors, commit criminal or unethical behaviors, and display striking lapses in judgment leading to catastrophic consequences. It turns out that the picture is far beyond our ability to explain by one or two reasons.

Sometimes good people commit corrupt or criminal behaviors because they lack moral sensitivity; they are simply not aware that a certain of course of action has legal or ethical implications. They do not understand the repercussions of their individual choices on others. Sometimes people know that a certain behavior is wrong, but they lack the sophistication to understand how to address it; they do not have the cognitive or emotional maturity to be able to choose right from wrong. At other times, people commit wrong behaviors because not enough personal or organisational incentives exist that inspire them to do the right thing. Beyond all of these potential reasons that explain bad behaviors, however, it is often the case that the right thing is not done because people do not have the capacity to display moral courage. They do not have the character that makes them take the leap into choosing the right thing.

Having a reference guide for the anti-financial crime community will -without any doubt- help professionals in making the right decision across many fronts. It will help in sensitizing them to the dire implications of financial crimes; it will help them appreciate the significant role that they individually play in combating it. It also provides some relevant tools to use, and explains how and when to use them. It contributes to motivating them to do the right thing, now that they know about the severity of the impact of financial crime on people, organisations, societies, and even countries at large.

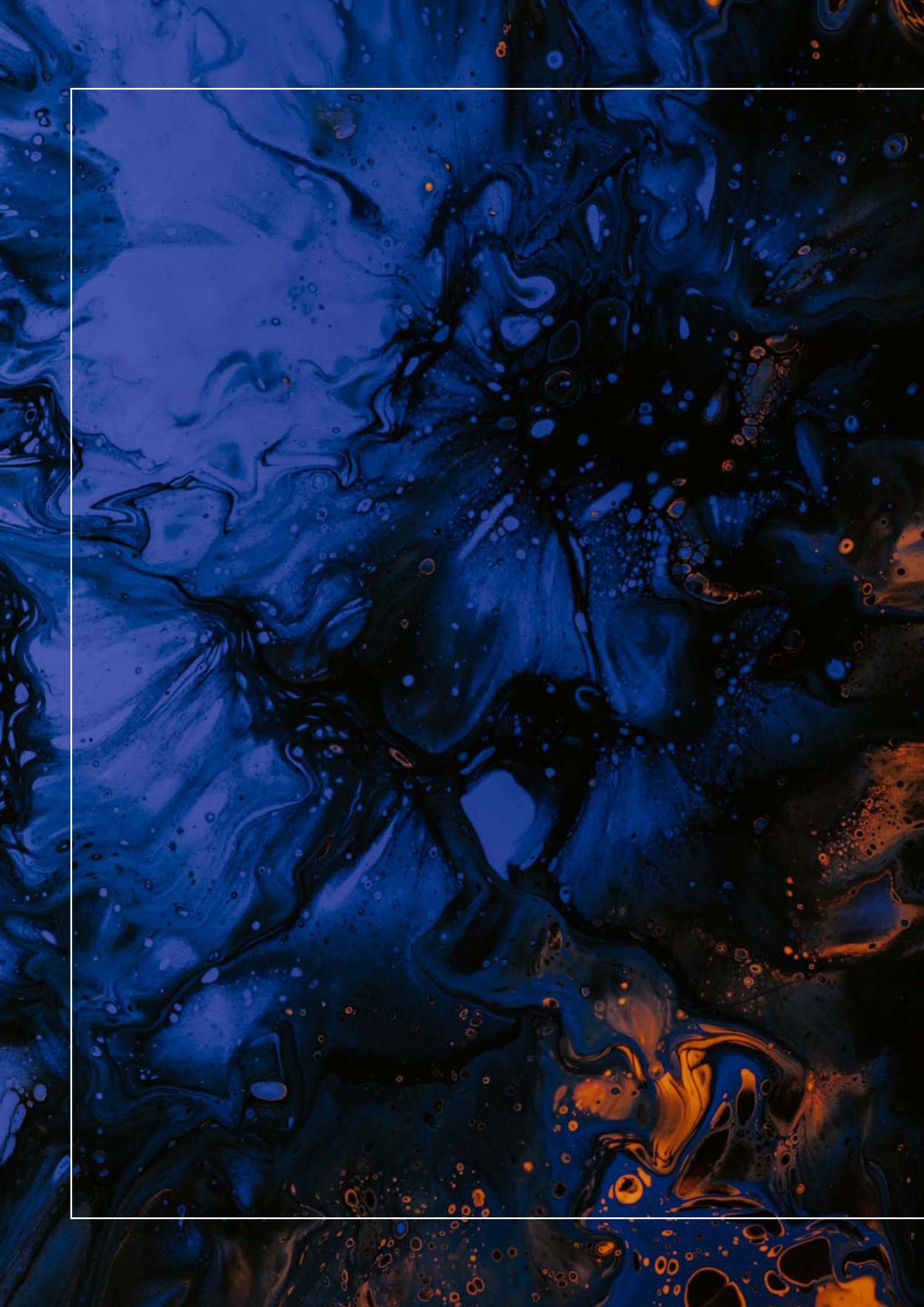
But beyond all of that, combating financial crime requires moral courage, the courage to do the right thing irrespective of repercussions, and irrespective of the disapproval from others. Organisational leaders and employees often face what are called defining moments: those are the moments when their values are put to test -often a severe test- in situations filled with uncertainty, confusion and doubt. Courage requires the ability to take risks while remaining cautious, the capacity to challenge other people’s perspectives while remaining open-minded, and the power to take a stand while still remaining humble. In that, organisational members need to be alert to situations where their fear or their pride makes them less sensitive to situations that require a moral stand against crime. It is in those moments that real leaders emerge, and their genuine and authentic character will arise helping in the collective effort against financial crime.



Yusuf M. Sidani

Dean & Professor of Leadership and Business Ethics

Suliman S. Olayan School of Business, American University of Beirut





**Introduction
to Trade**

Introduction to Trade

In essence, trade consists of the purchase of goods and/or services by a buyer, and their sale by a seller. Where there is an agreement to do so, the seller must deliver what is purchased and transfer the rights to it, and the buyer must accept what is delivered, if it conforms with the agreement, and pay for it.

Trade can be domestic or international. Domestic trade takes place within the confines of a nation state. International trade is the exchange of goods and services between parties in different nation states. International trade transactions are often more complex in nature, as they usually involve a number of parties beyond the buyer and seller, a variety of agreements with and between these parties, various standards and customary practices, and various bank products, including those which facilitate delivery and payment, as well as assure performance.

Whilst international trade is typically the focus of TBFC compliance, domestic trade can equally be used to launder funds, support terrorism, facilitate corruption, or serve as a vehicle for commercial fraud. Because there are typically limited regulatory checks on domestic trade, such as customs, there are limited statistics for domestic trade.³

The World Trade Organization states that world trade in goods and services was worth US\$22 trillion in 2020¹ and UNCTAD estimated that global trade hit a historical record of US\$28.5 Trillion in 2021.²

Parties to a Trade Transaction

The buyer and seller form the base of every trade transaction; however, more parties may be involved depending on the complexity of the transaction. This may include parties such as guarantors, financiers, insurers, inspectors, brokers, and logistical intermediaries. Government agencies may also play a variety of roles when it comes to trade; for example, government and state-owned entities may act as both buyer and seller.

The following table (Table 1) provides an overview of some of the most common parties involved in a trade transaction.

Table 1 – Parties involved in a trade transaction

Party	Role
Buyer	Any entity which purchases goods or services either for use, to manufacture into another product, or for resale.
Seller	Any entity who sells goods or services to a buyer.

¹World Trade Organization, *World Trade Statistical Review 2021* (Vienna: World Trade Organization, 2021), 11, https://www.wto.org/english/res_e/statis_e/wts2021_e/wts2021_e.pdf.

²<https://unctad.org/news/global-trade-hits-record-high-285-trillion-2021-likely-be-subdued-2022>

³James E. Byrne and Justin B. Berger, *Trade Based Financial Crime Compliance* (Montgomery Village, MD: Institute of International Banking Law & Practice; London Institute of Banking & Finance, 2017), 18.

Middlemen	This is a broad category of parties and includes any intermediary, except for the buyer/seller, who may be involved in the purchase and sale of goods, or the financing, facilitating, or transporting of such goods and commodities.
Financiers	Any entity providing finance to another entity, which can be the seller, buyer, an intermediary, a bank, or other financial institution. For example, a seller can provide finance to a component manufacturer, to sales agents, or even to the buyer. Most typically, it is a financial institution that provides financing.
Transport Providers	When the goods are moved from the location where the seller stores them to another place, there is a need for transportation. While either the buyer or seller can provide transportation, it is common to use third parties, such as air freight, maritime shipping, and trucking services. ⁴
Freight Forwarder	Freight forwarders facilitate the shipment of goods, “helping buyers and sellers navigate often complex customs and shipping routines and processes. They act as experts in determining the most efficient transportation method in moving the goods, which can incorporate multiple modes for a single shipment.” ⁵
Customs Brokers	Customs brokers “work to make the import and export of goods run smoothly, by facilitating the clearance of goods through customs processes. The broker will work with importers to check whether the necessary documentation or licences are in place, while ensuring the correct duty and taxes are paid, to reduce any delays.” ⁶ They may be affiliated with a freight forwarder or can work independently.
Transport Facilitators	Any third-party intermediaries who facilitate shipment (e.g. freight brokers) or receipt (e.g. customs brokers).
Warehousing / Warehouseman	A warehouseman is often involved when the ownership of the goods is transferred without the goods being physically moved, and the goods are in the control of a third party. The obligation of a warehouseman is to deliver the goods to the person entitled to receive them according to the warehouse agreement.

⁴Historically, the mode of transport associated with international trade was maritime or ocean transport which was the only practical, or the cheapest, form of transport, particularly for bulk products. In this form of transport, the goods are entrusted to the carrier by the shipper, who is the seller or a third party who contracts with the party providing transport (the carrier). The carrier is obligated to deliver the goods in accordance with the terms of the contract of carriage. The principal modes of transport are water (ocean, maritime or inland, by common carrier or chartered vessel), rail, road, or air. Except for bulk goods and commodities (for example: oil, iron ore or other metals and mining products, grain, and sugar), most contemporary transportation of goods is done by means of standardized containers. This means of shipment has given rise to a significant increase in multimodal transportation; that is, transportation involving more than one mode of transport, thus avoiding the need to repack or reconsolidate in transit. For example, the goods can be placed into a container which is loaded onto a truck at an inland point, trucked to a railhead, loaded on board a train and transported to a port, where the container is laden on board a marine vessel. The reverse process can occur at the destination, until the container reaches the buyer's facilities.

⁵Financial Action Task Force and Egmont Group, *Trade-Based Money Laundering: Trends and Developments* (Paris: Financial Action Task Force, 2020), 25, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html>.

⁶Financial Action Task Force and Egmont Group, 26.

Third Party Inspection Agencies	This category includes private sector entities that inspect goods and certify the results according to requested and commercially agreed standards. ⁷ Such inspections provide comfort to buyers and their financiers that the product being delivered reflects what was ordered.
Government Authorities	This category includes tax or excise agents, inspectors (including health inspectors) and agencies responsible for granting export or import licences or permits.
Insurers	This category includes entities that exist to spread the risk of loss related to trade. There are various types of insurers that relate to trade, including coverage of transport (such as maritime insurance), country risk, or payment risk. Often, provision of some type of insurance is part of the bargained for agreement between the buyer and seller or is mandated by financiers. It is common for insurance to overlap. Some insurers are commercial enterprises while others are connected with government efforts to encourage exports.
Financial Institutions	This category includes organisations established to provide funding and support for trade, processing documents, and payments.
Parties Providing Assurance of Payments	In addition to Financial Institutions, other entities provide assurance of payment or otherwise lend their credit standing to facilitate trade as guarantors or sureties. Their role is discussed in detail below.
Lawyers	Virtually every phase of a trade transaction involves potential legal issues and legal relationships. As a result, it is not uncommon for lawyers to advise parties at an early stage of trade negotiations, draft or review undertakings and documents, or to otherwise represent parties at any time during, or after, the commercial transaction.
Trade Associations and Standard Making Bodies	This category includes organisations that represent entities involved in trade or related services on a national or international level. Often, they establish and issue standards, rules, and provide various other services. ⁸

Agreements Involving Trade and Trade Finance

While trade transactions are varied and complex in nature, at their core, they have a simple challenge with which to contend: the delivery of goods, and payment for them.

In a transaction for the sale of goods, the seller does not wish to part with control over the goods (i.e. to deliver them) without having received payment or dependable assurance of payment. The buyer, on the other hand, will not want to pay without having goods in hand and being assured that they are of the type, quality, and quantity agreed. There are similar concerns with the provision

⁷An example of one of the better-known third-party inspection agencies is Société Générale de Surveillance (SGS).

⁸Byrne and Berger, *Trade Based Financial Crime Compliance*, 20–22.

of services: the person providing the service does not want to do so unless they are paid, but the person seeking the service does not want to make payment until it is assured that the service is as promised.

Most of the details regarding delivery and payment involve balancing these concerns; a process which is affected in accordance with the relative strength of the positions of the parties, or their bargaining power. This section provides an overview of the different types of agreements made between the parties of a trade transaction involving the delivery of goods, the payment for the goods, as well as additional considerations.

There may be an agreement between the buyer and the seller, where the buyer pays in advance of the goods being sent, partial payment might be made, or the buyer may pay upon receipt of the goods. There are a number of financial services products available to the parties to facilitate trade, for example a trade loan, or a Letter of Credit (LC), by means of which a Financial Institution may move the documents that support the trade along with a document of a promise to pay if all the conditions are met. The different products are discussed in more detail later on in this document.

A number of Financial Institutions offer trade finance products. Typically, the starting point for trade finance is a series of agreements. These agreements may or may not be embodied in a highly formal written and signed contract, which may be either concise or expansive. It is useful to note that the word "contract" has two different meanings; the enforceable agreement of the parties, or the written text that attempts to reflect that agreement. Where there is a written agreement, the question arises as to whether it is a complete and final statement of what was agreed by the parties, or if extraneous and additional circumstances and documents may supplement or modify the agreement.

Depending on the previous dealings and experiences of the parties, agreements can be rather informal. Typically, however, the parties will at least agree on how the seller is to deliver the goods, their type, quality and quantity, how the buyer is to pay for them, and the total contract price.

Delivery of Goods

Delivery is one of the fundamental obligations of a seller in a contract for the sale of goods, signifying the tendering of the goods from the seller to the buyer (or their representative). It can involve the movement of the goods and the transfer of control and ownership of them, or only the transfer of control and ownership without the physical movement of the goods themselves.

Bill of Lading

When the sale of goods requires the physical movement of the goods by way of shipping, a bill of lading (B/L) is required. A bill of lading is "a document issued by a carrier, or its agent, to acknowledge receipt of cargo for shipment."⁹ It serves three main functions:

- As a conclusive receipt, acknowledging goods have been loaded
- It contains or evidences the terms of the contract of the carriage
- As a document of title to the goods. Essentially, it "confers title over the goods to the named consignee or lawful holder."¹⁰

⁹"What Is Bill of Lading?," NYC Supply Chain Solutions Inc., accessed March 17, 2022, <https://nycscs.com/what-is-bill-of-lading/>.

¹⁰Financial Action Task Force and Egmont Group, *TBML: Trends and Developments*, 26.

Due to the important role that a B/L plays, it is imperative that it:

- Is always kept with the goods until they reach their final destination
- Is complete, and properly filled out
- Indicates the name of the carrier and is signed by:
 - the carrier, or a named agent for or on behalf of the carrier; or
 - the master, or a named agent for or on behalf of the master.¹¹

As the Legal Dictionary explains, the B/L “is evidence that a contract exists and, as such, it needs to be appropriately filled out at each step, from the moment the shipment is received, until the moment that it is delivered.”¹²

There are several types of B/L that are used depending on the situation. Table 2 outlines some of the most common types of B/L.

Table 2 – Types of bills of lading

Type	Description
Negotiable B/L	A negotiable B/L “acts somewhat like a cheque, consigned (or made payable) to a company, the shipper, or some other entity. This type of [document] is used to get paid, making it important. Not only that, but obtaining a replacement negotiable bill of lading is a difficult process, which is why those handling this particular type [of document] should be incredibly careful not to misplace it”. ¹³
Straight B/L	A straight B/L is non-transferrable, so only the consignee is allowed to sign for the goods and accept them, that is, assume ownership.
Seaway B/L	A seaway B/L is “a non-negotiable contract between the ocean carrier and the customer to deliver the goods booked by the customer to a specific consignee. The seaway bill is usually preferred by companies that deal directly with each other on a regular basis”. ¹⁴
Switch B/L	A switch B/L “is simply the second set of the bill of lading that may be issued by the carrier or their agent ‘in exchange of’ or ‘substituting’ the first set of the bill of lading originally issued when the shipment was affected. The second set of the bill of lading cannot be issued while the full first set is still in circulation and active”. ¹⁵
Blank Endorsed B/L	A blank endorsement on a B/L “indicates the seller has not specified a recipient or buyer for the goods at the time of shipment, [so] they can indicate ‘to order’ or ‘to order of’ in the consignee section of the bill of lading. The carrier now becomes responsible for the delivery of the goods and for any ancillary costs related to the shipment”. ¹⁶

¹¹ICC Uniform Rules for Documentary Credit (UCP600), Article 20-a-i

¹²“Bill of Lading”, Legal Dictionary, accessed December 20, 2021, <https://legaldictionary.net/bill-of-lading>. – Article 20-a-i of UCP600 Bill of Lading.

¹³“Bill of Lading”.

¹⁴Hari Menon, “What Is Seaway Bill in Shipping?”, *Marine Insight* (blog), December 21, 2021, <https://www.marineinsight.com/maritime-law/what-is-seaway-bill-in-shipping/>.

¹⁵Hariesh Manaadiar, “What Is a Switch Bill of Lading and When and Why Is It Used.??”, *Shipping and Freight Resource*, February 1, 2019, <https://www.shippingandfreightresource.com/what-is-a-switch-bill-of-lading-and-when-and-why-is-it-used/>.

¹⁶“Blank Endorsement on a Bill of Lading,” Investopedia, accessed December 20, 2021, <https://www.investopedia.com/ask/answers/032615/what-endorsement-blank-bill-lading.asp>.

B/Ls also differ in type depending on when and how the goods are shipped; there are on-board B/Ls and received for shipment B/Ls. A received for shipment B/L would need to have a separate notation evidencing that goods have been shipped 'on board'.

The parties typically agree as to how and where delivery is to be affected, often in frequently used shorthand terms to reflect the relative obligations of the parties. The most commonly used terms are known as international commercial terms, or Incoterms, which link delivery, payment, various dimensions of documents as well as obligations and risks of the respective parties.¹⁷ While Incoterms are the most universally used, each trade transaction can have its own shorthand terms with slightly different meanings. It should be noted that certain Incoterms only apply to certain modes of transport; some are to be used only with sea and inland waterway transport, while others are multi-modal.¹⁸

Delivery concerns that must be addressed in the agreement include where the control of the goods is passed to, the role of third-party intermediaries, whether there are documents that represent control of the goods, and how the delivery terms are linked to the payment terms.

A trade transaction almost invariably involves third parties moving the goods or holding them, which invokes questions of possession and ownership of the goods. There are a variety of options by which the control of the goods can be transferred from the seller to the buyer, each involving different benefits and risks. Financial Institutions that offer trade finance are not only familiar with the options but link their products to them, which is typically reflected in the agreement between the buyer and seller.

Movement of Goods

An integral component in the delivery of goods is their movement from seller to buyer and the mode of transport used. The mode of transport is determined by various factors including: type, quantity, and the value of the goods, and the time by when the buyer requires them to be delivered. The mode of transport can take the form of air, land or sea. When considering sea freight there are variations of container usage and routes the goods may take.

When discussing container shipment, there are two primary modes: full container load (FCL) and less than container load (LCL). A FCL "is a shipment that occupies the entire space of a container without having to share it with other merchandise. LCL, or groupage, as it is otherwise known, refers to shipments that take up only a portion of the entire container, and is shipped alongside other merchandise from other shippers in the same container."¹⁹

Another important aspect involving the delivery of goods is transshipment. Goods do not always move directly from seller to buyer, or from Point A to Point B. Transshipment "means the unloading of goods from one ship and its loading onto another to complete a journey to a further destination, even when the cargo may have to remain ashore for some time before its onward journey. But the term can also be applied more generally to other transport modes, such as freight transport by road or rail or air, or any combination of them."²⁰

¹⁷The most recent edition of these Incoterms is the 2020 revision. Incoterms also referred to Domestic and International Trade Terms.

¹⁸Byrne and Berger, *Trade Based Financial Crime Compliance*, 23–24.

¹⁹"LCL vs FCL," iContainers, accessed December 20, 2021, <https://www.icontainers.com/help/lcl-vs-fcl/>.

²⁰"Glossary: Transshipment," Eurostat, accessed December 20, 2021, <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Transshipment>.

Transit is different from transshipment, and it is important to clarify the difference between these terms, particularly in the context of sanctioned countries such as Iran. "Transit is the transport of goods through a territory where the goods remain on board the original means of transport (e.g. vessel, train or aircraft), and transshipment is the transport of goods through a territory where the goods are unloaded from one means of transport and loaded on to another means of transport (e.g. from a vessel to a train).²¹

This is relevant to sanctions due to the extent to which goods are considered to have passed through or interacted with a jurisdiction. The US Department of the Treasury states that "goods have come into contact with Iran, if, for example, they are removed from a port or airport in Iran or are processed through Iranian customs, or if they transit Iran by truck or train enroute to a destination outside of Iran."²² For example, if tomatoes are grown in Turkey and shipped to Uzbekistan via truck through Iran, the US Office of Foreign Assets Control (OFAC) would consider this to be transshipment and the goods to be of Iranian origin. On the other hand, if the goods were never removed from the port and the ship had only stopped at an Iranian port to re-fuel this would be deemed to be goods in transit. A transaction involving a port stop only is called a port of call transaction and are generally permissible as per international sanctions regulations.

Payment for Goods

The other important component of the trade agreement involves how the buyer is to effect payment. Common payment options include:

- Credit with payment due in 30, 60, or 90 days after a certain event (for example, the issuance of transport documents or the commercial invoice, or acceptance of delivery at the buyer's facility)
- Guarantee by a third party of payment on performance by the seller. The third party can include a parent or subsidiary entities, a guarantee company, or an export agency
- Payment or acceptance of a draft or bill of exchange drawn on the buyer, upon presentation by its bank of the indicated documents sent through the banking system by the seller, enabling the buyer to obtain the goods (so-called documentary or bank collection)
- Promise by the buyer to pay, backed by commercial standby LC or independent guarantee undertaking payable on demand
- Commercial LC issued by a third party in favour of the seller indicating that payment will be made against the timely presentation of certain documents
- Cash on Delivery (COD), also called "collect on delivery". Upon receipt of the goods the buyer will pay the seller
- Cash in advance, which means payment of some or all the amount due is made in advance, before delivery of the goods.²³

²¹Aaron Dunne, "The Role of Transit and Transshipment in Counterproliferation Efforts", SIPRI Good Practice Guide (Stockholm: SIPRI, September 2016), 2, https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2006_Dunne.pdf.

²²486. What Is an Example of Goods Otherwise Coming into Contact with Iran?", US Department of the Treasury, December 22, 2016, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/486>.

²³Byrne and Berger, *Trade Based Financial Crime Compliance*, 23–24.

The payment terms selected by the parties will depend on a number of factors, including the relationship between the buyer and seller, the availability of facilities and working capital to the buyer and the seller, and the countries involved in the transactions. The following section provides an in-depth explanation of the six main payment methods available to the buyer and the seller in international trade finance, highlighting the benefits and risks of each to the buyer and the seller.

Open Account

Open account trade is the most common payment method in international trade; over 80 per cent of world trade is conducted on open account terms.²⁴ In an open account transaction, the seller will despatch their goods to the buyer and send an invoice (and any other customary or required documents) direct to the buyer, requesting payment or an agreement for the buyer to pay on a specified date. If the goods are shipped by sea, the goods are consigned to the buyer and the documents of title will be sent direct to the buyer; if the goods are despatched by air, then the goods are consigned directly to the buyer. A set date for payment is given and the buyer remits the necessary funds to the seller as agreed.

Open account arrangements therefore require the seller to place a considerable amount of trust on the buyer. Once the goods have been despatched or services delivered, a seller will lose all control over payment, and is reliant on the trustworthiness and creditworthiness of the buyer. Where necessary, sellers can seek to obtain credit insurance on their overseas debtors and can use an export invoice discounting facility to accelerate cash flow.²⁵

It is particularly useful in transactions involving shipments that occur regularly, where the importer often makes payments at set intervals for goods received during a preceding period. In many cases, sellers will assign limits to their buyers that determine how large the buyer's unpaid balance can be; the size of the limit depends on the creditworthiness of the buyer. As long as the buyer meets the payment terms of the contract and the outstanding balance remains within the limit, the delivery of goods will continue. However, should the buyer delay payment or default on it, the limit will become overdrawn, and the seller may stop delivering goods. In some cases, such limits can be secured by payment guarantees issued by the buyer's bank or by a credit insurance policy.²⁶ The seller's credit department has an important role to play — they must monitor the buyer's position, and may have to intervene and stop the delivery of goods if the buyer stops paying or looks to be less creditworthy than previously thought.²⁷

If the buyer and the seller decide to trade via open account arrangement, the financial institution(s) that facilitate(s) the movement of the agreed funds will usually only see the details of the buyer and the supplier in the payment message.²⁸ On some occasions there may be additional information in the message, for example an invoice number enabling the seller to reconcile the payment from the buyer. This invoice number may be the only identifiable information that a financial institution sees which would indicate that this payment is for the purchasing of goods or services. This limited information presents a number of challenges for the financial institution to identify and mitigate TBFC, especially taking into consideration the amount of trade which is settled this way.

²⁴London Institute of Banking & Finance, *Certificate of International Trade and Finance Manual* (London: London Institute of Banking & Finance, 2019), 107, <https://www.libf.ac.uk/study/professional-qualifications/trade-finance/certificate-in-international-trade-and-finance>.

²⁵Export invoice discounting facility is a type of short-term trade finance that allows the seller to sell their receivables (i.e. payment from the buyer) to a third party for an advanced, albeit discounted, payment rather than waiting to receive payment from the buyer directly.

²⁶Payment guarantees cover the risk of nonpayment, that is if the buyer does not pay the seller for goods delivered.

²⁷London Institute of Banking & Finance, *CITF Manual*, 107.

²⁸The payment message is most likely to be sent via the SWIFT network, a member-owned cooperative that facilitates safe and secure financial transactions for its members. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) uses a standardized proprietary communications platform to send payment orders between Financial Institutions.

Payment in Advance

Payment in advance refers to payment by the buyer for the goods or services prior to receiving them; once the seller is in receipt of the funds, they arrange for the goods to be despatched. From the seller's point of view, receiving payment in advance of the shipment or providing the services is an ideal situation, as it seemingly eliminates all the risks associated with non-payment.

However, risks can still be present depending on the type of payment. For example, if payment is made by a cheque issued by a foreign bank, the risk of non-payment remains until the cheque clears and is honoured. Some sellers may accept payment by credit card; in the event that a fraudulent credit card is used, then the seller's merchant processor may reclaim the money from the seller's account.

From the buyer's point of view, payment in advance carries the greatest risk, as it is wholly dependent on the seller shipping the correct goods or providing the services in accordance with the contract. In addition, payment in advance can create cash-flow problems for the buyer, as they have to wait to receive the goods or services. Occasionally, a transaction can be arranged where a partial payment is made in advance (for example, a deposit of 30 per cent) and the balance is paid at a later date using one of the other three methods of payment discussed below.

Open account and payment in advance can also be settled using an electronic funds transfer, such as a wire payment.²⁹ A funds transfer is a transfer of credit from one financial institution to another. To be effective, it requires a relationship management application between the sender and receiver.³⁰ Within a given country, these payment orders can be immediately effective where they are backed by the central bank (e.g. FedWire in the US), or can be run through clearing houses and be subject to their rules (for example, the Clearing House Automated Payments System (CHAPS), which is administered by the Bank of England and facilitates large money transfers denominated in British Pounds, or CHIPS, which is the largest private sector USD clearing system in the world).

Documentary Collection (DC)

To discuss documentary collection (DC), it is important to first define two terms as they relate to trade finance: "Documents" and "Collection".

"Documents" refers to financial documents and/or commercial documents:

- Financial documents include bills of exchange, promissory notes, cheques, or other similar instruments used for obtaining the payment of money
- Commercial documents include invoices, transport documents, documents of title or other similar documents, or any other non-financial documents

"Collection" refers to the handling of documents by Financial Institutions, in accordance with instructions received, in order to:

- Obtain payment and/or acceptance;
- Deliver documents against payment and/or
- Against acceptance; or
- Deliver documents on other terms and conditions (for example – against availisation³¹).

²⁹Sent, for example, via the SWIFT network.

³⁰From SWIFT, the RMA is a "SWIFT-mandated filter that enables Financial Institutions to define which counterparties can send them FIN messages. Any unwanted traffic is blocked at the sender level, reducing the operational risks associated with handling unwanted messages and providing a first line of defence against fraud." See "RMA and RMA Plus: Managing Correspondent Connections," SWIFT, July 10, 2018, <https://www.swift.com/news-events/news/rma-and-rma-plus-managing-correspondent-connections>.

³¹In some countries, a bank or other party can guarantee payment of a draft or promissory note by giving its 'avail'. By signing the note in this way on the back, the bank or other organization commits itself unconditionally to pay should the maker or drawee default. This practice is well established by legislation in most European countries - London Institute of Banking & Finance, Certified Documentary Credit Specialist (CDCS) Manual I, 2014 Edition page (42)

“**Documentary collection**” therefore refers to the collection of financial documents and / or commercial documents by a financial institution in order to execute an agreement.³²

In a DC transaction, the seller will ship or despatch their goods; however, instead of sending the documents directly to the buyer, the seller will send them via the banking system to hold pending payment or acceptance by the buyer. DC is neither the safest nor the riskiest method of settlement for either party. However, it does provide some protection for both the buyer and the seller, as well as being a simple and cheap form of securing payment. The International Chamber of Commerce’s (ICC) Uniform Rules for Collections (URC522) governs DC if the collection instruction refers to their application.³³

Commercial Documentary Credit (Letter of Credit or LC)

A letter of credit (LC) allows the buyer and the seller to contract a trusted intermediary (i.e. nominated bank) that will guarantee full payment to the seller, provided that the seller has shipped the goods and complied with the terms agreed upon.³⁴ The LC serves to evenly distribute risk between the buyer and the seller, as the seller is assured of payment when the conditions of the LC are met and the buyer is reasonably assured of receiving the goods ordered. Depending on the stage of the LC between the buyer, the seller and their respective financial institution, the LC may be termed as an Import LC or an Export LC, which may enable financing to be drawn by either the buyer or the seller.

A commercial LC is simply defined as a written undertaking by a bank (Issuing bank) given to the seller (Beneficiary) at the request of the buyer (Applicant) to pay a stated sum of money against presentation of documents, complying with the terms of the credit within a set time limit. There are three types of commercial letter of credits: Sight payment, Acceptance and Deferred Payment.

In Local LC’s, the requirements are different and the Financial Institutions are exposed to the risk of not obtaining transport documents.

Table 3 – Parties commonly involved in a letter of credit

Party	Role
Applicant or buyer	The party on whose request the credit is issued
Issuing Bank	The bank that issues a credit at the request of an applicant or on its own behalf
Beneficiary or seller	The party in whose favour a credit is issued
Advising Bank	The bank that advises the credit at the request of the issuing bank
Confirming Bank	The bank that adds its confirmation to a credit upon the issuing bank’s authorisation or request
Nominated Bank	The bank with which the credit is available, or any bank in the case of a credit available with any bank
Reimbursing Bank	The bank instructed or authorised to provide reimbursement pursuant to a reimbursement authorisation issued by the issuing bank

³²“Clean collection” means collection of financial documents not accompanied by commercial documents.

³³For more information see Appendix I.

³⁴Article 2 of the Uniform Rules of Documentary Credit defines “credit” as any arrangement, however named or described, that is irrevocable and thereby constitutes a definite undertaking of the issuing bank to honour a complying presentation. In this circumstance, “honour” means a) to pay at sight if the credit is available by sight payment; b) to incur a deferred payment undertaking and pay at maturity if the credit is available by deferred payment; or c) to accept a bill of exchange (“draft”) drawn by the beneficiary and pay at maturity if the credit is available by acceptance. For more information, see International Chamber of Commerce, *Uniform Rules for Documentary Credit (UCP600)*, E600E (Paris: International Chamber of Commerce, 2007), https://2go.iccwbo.org/uniform-rules-for-documentary-credits-config+book_version-eBook/.

This instrument, although inherently simple, can have many variations.³⁵ The following are two examples:

- **Back-to-Back Mechanism:** An LC may involve an intermediary between the buyer and the seller. In such a case, two LCs will be issued. One from the buyer to the intermediary, and another one from the intermediary to the seller. This type of LC is called back-to-back.³⁶
- **Transferable Letter of Credit Mechanism:** Transferable credit means a credit that specifically states it is “transferable”. A transferable credit may be made available in whole or in part to another beneficiary (“second beneficiary”) at the request of the primary beneficiary (“first beneficiary”).³⁷ For example, a transferred letter of credit is one that Bank A issues in favour of Bank B. Bank B then “transfers” the letter of credit through an advising bank, Bank C, to the ultimate beneficiary.

Standby Letter of Credit (SBLC)

A standby letter of credit (SBLC) is unlike other LCs and is more of a bank guarantee: it is most often used not as the primary payment method, but rather as a failsafe method or guarantee for longer-term agreements.³⁸ SBLCs can remain valid for years (known as the “evergreen clause”),³⁹ which eliminates the cost of separate LCs for each transaction with a regular client.

A SBLC promises payment only in the event that the buyer fails to make an arranged payment, or otherwise fails to meet pre-determined terms and conditions; otherwise, the buyer pays on receipt of goods or according to the credit terms arranged with the seller. Should the buyer default, the seller must then apply to the bank for payment; a relatively simple process without the burden of complicated documentation.

By its nature, a SBLC is an *irrevocable, independent, documentary, and binding* undertaking when issued, and need not so state.⁴⁰ This means that:

- Because a SBLC is *irrevocable*, an issuer’s obligations cannot be amended or cancelled by the issuer except as provided in the SBLC, or as consented to by the person against whom the amendment or cancellation is asserted
- Because a SBLC is *independent*, the enforceability of an issuer’s obligations under a SBLC does not depend on: a) the issuer’s right or ability to obtain reimbursement from the applicant; b) the beneficiary’s right to obtain payment from the applicant; c) a reference in the SBLC to any reimbursement agreement or underlying transaction; or d) the issuer’s knowledge of performance or breach of any reimbursement agreement or underlying transaction
- Because a SBLC is *documentary*, an issuer’s obligations depend on the presentation of documents and an examination of required documents on their face
- Because a SBLC or amendment is *binding* when issued, it is enforceable against an issuer whether or not the applicant authorised its issuance, the issuer received a fee, or the beneficiary received or relied on the SBLC or the amendment.

The ICC’s International Standby Practices (ISP98) governs SBLC agreements / transactions.⁴¹

³⁵The ICC’s Uniform Rules for Documentary Credit (UCP600) governs LC agreements. See Appendix I for more information.

³⁶Under Article 38 of UCP 600 transferrable LCs are discussed in detail; however, UCP600 does not mention back-to-back LCs

³⁷Under MT720 (for further details see Appendix 2) there is no “Applicant Name” field; instead, is a field for the “beneficiary”. Bank B is only authorised to change the following information: applicant name (this will be replaced by their customer’s name); expiry date (which should be for a shorter period than for Bank A); the period of presentation; unit price; the amount of the LC; and the latest shipment date or given period for shipment.

³⁸Article 1.01 states that SBLCs or other similar undertaking, however named or described, whether for domestic or international use, a) may be made subject to the Rules by express reference to them. Additionally, an undertaking subject to ISP98 Rules, referred to as a “standby”, may expressly modify or exclude their application. See James E. Byrne, James G. Barnes, and Gary W. Collyer, *International Standby Practices (ISP98)*, E590E (Paris: International Chamber of Commerce, 1998), https://2go.iccwbo.org/international-standby-practices-isp98-config+book_version-eBook/.

³⁹An evergreen contract automatically renews after the expiry date (i.e. it is automatically extended). The parties involved in the contract agree that it rolls over automatically until one gives the notice to terminate it.

⁴⁰See Article 1.06, Byrne, Barnes, and Collyer, *ISP98*, 5.

⁴¹Byrne, Barnes, and Collyer, 1.

Letter of Guarantee (LG)

The terms “guarantee” or “demand guarantee” or “independent guarantee” refer to any signed undertaking, however named or described, providing for payment on presentation of a complying demand.⁴² In trade finance, a LG is a commitment issued by a bank on behalf of the buyer to provide assurances to the seller that the bank, assuming all other parts of the sale agreement are met, will pay the seller if the buyer is unable to.⁴³

An independent guarantee is also an undertaking to honour a complying documentary presentation and is similar to a SBLC. Typically, independent guarantees are used in trade-based transactions to guarantee the performance of a product, or in lieu of a warranty.

Because of the use of the word “guarantee”, LGs are often confused with traditional dependent (accessory or suretyship) guarantees,⁴⁴ and the terms of such guarantees are often not particularly helpful in distinguishing them from one another.⁴⁵

The choice of settlement method is important. Some kind of guarantees will need advance payment to the beneficiary (the buyer, the seller or a third party as stipulated in the guarantee) and in case of default from the beneficiary then the instructing party/applicant (the buyer or the seller) may face difficulties in receiving back any funds already paid. Depending on the method used, the buyer or the seller will need to examine their position with regard to the risks they are willing to take and the bargaining position they are in.

Independent guarantees are most commonly issued subject to local law. The ICC’s Uniform Rules for Documentary Credit (UCP600) typically govern independent guarantees when they are subject to practice rules; if not, they are increasingly governed by the ICC’s Uniform Rules for Demand Guarantees (URDG 758) or the International Standby Practices (ISP98).⁴⁶

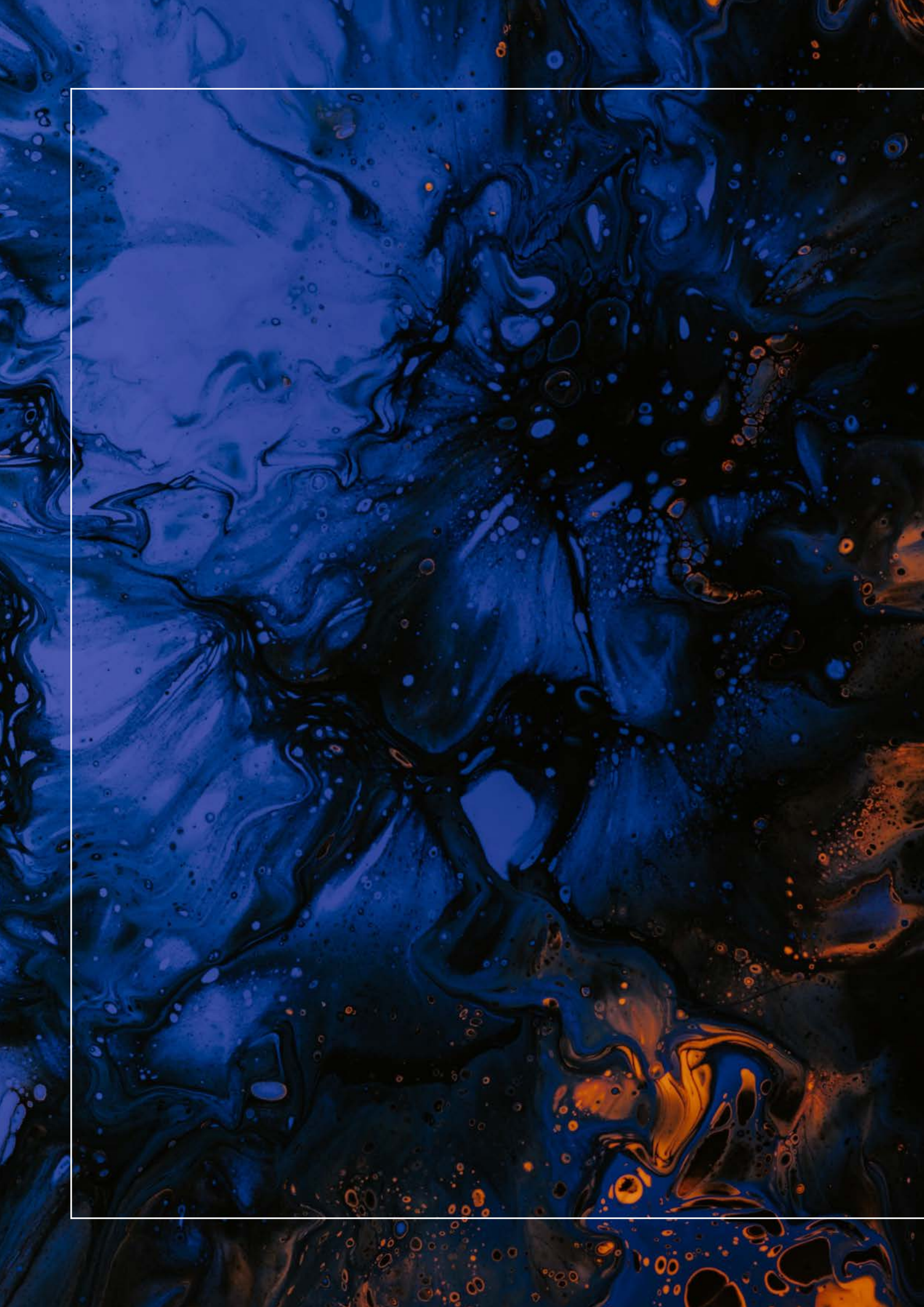
⁴²See Article 2, Georges Affaki et al., *Guide to ICC Uniform Rules for Demand Guarantees (URDG758)*, E702E (Paris: International Chamber of Commerce, 2010), X, https://2go.iccwbo.org/guide-to-icc-urdg-config+book_version-eBook/.

⁴³Many types of guarantees used in international trade, including payment guarantee, performance guarantee, advance payment guarantee, retention money guarantee, warranty guarantee, customs guarantee, tender guarantee, subcontract guarantee, court/arbitration guarantee, financial guarantee, and parent company guarantee.

⁴⁴Define traditional dependent (accessory or suretyship) guarantees create a secondary liability on the part of the guarantor.

⁴⁵See Article 5, Affaki et al., *URDG758*.

⁴⁶There is no prohibition to issue LGs subject to UCP. See Appendix I for more information.





**Trade-Based
Financial
Crime**

Trade-Based Financial Crime

Financial crime is not new. Historically, it has involved the misuse, or abuse, of the financial system for improper ends.⁴⁷ Deceit, concealment and violation of trust are at the root of these crimes. According to the Wolfsberg Group's *Trade Finance Principles*, the term "financial crime" refers to "money laundering (all crimes including but not limited to, fraud, tax evasion, human trafficking), bribery and corruption, terrorist financing, the financing of proliferation of weapons of mass destruction (WMD) and other related threats to the integrity of the international financial system."⁴⁸

Financial crime, and specifically money laundering, can involve the movement of money obtained illegally into the normal system of commerce so that it appears legitimate or hiding such funds from authorities through the financial system. It can also involve the illegal use of the financial system to misuse legitimate funds.

Money may not be the only goal of criminal enterprises, but it is necessary for them to operate; for example, terrorist organisations are politically motivated, but they still need financing to achieve their objectives. Money is necessary to pay subordinates, obtain real and personal property used to conduct the enterprise, to pay for goods and services that cannot be obtained through other means, and bribe officials and others.

Some of these crimes can inflict direct harm on people, while others involve institutional or societal harm. For example, identity theft can harm the person whose identity is stolen, whereas improper avoidance of taxes is typically a matter of harm on society.

While financial crimes can be international in nature, the remedies for them, whether civil or criminal, are rooted in the law of the nation state. Financial crime is not a specific crime in most jurisdictions, but is regarded as a category of crimes and fraudulent activities of a similar nature. For the purpose of this guidance document, any reference to financial crime includes one or more criminal acts including money laundering, terrorist financing, financing of WMD, bribery and corruption, tax evasion and fraud.

There are two major categories of financial crime: 1) money laundering, and 2) the movement of goods or money in violation of government sanctions, or prohibitions, against such movement, including support of terrorist elements. Other aspects of financial crime covered in this guidance are either subsets of or related to these activities, such as financing of WMD, bribery, commercial fraud, and circumvention of sanctioned boycotts.⁴⁹ These are known as predicate offences, so called because they are the underlying offences which generate the proceeds of crime.

While money laundering and other financial crimes are not directly related to trade or to trade finance products, TBFC has come to attract significant attention in the evolution of the efforts to control the movement of money, goods and services which support illegal activities, ranging from drug trafficking to terrorist financing. As government and private sector efforts have addressed the more obvious methods by which money and goods are moved, attention has shifted to TBFC. This presents several challenges for Financial Institutions as regulators have increased their scrutiny over the control environment and expect Financial Institutions to take steps to increase their efforts in identifying and mitigating TBFC. Due to the complexities of the financial services sector, Financial Institutions have

⁴⁷Byrne and Berger, *Trade Based Financial Crime Compliance*, 45.

⁴⁸The Wolfsberg Group, International Chamber of Commerce, and BAFT, *The Wolfsberg Group, ICC and BAFT Trade Finance Principles: 2019 Amendment* (Paris: The Wolfsberg Group; International Compliance Association; BAFT, 2019), 8, <https://iccwbo.org/content/uploads/sites/3/2019/03/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf>.

⁴⁹Byrne and Berger, *Trade Based Financial Crime Compliance*, 45.

been struggling to increase their efforts to demonstrate, in an efficient and cost-effective manner, that they have increased their control environment enough to satisfy regulators that they are able to identify and mitigate TBFC. The steps Financial Institutions can take are discussed below.

As previously stated, financial crime encompasses numerous illegal activities and can be complex in nature. Due to the fact that there no single classification of financial crime, the categories that have been chosen in this guidance document are those that are most likely to involve the misuse of trade finance products, and that are most heavily emphasised by regulators. Trade Finance products offer an added advantage of identifying and therefore mitigating TBFC due to the documents and data available providing an opportunity to better understand the client's activity. But because of the focus below on trade finance products, it is important to not underestimate the volume of trade, and therefore the potential illicit activity that exists in open account transactions. As a result, it is imperative that the financial sector assess the risks and develop mitigating plans to cover risks across the spectrum – reputational, legal, compliance, settlement, credit as well as solvency risks.

Money Laundering

The 1988 UN Vienna Convention defines money laundering as “the conversion or transfer of property, knowing that such property is derived from any offence or offence for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offence(s) to evade the legal consequences of his actions.”⁵⁰

Simply put, money laundering is the process of disguising illicit funds, which “is of critical importance, as it enables criminals to enjoy their profits without jeopardising the source”⁵¹, thereby allowing the criminal enterprise to continue. To enable criminals to use their illicit funds, they may funnel these into the traditional banking system, among other avenues.

Traditionally, there are three stages to this process (see Figure 1):

- **Placement:** The launderer introduces their illegal profits into the financial system. For example, they can break up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or purchase a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.
- **Layering:** The launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering (AML) investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.
- **Integration:** Having successfully processed criminal profits through the first two phases, the launderer then moves them to the third stage of integration, in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

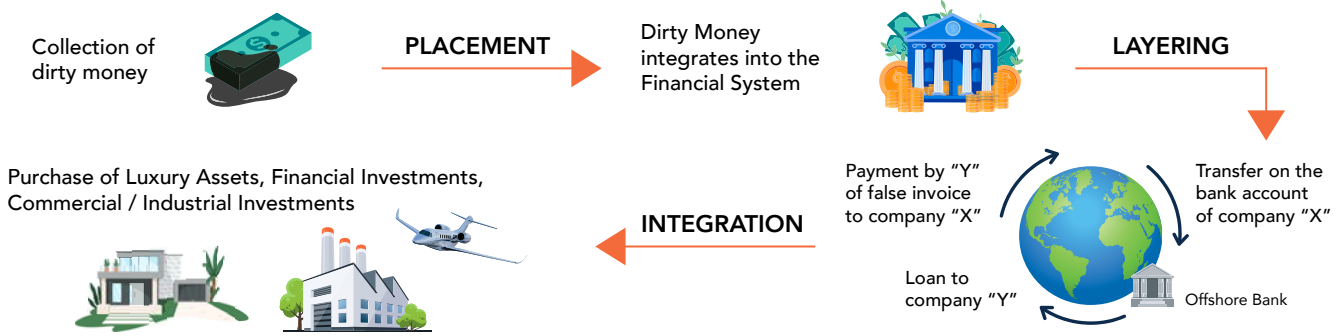
Wolfsberg's Trade Finance Principles Section 3.2.1 (Escalation Procedures) refers to what is described as “the Three Lines of Defence model”, which is recommended as the most effective approach to risk mitigation. Generally, the three lines are: 1) business operations; 2) financial crime unit scrutiny; and, 3) review.⁵²

⁵⁰United Nations, “United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances” (1988), 3, https://www.unodc.org/pdf/convention_1988_en.pdf.

⁵¹“Money Laundering,” Financial Action Task Force, accessed December 13, 2021, <https://www.fatf-gafi.org/faq/moneylaundering/>.

⁵²Trade Finance Principles Wolfsberg, et al. (2017) Section 3.2.1 (Escalation Procedures).

Figure 1 – Money laundering cycle



Source: "Money Laundering," [United Nations Office on Drugs and Crime](#)

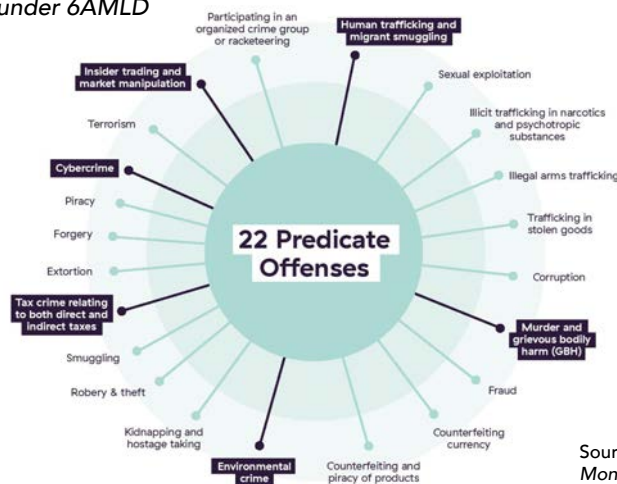
In reality, a case of money laundering may not have all three stages; some stages could be combined, or several stages repeated several times. For instance, one method of laundering cash from drug sales involves dividing cash sums into small amounts, which are then deposited by "money mules," and afterwards transferred as payment for services to a shell company. In this example, the placement and layering are done in one stage.

The United Nations Office on Drugs and Crime (UNODC) notes that "due to the clandestine nature of money laundering, it is... difficult to estimate the total amount of money that goes through the laundering cycle," however the figure of **2 to 5% of global GDP, or USD800 billion to USD2 trillion, is commonly given as the estimated amount of money laundered globally in one year.**⁵³

Money laundering cannot occur in isolation; there has to be an initial offence that renders money the proceeds of crime. As above, this is referred to as a "predicate offence" or "predicate crime". In a financial context, the predicate crime would be any crime that generates the monetary proceeds.

The EU Sixth Money Laundering Directive (6AMLD), which came into effect in June 2021, expanded the list of money laundering predicate offenses to better reflect the modern threat landscape (see Figure 2).⁵⁴ In addition, under 6AMLD, aiding and abetting money laundering as well as self-laundering now also constitute criminal acts.

Figure 2 – Predicate offenses under 6AMLD



Source: "6AMLD: 22 Predicate Offenses for Money Laundering," [Comply Advantage](#)

⁵³"Money Laundering," United Nations Office on Drugs and Crime, accessed December 13, 2021, <https://www.unodc.org/unodc/en/money-laundering/overview.html>.

⁵⁴European Parliament, "Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on Combating Money Laundering by Criminal Law," PE/30/2018/REV/1 §(2018), <https://eur-lex.europa.eu/eli/dir/2018/1673/oj>.

It is important to note that the individual(s) who launder the criminal proceeds may not be the original/same individual(s) who committed the underlying criminal offence and operate in such a way in which transactions may appear as legitimate financial activity. This challenges the ability of Financial Institutions and law enforcement agencies to fully understand the flow of funds, as some complex money laundering schemes involve multiple cross-border transactions, vehicles, and actors.

The Financial Action Task Force (FATF) defines 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 legitimise their illicit origins.”⁵⁵ As noted above, TBFC can generally be categorised as being carried out with or without document fraud; the same can be said for TBML. Regardless of whether, a trade transaction involves falsified documents, TBML schemes “vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.”⁵⁶

Trade Mis-invoicing

TBFC schemes can involve the misrepresentation of the price, quantity, or type of goods in trade transactions (i.e., trade mis-invoicing) to transfer value and disguise the origin of illicit proceeds. It is important to note that trade mis-invoicing is a *method* for illicitly moving money, that is, that it can serve as a means or technique to launder money, finance terrorism, evade taxes, or engage in other TBFC.

According to Global Financial Integrity, trade mis-invoicing “is one of the largest components of measurable illicit financial flows (IFFs) [and] represents a major global challenge on two fronts: for customs and tax authorities around the world, particularly in developing countries, trade mis-invoicing reflects the loss of USD billions in uncollected trade-related tax revenues every year; and for law enforcement, trade mis-invoicing facilitates [IFFs] throughout the global economy.”⁵⁷

There are several ways to mis-invoice trade, such as falsely inflating or deflating the price (“over-invoicing” or “under-invoicing”, respectively), shipping more or less (“over-shipping” or “short-shipping”, respectively) of a good than is declared, or falsely describing goods or services provided. More complex trade mis-invoicing schemes can involve the repeated import and export of the same goods (“carousel transactions”), not shipping any goods at all (“phantom shipping”) or creating/using two or more invoices for a single trade transaction (“double invoicing”, “duplicate invoicing” or “multiple invoicing”).

Mis-invoicing is important to TBML due to the frequency with which it is used in trade-related criminal schemes. Although technically mis-invoicing is a type of fraud, fraud schemes can encompass an extensive range of criminal schemes, many of which are not relevant to or transcend trade-based crime. Fraud schemes can also be exceptionally complex, so an in-depth discussion of fraud beyond mis-invoicing schemes is beyond the scope of this reference guide.

⁵⁵Page 5, *Trade-Based Money Laundering*, Financial Action Task Force, 23 June 2006

⁵⁶Page 5, *Trade-Based Money Laundering*, Financial Action Task Force, 23 June 2006

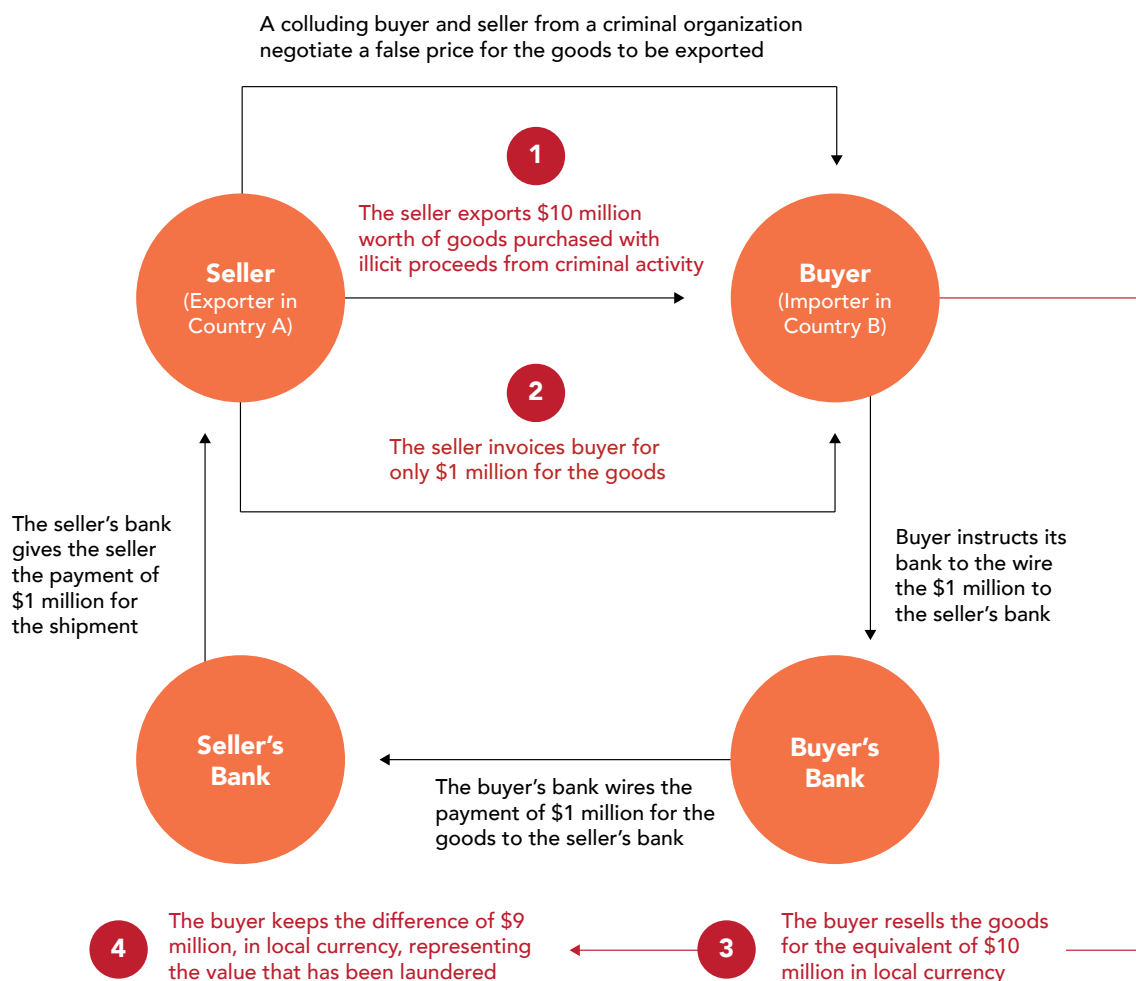
⁵⁷“Trade-Related Illicit Financial Flows in 134 Developing Countries 2009-2018,” Global Financial Integrity, December 16, 2021, <https://gointegrity.org/report/trade-related-illicit-financial-flows-in-134-developing-countries-2009-2018/>.

In some instances, the seller and the buyer could be controlled by the same organisation and be in collusion with each other. A parent company for example could set up an entity in a separate jurisdiction with weaker money laundering controls, and then sell goods to that entity at a “fair market” price, based on legitimate documents. The entity might then sell these goods on to a final purchaser, at either a lower or higher price. This process moves the location of the over- or under-invoicing scheme to another jurisdiction, thereby potentially lowering the risk of detection. The structuring could be even more complex if the parent company sets up additional entities in the chain, perhaps in additional jurisdictions. This complexity clearly presents challenges to those who are responsible for the prevention, detection and investigation of TBFC.

Under-invoicing exports is one of the most common TBFC techniques used to move money. This is likely due to the fact that the primary focus of most customs agencies is to stop the importation of contraband and ensure that appropriate import duties are collected. Thus, customs agencies generally monitor exports less rigorously than imports.⁵⁸

As a result, Figure 3 below shows how a criminal organization operating between two countries can misrepresent the price of the goods being exported from Country A to Country B to launder illicit proceeds and transfer value.⁵⁹

Figure 3 – TBML scheme with trade mis-invoicing



Source: Government Accountability Office, [Trade-Based Money Laundering](#)

⁵⁸Financial Action Task Force, *Trade Based Money Laundering* (Paris: Financial Action Task Force, 2006), 5, <https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf>.

⁵⁹US Government Accountability Office, *Trade-Based Money Laundering: US Government Has Worked with Partners to Combat the Threat, but Could Strengthen Its Efforts* (Washington, D.C.: US Government Accountability Office, 2020), 6, <https://www.gao.gov/assets/gao-20-333.pdf>.

Money launderers can also use criminal proceeds to purchase goods or services that are then imported or exported without having to manipulate the trade documents (i.e. no trade mis-invoicing). This type of TBML scheme is commonly referred to as the black-market peso exchange (BMPE). In a BMPE scheme:

The value of the criminal proceeds is converted from liquid (typically cash) to a commodity (e.g. electronics or clothing) in one jurisdiction and currency (e.g. the US in US dollars) and then converted back to liquid (e.g. cash or bank transfer) in another jurisdiction and currency (e.g. Mexico and Mexican pesos). This conversion of value means that the proceeds are able to be moved from one country to another without the use of the financial system. In a BMPE scheme, there is no need to manipulate the value of the trade transaction, as the goods themselves embody the criminal proceeds.⁶⁰

Service Based Money Laundering (SBML)

Among the tactics used in financial crimes is the often-ignored problem of service-based money laundering (SBML). Like the TBML trade mis-invoicing scheme described above, SBML involves the manipulation of invoices related to the trade in services. Compared to TBML, SBML can present additional challenges because “when investigating TBML, authorities can often track an item or a commodity, following a physical trail. SBML, by contrast, leaves no physical commodity trail, and the value of an invoice is subjective”.⁶¹

The US Department of State’s extended 2015 global money laundering review provides a good example of an SBML methodology originating in Montenegro, whereby “offshore companies send fictitious bills to a Montenegrin company (for market research, consulting, software, leasing, etc.) for the purpose of extracting money from the company’s account in Montenegro so funds can be sent abroad.”⁶² SBML arrangements often comprise services that are complex and/or difficult to quantify, such as concert promotions or writing computer code.⁶³

Another SBML methodology involves the use of consultancy firms, which are businesses that, quite simply, provide expert advice for a fee. Such firms can be fairly easy to set up, especially in offshore or secrecy jurisdictions; a complex network of consultancy firms can be established to facilitate moving illicit funds between jurisdictions.⁶⁴ Criminals as well as so-called “gatekeepers” can use a consultancy firm to justify the movement of funds, representing (or rather, misrepresenting) the financial flows as the payment or receipt of consultancy fees. In addition, “while money laundering tends to be expensive in other business sectors, the consulting sector provides a potentially profitable alternative for money launderers, largely due to tax benefits obtained through the involvement of offshore companies.”⁶⁵

FATF and the Egmont Group under their 2020 TBML report specifically highlighted that 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
- Trademarks and similar intangible items such as intellectual property rights

⁶⁰Julia Yansura et al., *Financial Crime in Latin America and the Caribbean: Understanding Country Challenges and Designing Effective Technical Responses* (Washington, D.C.: Global Financial Integrity, 2021), 162, <https://gfinetegrity.org/report/financial-crime-in-latin-america-and-the-caribbean/>.

⁶¹John Cassara, “Service-Based Money Laundering: The Next Illicit Finance Frontier,” Foundation for Defense of Democracies, May 19, 2016, <https://www.fdd.org/analysis/2016/05/19/service-based-money-laundering-the-next-illicit-finance-frontier/>.

⁶²US Department of State, *Money Laundering and Financial Crimes Country Database* (Washington, D.C.: US Department of State, 2015), 308, <https://2009-2017.state.gov/documents/organization/239329.pdf>.

⁶³Cassara, “Service-Based Money Laundering.”

⁶⁴Fabian M. Teichmann and Madeleine Camprubi, “Money Laundering Through Consulting Firms,” *Compliance Alliance Journal* 5, no. 2 (2019): 69–70.

⁶⁵Teichmann and Camprubi, 72.

Terrorism Financing

Terrorism is a complex problem, with diverse origins and actors. Likewise, “any attempt to understand the motivations and actions of terrorist individuals and groups must... take into account that enormous diversity.”⁶⁶

Defining “terrorism” is difficult and modern definitions are inherently controversial. This document uses the definition given in the Arab Convention for the Suppression of Terrorism, which was adopted by the Council of Arab Ministers of the Interior and Council of Arab Ministers of Justice in Cairo, Egypt in 1998. The Convention defines terrorism as:

Any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardised national resources.⁶⁷

Trade Based Terrorism Financing (TBTF) utilises trade processes the same way they are vulnerable to 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, the report defines TBTF as “disguising the movement of value through the use of trade transactions in an attempt to finance terrorism, whether from legitimate or illegitimate sources”. However, given the (low) values usually involved and the additional layers of complexity, detecting TBTF schemes is inherently more difficult.⁶⁸

The *Global Terrorism Index 2020* reported that there were 13,826 deaths in 2019 due to terrorism.⁶⁹ Besides the significant cost to human life, the economic impact of terrorism was estimated at USD26.4 billion the same year.⁷⁰ While terrorist attacks can occur anywhere in the world, fatalities in the MENA region have accounted for 40% of the global total deaths from terrorism since 2002.⁷¹

Terrorist Groups in the Middle East and Africa

The United Nations Security Council (UNSC) has designated the following MENA-based groups as terrorist organisations:

- Under resolution 1267 (1999) and successor resolutions, Al-Qaida or ISIL (Da'esh) and other individuals, groups, undertakings and entities associated with them. More than 80 terrorist entities are listed on the UN website under this category
- The ISIL-associated Al Nusra Front is listed under resolution 2170 (2014)
- Under resolution 1988 (2011), individuals and entities associated with the Taliban, including the Haqqani Networks

⁶⁶Walter Reich, *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind* (Woodrow Wilson Center Press, 1998), 1.

⁶⁷League of Arab States, “The Arab Convention For The Suppression of Terrorism,” Cairo § Council of Arab Ministers of the Interior and Council of Arab Ministers of Justice (1998), 2.

⁶⁸FATF-Egmont 2020 TBML report - Page (12).

⁶⁹Institute for Economics & Peace, *Global Terrorism Impact 2020: Measuring the Impact of Terrorism* (Sydney: Institute for Economics & Peace, 2020), 2, <https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf>.

⁷⁰Institute for Economics & Peace, 2.

⁷¹Institute for Economics & Peace, *Global Terrorism Impact 2020*.

The lists on the UN website are regularly updated and the most current information can be found at:

- Al-Qaida or ISIL: https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries;
- Taliban: <https://www.un.org/securitycouncil/sanctions/1988/materials/summaries>

al-Qaeda - a radical Islamist terrorist group whose origins stem from the Soviet war in Afghanistan

ISIS and ISIL - ISIS and ISIL are the same group translated slightly differently (Islamic State of Iraq and Syria or Islamic State of Iraq and the Levant). ISIS is a radical Islamist terrorist group that splintered from al-Qaeda and is based in Syria

IS - (Islamic State) a radical Islamist terrorist group formed from ISIS/ISIL but broadening its geographic area worldwide, claims authority over all jihadist groups⁷²

The financing of terrorism can be described as the process by which a person tries to collect or provide funds for the purpose of carrying out a terrorist act by a terrorist or a terrorist organization, as defined in the International Convention for the Suppression of the Financing of Terrorism.⁷³

The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organisations the opportunity to transfer value and goods through seemingly legitimate trade flows.

The specific methods and techniques used to launder money through the trade system were described in the 2006 FATF Report on TBML, although terrorist financing was not a focus of that work. Further examination of the specific methods and techniques used to exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

Terrorist use of the trade sector to move funds

The following case study is from Belgium and is taken directly from the 2006 FATF Trade Based Money Laundering Report

An FIU received disclosures from several banks concerning account holders: Persons A and B and Company C, all active in the diamond trade. In the space of a few months, A, B and C's accounts saw a large number of fund transfers to and from foreign countries. Moreover, soon after the opening of his account, person B received several bank cheques for large amounts in US dollars.

Financial information collected by the FIU showed that Company C received large US dollar transfers, originating from companies active in the diamond industry and debited by several transfers to the Middle East in favour of Person A, a European citizen born in



**CASE
STUDY**

⁷²Hot Topics: Terrorism in the Middle East: Terrorist Groups," University of Maine, accessed December 16, 2021, <https://libguides.library.umaine.edu/c.php?g=144444&p=2961556>.

⁷³United Nations, "International Convention for the Suppression of the Financing of Terrorism" (1999), https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en.

Africa and residing in the Middle East. One of the directors of Company C, a Belgian citizen residing in Africa, held an account at a bank in Belgium through which transfers took place to and from other countries in Europe, Africa, North America, and the Middle East. Inward transfers from foreign countries mainly took place in US dollars. These were then converted to EUR and used to make transfers to foreign countries and to accounts in Belgium belonging to Person B and his wife.

Police information collected by the FIU showed that the prosecutor had opened a file related to trafficking in diamonds originating in Africa. The largest transfers of funds by the company trading in diamonds were mainly destined to the same person, A, residing in the Middle East. Police sources revealed that both Person A and Person B were suspected of having bought diamonds from the rebel army of an African country and of smuggling them into Belgium for the benefit of a terrorist organisation.

Moreover, it appeared that certain persons and companies linked with Persons A and B had already been referred to prosecutors by the FIU in other cases for money laundering derived from organised crime.⁷⁴

Proliferation Financing

The proliferation of nuclear, chemical and biological weapons (weapons of mass destruction or WMD) and their delivery systems is a major threat to international peace and security. Currently, state actors are seen as the main sources of the threat. The WMD programmes of North Korea, Iran and Syria are subject to either UN sanctions or unilateral sanctions (imposed by the EU or individual States). Other WMD programmes, such as those of India and Pakistan, are not subject to such sanctions although individual countries (such as the US or UK) may have controls in place to prevent exports of proliferation-sensitive equipment, materials and technology. However, States are not the only source of proliferation threats. For example, a procurement network set up by a Pakistani nuclear scientist, A.Q. Khan, became notorious for having supplied proliferation-sensitive equipment and technology to Libya, North Korea and Iran on a commercial basis until it was dismantled in 2003.

In 2016, the then Financial Action Task Force (FATF) President Ji-Yoon Shin argued to the United National Security Council (UNSC) that financial measures were “one of the most effective tools to counter proliferation.”⁷⁵ He highlighted the importance of effective financial measures:

- Preventive measures make it difficult for criminals to raise and move funds, reducing the capacity of proliferation networks
- Financial intelligence provides advance warning of attempts to illegally transfer sensitive goods and materials. Shipments can be discovered and interdicted on the basis of suspicious transaction reports submitted by Financial Institutions
- Every movement of goods has an associated financial transaction [so that investigators] can follow money trails to look behind declarations, analyse proliferation networks, and identify facilitators.⁷⁶

The UNSC has approved a number of resolutions that require States to take measures to counter proliferation financing (PF):

- Resolution 1540 (2004) is targeted at proliferation of WMD by non-state actors
- Resolution 2231 (2015) is directed at Iran’s nuclear activities and includes PF-related targeted financial sanctions

⁷⁴Financial Action Task Force, *Trade Based Money Laundering*, 16.

⁷⁵“FATF President Juan Manuel Vega-Serrano’s Remarks at the Meeting of the UN Security Council, December 15, 2016,” Financial Action Task Force, December 15, 2016, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-vega-serrano-un-security-council-meeting-dec2016.html>.

⁷⁶“FATF President Juan Manuel Vega-Serrano’s Remarks.”

- Resolution 1718 (2006) and successor resolutions are focused on North Korea's (DPRK's) WMD programmes and include PF-related targeted financial sanctions

Like terrorist financing (TF), there is no universally agreed upon definition of proliferation financing (PF), although the FATF published an informal definition in 2010, based on UNSC Resolution 1540, which is widely used:

“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, transshipment, 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 nonlegitimate purposes), in contravention of national laws or, where applicable, international obligations.⁷⁷

This definition:

- Takes account of proliferation by both state and non-state actors
- Excludes trade in arms and dual-use goods for legitimate purposes
- Deals with the act of proliferation financing and excludes issues of knowledge, intention, or negligence
- Extends to related financial services (not simply financial transactions)
- Includes chemical, biological and nuclear weapons, means of their delivery and also “related materials” (a term defined in resolution 1540 (2004) as including technologies and dual-use goods).

The implementation of UNSC sanction resolutions on Iran and DPRK does not necessarily equate to countering proliferation financing as defined by the FATF. Furthermore, the FATF Recommendations make no reference to Resolution 1540 and are focused exclusively on targeted financial sanctions.⁷⁸ To help identify PF, the FATF, as well as States, academic organisations, and think tanks have published guidance and information related to PF typologies and PF risk assessments.⁷⁹

WMD-related illicit procurement of equipment, materials and technology can look very much like legitimate international trade, and characteristically involves:

- Industrial items that may or may not be dual-use, and may or may not be listed for export control⁸⁰
- Transactions that normally take place through formal financial channels
- Complex networks of procurement agents and front companies across multiple jurisdictions
- Deceptive practices by procurement agents intended to hide the destination of proliferation-sensitive shipments or sources of funding (which may be entities or countries under sanctions).

Proliferation financing may therefore be difficult to distinguish from the financing of legitimate international trade. As a further complication, international trade financing takes place mainly in two ways: First, using trade finance products offered by international and local Financial Institutions to

⁷⁷Financial Action Task Force, *Combating Proliferation Financing: A Status Report on Policy Development and Consultation* (Paris: Financial Action Task Force, 2010), 5, <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>.

⁷⁸Recommendation 1 includes a requirement on states and Financial Institutions to conduct proliferation financing risk assessments; Recommendation 2 relates to domestic cooperation and coordination in countering proliferation financing; Recommendation 7 relates to implementation of UNSC proliferation finance-related targeted financial sanctions; and Recommendation 15 extends the requirements of these recommendations to virtual asset service providers.

⁷⁹For a list of some of the primary resources on PF typologies and risk assessments, see Appendix I: Recommend Resources

⁸⁰For example, under [Nuclear Suppliers Group](#), [Missile Technology Control Regime](#) or other export arrangement guidelines

help their customers make payments and manage risks; and second, by means of inter-firm trade credit between buyers and sellers. LCs are the most commonly used form of trade finance. Inter-firm trade credit can consist of both open account transactions (as described above, goods are shipped in advance of payment) and cash-in-advance transactions (payment is made in advance of shipments). Estimates for the proportion of international trade that takes place through bank-intermediated trade finance versus inter-firm trade credit varies, however as outlined above the Wolfsberg Group estimates that typically about 20% of world trade takes place on trade finance terms.

The divide between trade conducted on trade finance terms and trade conducted on open account terms is important to assessments of proliferation finance risk. Over half of the case studies in a FATF Typologies Report published in 2008 involved trade financing.⁸¹ But a study published by King's College London in 2017 found that trade finance was involved in a proportionally much smaller number of cases of proliferation financing.⁸² This contrast may reflect inadequate data, but it could also reflect changes in financial techniques used by proliferators, particularly if LCs are becoming less used in international trade in general.

Trade finance-related transactions offer more opportunities for banks to carry out due diligence than open account transactions (as described below in the chapter on Transaction Monitoring). Banks involved in trade finance typically require copies of relevant documents, such as invoices, bills of lading and export licences (if necessary) relating to the shipments concerned. Information in these documents can be checked against trade-related risk indicators including proliferation finance.⁸³ Open account transactions, by contrast, are usually accompanied by SWIFT MT103 messages, which typically provide little information on the underlying transaction.⁸⁴ In such cases, Financial Institutions need to rely on a combination of risk assessments along with customer and transaction monitoring (incorporating FATF's indicators into existing ML/TF monitoring procedures; for an overview of risk indicators see Appendix VI) to mitigate the risk of involvement in PF.

Proliferation Financing: Vacuum pumps from the Netherlands to Iran

The following case was adapted from Case 26 of the *Study of Typologies of Financing of WMD Proliferation* report.⁸⁵ It illustrates many of the most common proliferation financing indicators.⁸⁶

According to information supplied by the Customs Administration of the Netherlands, in 2011 a Netherlands company attempted to export a shipment of Viton "O" rings to Iran by courier. The shipment was intercepted by Netherlands Customs. The items required a licence for export, but no licence had been applied for. Investigations by the authorities revealed that the company concerned was a small Dutch trading company that had been set up in 1997 by an Iranian living in Germany, close to the Dutch border. According to Chamber of Commerce databases, the company was a wholesaler trading ferrometals. The company accounts were poorly organised. The authorities confiscated the "O" rings and sent a warning letter to the company.

CASE STUDY

⁸¹See Financial Action Task Force, *Proliferation Financing Report* (Paris: Financial Action Task Force, 2008), <https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>.

⁸²Jonathan Brewer, *Study of Typologies of Financing of WMD Proliferation* (London: King's College London, 2017), <https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf>.

⁸³See Appendix VI for a list of possible proliferation financing indicators collected from the FATF as well as other sources.

⁸⁴SWIFT (Society for Worldwide Interbank Financial Telecommunication) MT103 payment messages are used specifically for cross-border payments. See "Open Account" page 9 above; Although Field 70 of MT103s can be used to include remittance information it is not mandatory and so in practice SWIFT 103 messages contain little information that could be used to screen for proliferation financing.

⁸⁵Brewer, *Study of Typologies of Financing of WMD Proliferation*, 110.

⁸⁶See Appendix VI: Proliferation Financing Indicators for more information.

A year later Dutch authorities received an export declaration from the same company for a shipment to a consignee in Tehran, Company A, of materials described as “equipment for glass production” (Figure 4). The shipment was stopped and found to comprise 22 turbo vacuum molecular pumps manufactured and supplied by a company in another EU State, valued at EUR 232,500. These pumps were listed under EU sanctions regulations in force at the time as being of potential use in Iran’s nuclear programme. The company had made no attempt to obtain an export licence, and Dutch authorities carried out further investigations of the company.

These investigations showed that, as the previous year, the trading company’s accounts were incomplete. Although on paper it appeared that the company carried out a lot of business, in fact little of this was substantive and the company appeared to have no other business in the Netherlands. The authorities found a number of fake invoices. The authorities also noted that the owner often used a Dutch or German sounding name on emails rather than his real, Iranian name.

The trading company had told the supplier in the other EU State that the vacuum pumps were destined for a new glass company in Turkey, but according to documentation accompanying the shipment, the consignee was a company in Tehran, Company A. Furthermore, investigations revealed an email from another company in Tehran, Company B, asking the trading company to change the name of the consignee from Company B to Company A. Further investigations showed that Company B was a front company for the Iranian nuclear programme.

In order to finance the vacuum pump deal, the trading company had received five payments by wire transfer into an account at a local Dutch bank from companies based overseas during a four-month period in 2011. The authorities noted that in addition to the attempted export of these pumps to Iran without a licence, the trading company had never applied for a licence to receive these payments as required by EU regulations in force at the time.⁸⁷ Investigations of these five companies showed that they did not all have a website. They were presumably set up specifically to finance this deal (and perhaps other deals elsewhere).

Prior to shipment of the vacuum pumps to Iran in May 2012, the trading company paid the supplier in instalments over a five-month period in 2011. Although the total cost of the vacuum pumps was EUR 232,500, a total of about EUR 239,800 was paid into the trading company’s banks account, suggesting that the company made a profit of about EUR 7,300 on the deal.

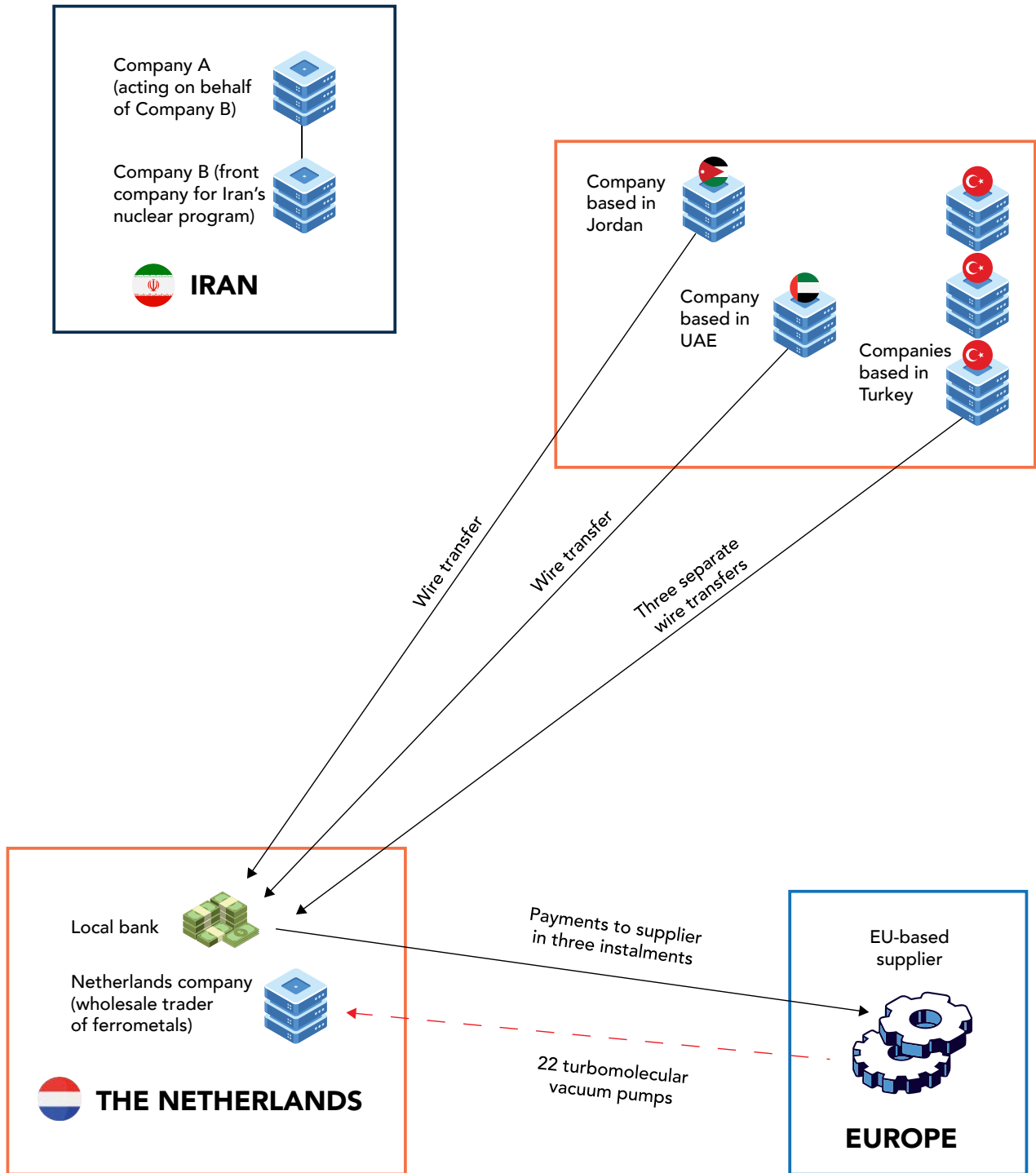
Following investigations by the authorities, the bank closed the trading company’s account. The bank had no records of additional transactions involving the five entities. The pumps were confiscated and sold into the local market by the Netherlands’ authorities. The proceeds were used to settle a tax bill owed by the company.

Although the case is ten years old, proliferation financing methodologies have probably not changed significantly since then. Whilst traditional methods work, proliferators will continue to use them.

As noted above, financing proliferation is not necessarily equivalent to evasion of sanctions, but according to reports of the UN Panel on DPRK, North Korean proliferation financiers are making increasing use of cyberattacks to raise funds which could be used for PF, as well as cryptocurrencies. If cryptocurrencies become used in international trade it seems likely that DPRK would use them for PF purposes, for example to pay for procurement of goods. FATF, to a certain extent, has future-proofed PF risks in this respect because virtual assets and virtual asset service providers need to be included in the risk assessments conducted by states and Financial Institutions under FATF’s Recommendation 1.






⁸⁷EU Regulations (961/2010) in force at the time required a licence for financial transactions involving Iran larger than EUR 40,000, so the company should have applied for a licence for three of the five payments and notified the authorities of the other two payments.

Figure 4 – The relationship and financial transactions between entities involved in the Dutch company’s procurement of vacuum pumps and their attempted shipment to Company A in Iran



The trading company received and originated payments connected with the pumps according to the schedule seen in Table 4.

Table 4 – Trading company transactions

Date	Payment received by trading company	Amount (€)	Description attached to payment	Action by trading company
March 2011	 Turkey	36,185.00	Invoice No...	
March 2011				Payment to supplier
11 April 2011	 UAE	44,926.00	Business transaction	
14 April 2011	 Turkey	25,000.00		
14 April 2011	 Jordan	55,480.00	Purchase	
15 April 2011				Payment to supplier
2 June 2011	 Turkey	68,220.00	Based on First Glass	
12 July 2011				Payment to supplier
May 2012				Attempted export of vacuum pumps

This case of proliferation financing illustrates the following:

- Involvement of dual nationals, a small trading company, and a company appearing to do little genuine business
- Persistence – although the company had previously come to the attention of the Dutch authorities, it continued attempting to export goods without a licence
- Unusual patterns of financial transactions – the large payments through the Dutch company's bank account in connection with the purchase of the pumps were not consistent with the company's normal business
- Payments – received from different companies based in different countries, that together enabled the supplier of the pumps to be paid
- Payments accompanied by vague and generalised descriptions of their purpose
- Involvement of companies with no website
- Transactions involving countries of diversion concern (Turkey and the UAE were, contemporaneously, considered as countries through which goods or finances may be channelled in order to circumvent sanctions)
- An apparent consignee of a proliferation-sensitive shipment acting on behalf of a front company of a programme of proliferation concern.



For additional red flags and risk indicators, refer to **Appendix VI**.

Tax Crimes

Taxes can be described as:

- a sum of money demanded by a government for its support or for specific facilities or services, levied upon incomes, property, sales, etc.
- a charge, obligation, duty, or demand.⁸⁸

The World Bank explains that collecting taxes “is a fundamental way for countries to generate public revenues that make it possible to finance investments in human capital, infrastructure, and the provision of services for citizens and businesses.”⁸⁹

While the words “avoid” and “evade” are quite similar in definition, the meanings of “tax avoidance” and “tax evasion” are radically different. Tax avoidance refers to the act of lowering “your tax bill by structuring your transactions so that you reap the largest tax benefits. Tax evasion, on the other hand, is an attempt to reduce your tax liability by deceit, subterfuge, or concealment.”⁹⁰ Simply put, tax avoidance is legal whereas tax evasion is illegal.

Over recent years, the media as well as policymakers and researchers have paid increasing attention to the subject of aggressive tax avoidance (also known as aggressive tax planning), whereby multinational companies have, in some instances, exploited mismatches and loopholes in the international tax framework to reduce their overall tax burden.⁹¹ According to the International Monetary Fund, “many jurisdictions have adopted a general anti-avoidance rule (GAAR)... [which] is a provision of last resort that is capable of being invoked by a tax authority to strike down unacceptable tax avoidance practices that would otherwise comply with the terms and statutory interpretation of the ordinary tax law.”⁹²

Research by the Tax Justice Network found that countries around the world lose more than USD427 billion annually due to individual tax evasion and multinational corporate profit-shifting.⁹³

Tax regulation and legislation can be complex and differ from country to country. Tax evasion, as noted above, is a criminal act where an individual or entity uses illegal methods to avoid paying taxes for which they are legally liable. Governments and regulators have adopted new policies to combat these practices, with a particular focus on strengthening financial reporting and information sharing. Examples include the Standard for Automatic Exchange of Financial Account Information in Tax Matters, developed by the Organization for Economic Co-Operation and Development (OECD), together with G20 countries and in close cooperation with the EU as well as other stakeholders in;⁹⁴ the Foreign Account Tax Compliance Act (FATCA),⁹⁵ introduced by the United States in 2010; and 2012⁹⁶ amendments to FATF Recommendations to better prevent tax crimes.

⁸⁸“Definition of Tax,” Dictionary.com, accessed December 17, 2021, <https://www.dictionary.com/browse/tax>.

⁸⁹“Taxes & Government Revenue,” World Bank, accessed December 17, 2021, <https://www.worldbank.org/en/topic/taxes-and-government-revenue>.

⁹⁰“Tax Avoidance Is Legal; Tax Evasion Is Criminal,” Wolters Kluwer, November 6, 2020, <https://www.wolterskluwer.com/en/expert-insights/tax-avoidance-is-legal-tax-evasion-is-criminal>.

⁹¹Ernesto Zangari, Antonella Caiumi, and Thomas Hemmelgarn, “Tax Uncertainty: Economic Evidence and Policy Responses,” Taxation Papers (Brussels: European Commission, 2015), 26–27, https://ec.europa.eu/taxation_customs/system/files/2017-04/taxation_paper_67.pdf.

⁹²Christophe Waerzeggers and Cory Hillier, “Introducing a General Anti-Avoidance Rule (GAAR)” (Washington, D.C.: International Monetary Fund, 2016), 1.

⁹³Mark Bou Mansour, “\$427bn Lost to Tax Havens Every Year: Landmark Study Reveals Countries’ Losses and Worst Offenders,” Tax Justice Network, November 20, 2020, <https://taxjustice.net/2020/11/20/427bn-lost-to-tax-havens-every-year-landmark-study-reveals-countries-losses-and-worst-offenders/>.

⁹⁴See Organisation for Economic Co-operation and Development, *Standard for Automatic Exchange of Financial Information in Tax Matters: Implementation Handbook; Second Edition* (Paris: OECD, 2018), <https://www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-information-in-tax-matters.pdf>.

⁹⁵See “Foreign Account Tax Compliance Act (FATCA),” Internal Revenue Service, accessed December 17, 2021, <https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca>.

⁹⁶“FATF Steps up the Fight against Money Laundering and Terrorist Financing,” Financial Action Task Force, February 16, 2012, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html>.

Illicit actors are able to engage in customs evasion in a variety of ways, “ranging from false declarations, routing goods through a low duty country to bribery and smuggling, all resulting in actual collection costs being understated. A number of features can favour tax evasion, for instance poor levels of law enforcement or distribution of tariffs.”⁹⁷ A decade ago, the Asia/Pacific Group on Money Laundering highlighted the vulnerability of duty-free zones and free-trade zones (FTZs) to TBFC. In particular, they noted that “duty-free zones or jurisdictions that have high import tax/export tax rebates are most likely to be used for TBML. Volume of trade, value of trade, type of commodity or service traded and/or domestic regulatory environment are the factors which determine the sensitiveness of a jurisdiction for TBML.”⁹⁸



For additional red flags and risk indicators, refer to **Appendix IV**.

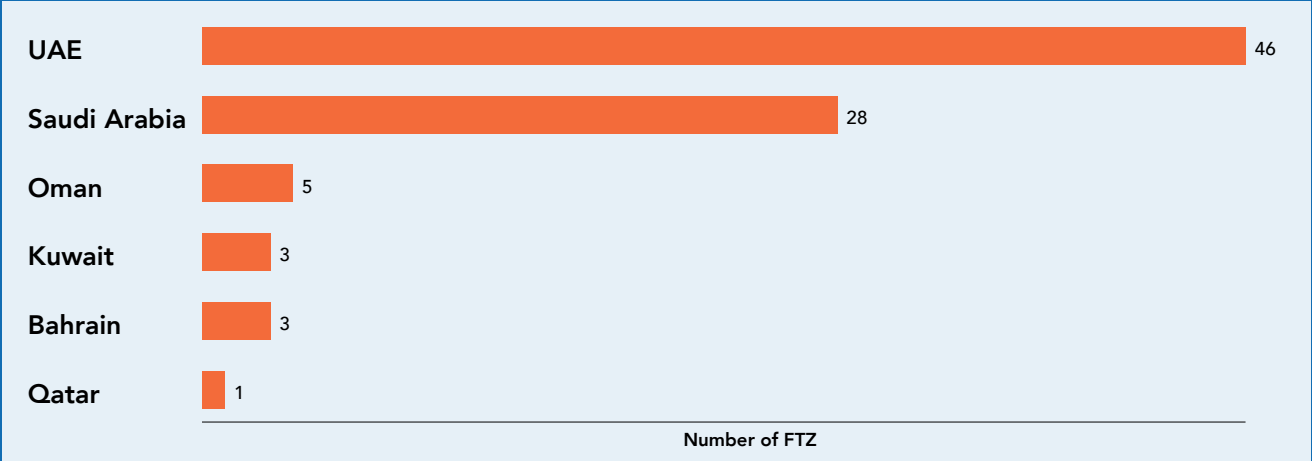
Free-Trade Zones

In the recent paper *Improving Governance and Tackling Crime in Free-Trade Zones*, the Royal United Services Institute highlights the features of free trade zones (FTZs) that attract both licit and illicit actors:

FTZs are designed to attract trade by suspending the collection of customs duties. These incentives are frequently coupled with advantages such as simplified customs inspection procedures, liberalized incorporation regimes and physical infrastructure superior to that available elsewhere in the same country. These features can be attractive to legitimate businesses and criminal groups alike. International organisations such as the OECD, the World Customs Organisation, the Financial Action Task Force and the EU have all highlighted criminal risks related to FTZs.⁹⁹

The OECD advises that there are over 3,500 FTZs across 130 countries which offer reduced tariffs and taxes, generating jobs and growth along with attracting foreign investment.¹⁰⁰ One estimate put the number of FTZs in the Middle East at 160.¹⁰¹

Figure 5 – Number of FTZs in the Gulf Region



Source: “Number of free trade zones (FTZ) in the Gulf Cooperation Council in 2018, by country,” *Statista*

⁹⁷Sébastien Jean and Cristina Mitaritonna, “Determinants of and Pervasiveness of the Evasion of Customs Duties,” CEPII Working Paper Number 2010-26 (CEPII, November 2010), 10.

⁹⁸Asia/Pacific Group on Money Laundering, “APG Typology Report on Trade Based Money Laundering” (Sydney: Asia/Pacific Group on Money Laundering, 2012), 35, http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf.

⁹⁹Anton Moiseienko, Alexandria Reid, and Isabella Chase, *Improving Governance and Tackling Crimes in Free-Trade Zones* (London: Royal United Services Institute, 2020), vii, https://static.rusi.org/20201012_ftzs_web_2.pdf.

¹⁰⁰“OECD Recommendation on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones,” Organisation for Economic Co-operation and Development, October 21, 2019, <https://www.oecd.org/gov/risk/recommendation-enhancing-transparency-free-trade-zones.htm>.

¹⁰¹“The Middle East Free Zones,” Sohatoos, accessed March 22, 2022, <https://sohatoos.com/en/the-middle-east-free-zones>.

Due to the perception that all are generically high risk, FTZs present a number of challenges to businesses seeking to set up in such zones, especially when they endeavour to obtain banking services. As the regulatory and rules landscapes vary across FTZs, no two zones are the same; therefore, certain zones may present a higher financial crime risk than others.

Research has identified several typical characteristics of FTZs that make them attractive for illicit trade purposes, including:

- Their role as common transit locations, which provides the opportunity to: repackage and relabel goods; forge key documentations, such as bills of lading or certificate of origins; and commingle licit and illicit goods
- The availability of infrastructure to manufacture or assemble illicit goods, with limited oversight providing an ideal environment for producing and shipping such goods to consumer markets
- The relaxed tariff regime, which creates incentives for leaking products to the rest of the country's territory in order to evade import duties.

There are several factors associated with FTZs being used for illicit trade in addition to being subject to specific regulations, including their geographic location as high-volume logistical hubs. Singapore is the most obvious example, where most (if not all) transshipment activities can only take place via an FTZ. It is uncertain whether designing a port, or another logistical hub as an FTZ makes it more attractive for illicit trade purposes. The risks associated with FTZs should be taken into consideration when assessing TBFC; however, these risks should be fully understood and assessed against other factors and not in isolation.¹⁰²

Freeports are a subset of FTZs that "are designed to specifically encourage businesses that import and then re-export goods, rather than general business support or regeneration objectives."¹⁰³ The Institute for Government describes them as "a special kind of port where normal tax and customs rules do not apply. These can be airports as well as seaports. At a freeport, imports can enter with simplified customs documentation and without paying tariffs. Businesses operating inside designated areas in and around the port can manufacture goods using imports and add value, before exporting again without paying the full tariff on the original goods they imported – although a tariff may be payable on the finished product when it reaches its final destination, including if that destination is in the same country outside the freeport."¹⁰⁴

Sanctions Evasion

For the purposes of this document, it is important to understand that the term "sanctions" relates to the international framework of controls on money laundering, terrorist financing and proliferation financing as opposed to fines or other retribution meted out on Financial Institutions by regulators. The main international sanctions regimes include those of the UNSC described above, obligatory in all UN Member States, and unilateral sanctions. The latter may include sanctions imposed by

¹⁰²For more information on FTZs, see the Royal United Services Institute (RUSI) paper [Improving Governance and Tackling Crime in Free-Trade Zones](#), as well as their [Free Trade Zone Risk Assessment Tool](#).

¹⁰³Jeremy Mills-Sheehy and James Kane, "Trade: Freeports and Free Zones," The Institute for Government, July 22, 2021, <https://www.instituteforgovernment.org.uk/explainers/trade-freeports-free-zones>.









¹⁰⁴Mills-Sheehy and Kane.

the EU, or by individual States such as the US, Japan or the UK. Implementation of unilateral sanctions is discretionary and dependent on local regulatory requirements. In practice, most international Financial Institutions are careful to comply with US regulatory requirements because most international trade is conducted in US dollars.

Sanctions can be generally categorised into three types:

- **Comprehensive:** Comprehensive programmes seek to prohibit most financial and commercial interaction with a specific territory, country and/or government. They generally prohibit all direct and indirect activity or facilitation with a territory or country, including imports, exports and the provision of any financial products or services.
- **Selective:** Selective programmes seek to prohibit specific activity, such as imports of certain goods, or dealings in certain financial products with targeted individuals and entities in a country or target activity involving certain industry sectors. They may also target current or former governments and/or their government officials including individuals and entities closely associated with the government. Belarus, DPRK, Ukraine/Russia (SSI), Zimbabwe, and Venezuela are examples of Selective Programme targets.
- **List-Based:** List-based sanctions impose more targeted restrictions than comprehensive or selective Programmes. List-based Sanctions can be split into activity-based sanctions and country-based sanctions.
 - **Activity-based sanctions** seek to restrict all activity with listed individuals, entities, groups and vessels that are deemed to be involved in particular criminal activities. These can include terrorists/terrorism, narcotics trafficking, WMDs, rough diamonds, human rights violations, and corruption.
 - **Country-based programmes** target listed individuals and entities associated with certain current or former governmental regimes that may threaten the stability of the country or region or commit large scale human right abuses. They typically impose fewer restrictions than comprehensive programmes. The table below (Table 5) includes countries commonly included in related list-based programmes, however the list is not exhaustive.

Table 5 – Countries frequently included in list-based sanctions programmes

 Afghanistan	 Lebanon	 South Sudan	 Egypt
 Libya	 Tunisia	 Iran	 Somalia

Sanctions evasion and circumvention refers to the attempt to withhold, alter or mis-state a name or other identifying or transactional information in an effort to obfuscate the true identity of the parties involved in order to counter targeted financial sanctions.

The Illegal Wildlife Trade

The need to protect our planet’s vegetation and wildlife from plundering by transnational organised crime has become a major priority for the international community in recent years.

In 2013, the United Nations General Assembly proclaimed March 3rd, the day of signature of the convention on “*International Trade in Endangered Species of Wild Fauna and Flora, often referred to as (CITES)*”, as UN World Wildlife Day.

CITES entered into force in 1975, and established the legal framework and procedures for the regulation of international trade in over 37,000 species of animals and plants. Its aim - to ensure that international trade in these species do not threaten their survival. To date, over 180 states and the European Union have ratified the Convention, including all FATF members.

In 2015, the General Assembly unanimously adopted a resolution on “Tackling Illicit Trafficking in Wildlife”, which sets a powerful framework for collective action. The Sustainable Development Goals launched this year include specific targets to combat poaching and trafficking of protected species, including by helping local communities to pursue sustainable livelihoods. There is increasing recognition of the dangers wildlife and forest crime pose not only to the environment but also to the rule of law and stability and of the potential for the criminal proceeds to fuel conflict and terrorism¹⁰⁵.

“Wildlife trade” can be domestic or international, and legal or illegal. Wildlife trafficking, also known as the illegal wildlife trade (IWT) is a major transnational organised crime, which generates billions of criminal proceeds each year. IWT fuels corruption, threatens biodiversity, and can have a significant negative impact on public health and the economy. To move, hide and launder their proceeds, wildlife traffickers exploit weaknesses in the financial and non-financial sectors, enabling further wildlife crimes and damaging financial integrity. Despite this, jurisdictions rarely investigate the financial trail left by this crime¹⁰⁶.

The illegal wildlife trade (IWT), involves the illicit trade of protected animals, animal parts, and derivatives thereof, including procurement, transport, and distribution, in violation of international or domestic law, and money laundering related to this activity. The United Nations estimates that in excess of 7,000 different species are illegally trafficked. This activity is increasingly carried out by transnational criminal organisations (TCOs) and both encourages and entrenches corruption.

In 2021, the US Department of State identified 28 countries of focus for wildlife trafficking, including six countries of particular concern for related corruption - Cambodia, Cameroon, Democratic Republic of Congo, Laos, Madagascar, and Nigeria. Further, wildlife trafficking bolsters illicit trade routes, threatens critical biodiversity, damages fragile ecosystems, and can lead to the spread of zoonotic diseases.

Proceeds from wildlife trafficking are estimated by international organisations to be between USD7 and USD23 billion per year and account for a quarter of all wildlife trade. IWT uses many of the same routes and methods used by drug traffickers and others engaged in illicit trade and can vary depending on the species. Common smuggling techniques include concealing items in personal bags and falsely identifying goods as legal wildlife or other products. IWT trade ranges from a single live animal to multi-ton commercial shipments, with the latter becoming increasingly common.

IWT can be facilitated by a myriad of funding mechanisms, including, but not limited to, cash, bank transfers (wires and automated clearing house), transfers through informal values transfer systems, transfers through money services businesses, transfers conducted using online or mobile payment processors, and transactions using convertible virtual currencies (CVCs). Traffickers are increasingly turning to social media platforms to advertise, sell, and otherwise engage in IWT, including facilitating payments and the movement of money¹⁰⁷.

Per FATF report June 2020 “Money Laundering and the Illegal Wildlife Trade”, it is essential that jurisdictions maintain their focus on illegal wildlife trade financial flows to address several challenges, jurisdictions should consider implementing the following good practices:

¹⁰⁵ UNODC - World Wildlife Crime 2016 Report - Trafficking in protected species - page (3).

¹⁰⁶ FATF report June 2020» Money Laundering and the Illegal Wildlife Trade – page (5) , sample of methods to Launder Proceeds from IWT Misuse of the formal Financial sector, front companies and co-mingling of licit proceeds, money value transfer systems (MVTS), facilitation role of new technologies. The recent methods of facilitation role of new technologies are (the use of pre-paid cards, use of mobile Apps to move value for IWT crimes).

¹⁰⁷ FinCEN notice – FinCEN Calls Attention to Environmental Crimes and Related Financial Activity Nov. 2021” pages (4) & (5).

- Prioritise combatting the financial flows associated with IWT proportionate to risk.
- Provide all relevant agencies with the necessary mandate and tools to conduct successful financial investigations into IWT.
- Improve co-ordination between authorities responsible for combatting wildlife crimes and those responsible for conducting financial investigations to ensure authorities more regularly exchange information and follow the financial trail.
- Cooperate with other jurisdictions, relevant international organisations and the private sector to combat IWT¹⁰⁸.

Supply Chain for the Illegal Wildlife Trade and Related Financial Flows

The supply chains for IWT impact countries differently, and are largely distinct across species. Nevertheless, in general, syndicates involved in wildlife crime usually poach, harvest or breed wildlife in countries that are rich in biodiversity and/or where there may be weaker law enforcement oversight and criminal justice. Similarly, most syndicates involved in such crime transit the wildlife through other countries in order to obfuscate the end-destination (“transit” and “destination” countries)¹⁰⁹.

Case Terrorist of Mark-up and Potential Proceeds for the Illegal Wildlife Trade¹¹⁰

The following examples give an indication of the magnitude of the proceeds generated in the IWT market, based on quoted prices. The examples only provide a snapshot in time due to various factors that can affect the price including the perceived quality of the wildlife in question, its species or geographic origin, market bans or national restrictions (i.e. country of final purchase) and the degree of processing (i.e. carved, dried, tanned, etc.).

- **Juvenile Glass Eels:** In Europe, juvenile glass eels are worth USD 300 to 500 per kg. However, the price can reach as high as USD 1,500 to 6,000 per kilo when exported to destination countries, representing significant mark-up.
 - According to EUROPOL data, between 2018 and 2019, European law enforcement seized 5,789 kg of smuggled juvenile glass eels with an estimated value of USD 2,153 per kilo, which equated to potential proceeds of around USD 12.5 million.
- **Ivory:** While the price paid to elephant poachers can be just USD 200 or less, in destination markets ivory can be priced at between USD 500 and USD 1,000 per kg (150% to 400% mark-up). Notably, the price of ivory has been decreasing in recent years due to high profile ivory bans in a number of countries (e.g. China, UK, US etc.).
 - Between March and July 2019, Vietnam, China and Singapore seized as much as 25.3 tons of ivory in three containers, representing potential revenue of around USD 12.5-24 million.



**CASE
STUDY**

¹⁰⁸“FATF report June 2020” Money Laundering and the Illegal Wildlife Trade – page (6).

¹⁰⁹“FATF report June 2020” Money Laundering and the Illegal Wildlife Trade – page (14).

¹¹⁰“FATF report June 2020” Money Laundering and the Illegal Wildlife Trade – pages (13 & 14).

- **Rhinoceros horn:** The price of rhinoceros horn can reach around USD 65,000 per kg, but has also been known to be sold as low as USD 9,000 per kg, according to US authorities.
 - Criminals trafficked approximately 4,500 African rhinoceros horns between 2016 and 2017, generating estimated proceeds of between USD 41 and 292 million.
- **Pangolin scales:** While hunters can receive from USD 2.5 to 9 per kg of pangolin scales, the price in demand countries is usually around USD 200 per kg, but has reached as much as USD 700 per kg, reflecting significant mark-ups.
 - Between 2016 and 2019, countries confiscated an estimated 206.4 tons of pangolin scales across 52 seizures globally, which amounts to USD 41-144 million in sales in destination countries.

Additional Considerations

Trade Finance products can contain several terms and conditions, and clauses. This guidance cannot cover all of them; however, there has been industry debate on the inclusion of certain clauses which may put into question the effectiveness of the instrument in which they are drafted¹¹¹. The inclusion of Sanction clauses and Boycott clauses will be covered to provide guidance on their use and the implications.

Sanctions Clause

A sanctions clause included in a contract is intended to provide grounds to suspend performance of that contract while the sanctions are in place. The suspended performance could relate to the delivery of goods, suspension of payments, or performance of other obligations. Neither party is held responsible for improper performance of contractual obligations. The relevant sanctions regimes could include those of the UN, EU or unilateral sanctions such as those of the US, UK, Canada, Japan, or other countries.

It is worth noting that the European Union's (EU) blocking statute (Council Regulation (EC) No 2271/96) is intended to protect EU operators, whether individuals or companies, from the extra-territorial application of third country laws, particularly US secondary sanctions.¹¹²

ICC rules do not cover sanctions clauses under their published rules. In recent years, international sanctions have become a major issue for Financial Institutions involved in international trade and projects. Several Financial Institutions have received very large fines from US authorities for breaching sanctions regulations, resulting in many withdrawing from all dealings with certain countries which are subject to sanctions. The first question Financial Institutions need to consider when new sanctions regulations are issued or amended is whether there is an obligation to comply with the regulations by ceasing business with companies and individuals designated in the sanctions' regulations. For example, sanctions regulations often start with a resolution of the UN Security Council (UNSC) pursuant to Article 41 of the UN Charter. Such UN Resolutions are addressed to member states and not to specific Financial Institutions or trading companies. One has to consider how those resolutions are implemented by regulations issued at regional or national level. The EU will usually publish its own sanctions regulations shortly after a UNSC Resolution is issued. EU regulations are binding not only on EU nationals when doing business inside the EU, but also on EU nationals when doing business outside the EU and also on non EU nationals when doing business in the EU. A financial institution based in the EU or doing business through a branch registered in the EU will therefore have to consider EU regulations before proceeding with any transactions which may be subject to those regulations. Similar considerations apply also in respect of the US

¹¹¹<https://iccwbo.org/content/uploads/sites/3/2020/05/20200504-addendum-to-sanction-clauses-paper.pdf>

¹¹²For more information, see European Union, "Council Regulation (EC) No 2271/96 of 22 November 1996 Protecting against the Effects of the Extra-Territorial Application of Legislation Adopted by a Third Country, and Actions Based Thereon or Resulting Therefrom," Pub. L. No. 2271/96 (1996), <http://data.europa.eu/eli/reg/1996/2271/2018-08-07/eng>.

Sanctions regulations override irrevocable commitments given in LCs and guarantees. A financial institution must not make a payment under a demand guarantee or a SBLC if the sanctions regulations prohibit it from doing so. Conversely, if the regulations do not in fact prohibit the processing of a LC or guarantee, the financial institution must fulfil its legal obligations under the relevant instrument. The financial institution cannot refuse to process a LC or pay under a guarantee simply because there is a connection with a sanctioned country. One must check whether the regulations actually prohibit the financial transaction in question.

International sanctions can have a significant impact on the payment obligation under all types of LCs and guarantees, as there is no mention of sanctions regulations under UCP 600.

In recent years, many Financial Institutions have started to introduce sanctions clauses into their LCs, SBLCs and guarantees, trying to cover themselves against the position where it is not entirely clear whether or not the transaction is permissible should any sanction regulations come to light. In March 2010, the ICC Banking Commission published a guidance paper (470/1129) stating that sanctions clauses in LCs should do no more than say that, if the processing of a documentary credit is prohibited by sanctions regulations, the financial institution is relieved of its obligation to do so. In 2014, the ICC published a second guidance paper on the use of sanctions clauses in trade finance related instruments subject to ICC rules (ICC document No. 470/1238). In this paper, the ICC discouraged the use of sanctions clauses which give the financial institution discretion whether or not to process the LC or pay under the guarantee, just because the financial institution is concerned that there may be some connection with sanctions, even if there is in fact no prohibition under the relevant regulations. The ICC was concerned that such clauses can cast doubt on Financial Institutions' irrevocable undertaking to pay a complying demand.

Boycott Clause

Boycotts are economic measures intended to place economic pressure on the target of the boycott. When states seek to impose boycotts on the citizens of other states, those states have sometimes adopted measures to prevent their citizens from being coerced to assist in a boycott which is not aligned with its policies.

The term "boycott" has also been used to refer to actions mandated by governments against other countries or private entities. It is in this sense that the term is relevant to most voluntary boycotts as they are legal in most countries. Although there are certain exceptions, they rarely relate to Financial Institutions. A boycott imposed by law is, in effect, an embargo and is often described as a sanction, although the penalties for failing to comply with such a boycott are also described as sanctions.

A boycott clause is a covenant by a buyer of goods or services to comply with US antiboycott laws and regulations. Adherence with a boycott or violation of anti-boycott provisions is a serious concern for Financial Institutions to whom such boycotts or anti-boycott provisions apply. Many of the fines imposed by US regulators have stemmed from the failure of Financial Institutions to identify violations of US anti-boycott regulations.¹¹³

Boycotts are classified as primary, secondary, or tertiary:

- **Primary boycott:** Directed at a target whose actions or inactions are desired to be changed.
- **Secondary boycott:** An indirect attempt to influence the actions of a target by seeking to discourage third parties from dealing with the target of the boycott.
- **Tertiary boycott:** A boycott that involves the use of a "blacklist" of businesses or companies that deal with the target of a boycott.

¹¹³For examples of boycott language, see "Examples of Boycott Requests," US Bureau of Industry and Security, accessed March 21, 2022, <https://www.bis.doc.gov/index.php/enforcement/oac/7-enforcement/578-examples-of-boycott-requests>.

For example, the US boycott imposed on Cuba is intended to coerce a regime change in Cuba that is acceptable to the US. In order to accomplish this goal, the boycott attempts to deny Cuba access to capital, resources, technology, markets, and restrict the free movement of Cuban citizens and their commercial entities.

A sovereign nation can elect to align with a boycott of another country, and can require its own citizens to comply. It is also recognised, however, that a nation state can prohibit its citizens and entities operating in its jurisdiction from being compelled to participate in a boycott that is not instituted or approved by that nation state. The issue is whether one country can require compliance with its boycott by other countries and their citizens.

CASE STUDIES

Targeted Financial Sanctions Related to WMDs

The following case studies were taken from the report *Typologies on the Circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction*, published by the United Arab Emirates' (UAE) Executive Office of the Committee for Goods Subject to Import and Export Control.¹¹⁴

Nickel Wire

In 2019, the UAE authorities received information that Person Z had ties to the Iranian Revolutionary Guards Corps (IRGC) and was involved in financing the nuclear programme in Iran in violation of UNSCR 2231. Person Z used the UAE as a transit point for a low-value shipment containing samples of nickel rods/wire which were imported from Country A and destined for Iran. The UAE authorities identified four bank accounts with a total balance of AED 22,000 that belonged to the suspect and his three companies and were used to support the IRGC. The investigations revealed that Person Z was in negotiations to ship larger quantities of the nickel rods/wire to Iran. The UAE Prosecution issued an order to arrest Person Z and immediately froze all funds in accounts controlled by Person Z and three companies he controlled, totalling AED 22,000. The UAE Prosecution also suspended the business activity of those companies.

As of the time of publishing, the case has been referred to the competent court and is pending a verdict.

Carbon Fibre

In collaboration with the UAE, OFAC designated 11 entities and individuals involved in the procurement of goods on behalf of Iran's ballistic missile programme, including Mabrooka Trading Co LLC (Mabrooka Trading) – based in the UAE – and a UAE-based network. This network obscured the end user of sensitive goods for missile proliferation by using front companies in third countries to deceive foreign suppliers. It has also designated five Iranian individuals who have worked to procure ballistic missile components for Iran. Hossein Pournaghshband and his company, Mabrooka Trading, were providing or attempting to provide financial, material, technological, or other support to Navid Composite Material Company (Navid Composite), an entity also sanctioned by

¹¹⁴Executive Office of the Committee for and Goods Subject to Import and Export Control, *Typologies on the Circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction* (Dubai: Government of the United Arab Emirates, 2021), 21–22, <https://www.centralbank.ae/sites/default/files/2021-08/Typologies%20on%20circumvention%20of%20Targeted%20Sanctions%20agst%20Terr.%20and%20the%20Prolif.%20of%20WMD%20-%20Ex.Office%20IEC%20May2021.pdf>.

the US in connection with Iran's ballistic missile programme. At the time of its designation, Navid Composite was contracting with Asia-based entities to procure a carbon fibre production line in order to produce carbon fibre probably suitable for use in ballistic missile components. Since at least early 2015, Pournaghshband used his company, Mabrooka Trading, to procure materials and other equipment for Navid Composite's carbon fibre production plan. Pournaghshband is also designated for having provided or attempting to provide financial, material, technological, or other support to Mabrooka Trading.¹¹⁵

Involvement of Financial Institution in Sanctions Evasion

The following case study includes excerpts taken from the report *Major Turkish Bank Prosecuted in Unprecedented Iran Sanctions Evasion Case*, published by the Wisconsin Project on Nuclear Arms Control.¹¹⁶ The names of individuals and entities have been removed.

A state-owned bank, "Bank A", was involved in a scheme to launder billions of dollars of Iranian oil proceeds through the institution under the guise of gold trade using a network of exchange houses and front companies in Turkey and the UAE.

"On October 15, 2019, US prosecutors unsealed an unprecedented six-count indictment against Bank A, a major Turkish state-owned financial institution, charging the bank with fraud, money laundering, and conspiracy to violate the International Emergency Economic Powers Act (IEEPA). The US Department of Justice decision to prosecute Bank A is an unusual step. US prosecutors usually seek to settle out of court with banks accused of sanctions violations, through deferred prosecution agreements."

An Iranian-Turkish businessman ("Individual X"), "funnelled money from Bank A accounts held by Iranian entities to accounts of his front companies in Turkey and the United Arab Emirates (UAE). Then, after laundering the money through illicit gold exports and later falsified food trade, Individual X ultimately used those funds to make international payments on behalf of Iranian entities that support Iran's proliferation programmes. According to the Department of Justice, the scheme 'fuelled a dark pool of Iranian government-controlled funds that could be clandestinely sent anywhere in the world'."

Overview of the Sanctions Scheme

"In early 2012, a representative from an exchange house ("Exchange House"), a money services subsidiary of Bank B, a private bank in Iran, informed Individual X that the Central Bank of Iran (CBI) and the National Iranian Oil Company (NIOC) held billions of dollars in accounts at Bank A. The funds consisted of the proceeds from Iranian oil and gas sales to Turkey.

"Pursuant to sanctions imposed by the US National Defense Authorisation Act (NDAA) of 2012, money from these oil escrow accounts could not be transferred back to Iran or used for international financial transfers on behalf of the government of Iran or Iranian banks. In July 2012, Executive

CASE STUDY

¹¹⁵"Treasury Sanctions Those Involved in Ballistic Missile Procurement for Iran," US Department of the Treasury, January 17, 2016, <https://www.treasury.gov/press-center/press-releases/pages/jl0322.aspx>.

¹¹⁶John P. Caves III and Meghan Peri Crimmins, *Major Turkish Bank Prosecuted in Unprecedented Iran Sanctions Evasion Case*, Iran Watch Report (Madison, WI: Wisconsin Project on Nuclear Arms Control, 2020), <https://www.wisconsinproject.org/wp-content/uploads/2020/04/Major-Turkish-Bank-Prosecuted-Unprecedented-Iran-Sanctions-Evasion-Case.pdf>.

Order 13622 further restricted petroleum-related transactions with CBI and NIOC specifically. At the time, however, funds from the accounts could legitimately be used to pay for Turkish exports to private Iranian companies – an exception known as the bilateral trade rule.

“First, CBI and NIOC would transfer the oil revenue held in their Bank A accounts (denominated in Turkish lira, so as to avoid the international financial system) to the Bank A accounts of private Iranian banks, such as Bank B. Those Iranian intermediaries then transferred the money to Bank A accounts controlled by Individual X’s network of front companies, thereby concealing the Iranian connection from outside Financial Institutions.

“Individual X’s front companies used the funds to buy gold on the Turkish market. To further cover his tracks, Individual X then falsified records to indicate that the gold was subsequently exported to private companies in Iran, as permitted by the bilateral trade rule. In this way, even if the internal Bank A transfers could be traced back to the Iranian oil accounts, the transaction would still appear to be in compliance with US sanctions (this falsified documentation later underwent several changes as US sanctions evolved).

“In reality, Individual X’s companies exported the gold to Dubai, where they then sold it on the market for cash. This step was critical to Individual X’s scheme and served two purposes. First, it allowed him to acquire currencies used for international payments, such as the US dollar and the euro. Second, it disguised the money’s Iranian origin. Unlike bank transfers, cash transactions cannot easily be traced.

“At this point, the money was ready to be moved in the international financial system. Individual X deposited the cash proceeds from the gold sales into accounts held by his companies at banks in Dubai. Iranian banks, such as Bank B and Bank C, then gave Individual X’s companies instructions to transfer the money to various entities in Iran’s sanctions evasion network, composed of front companies and foreign suppliers in several countries including Canada, China, and Turkmenistan. US banks then unwittingly processed several of these dollar transactions through correspondent accounts. As a result, from December 2012 to October 2013 alone, more than USD900 million of Iranian oil and gas money transited through US Financial Institutions to make payments on behalf of Iran.

Advantages to the Scheme

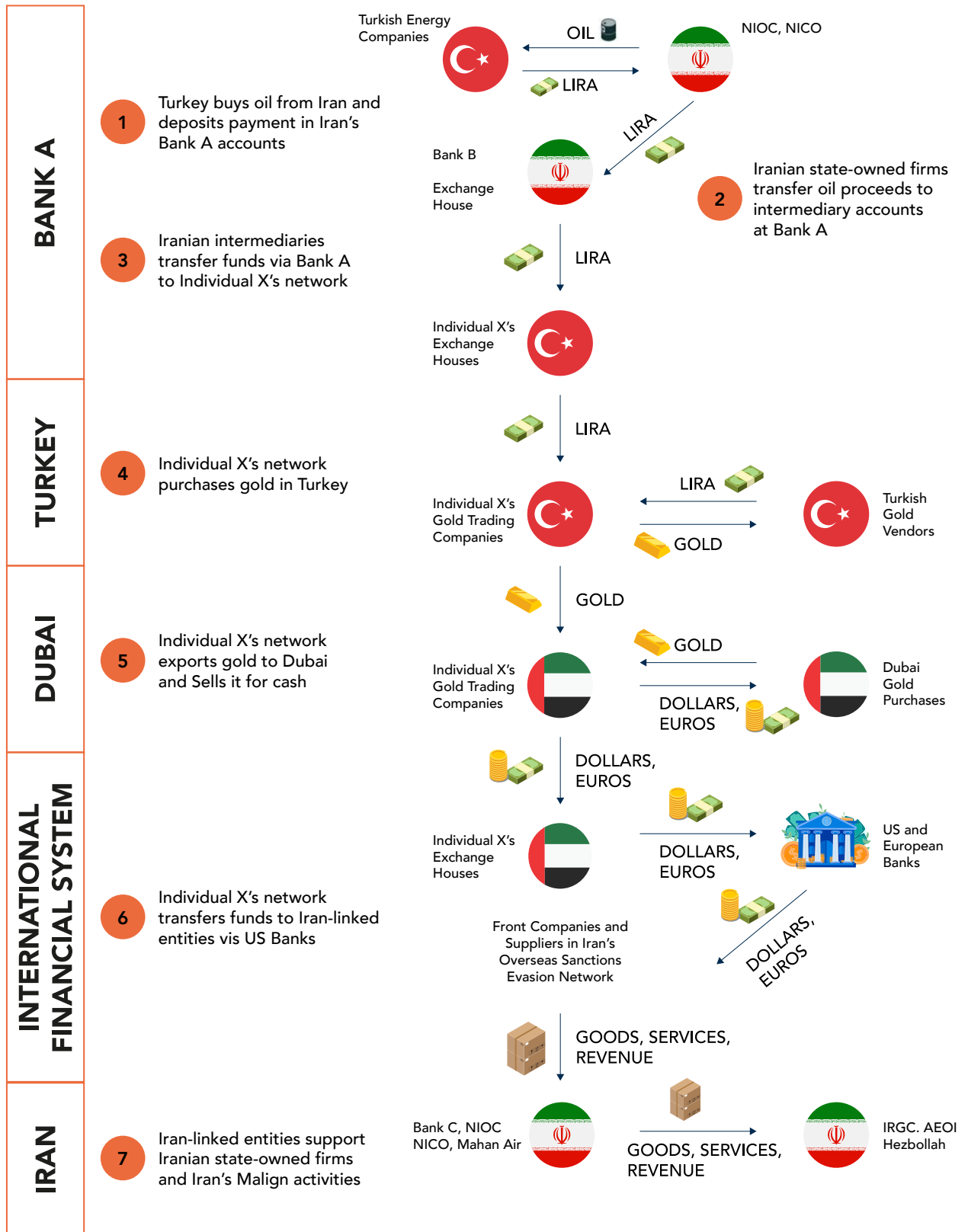
“The schemes aided Iran’s proliferation activities in two ways. First, it benefitted Iranian entities with ties to those activities. In both the gold and food scheme, the laundered funds’ ultimate destination was foreign companies participating in Iran’s sanctions evasion and illicit procurement networks.

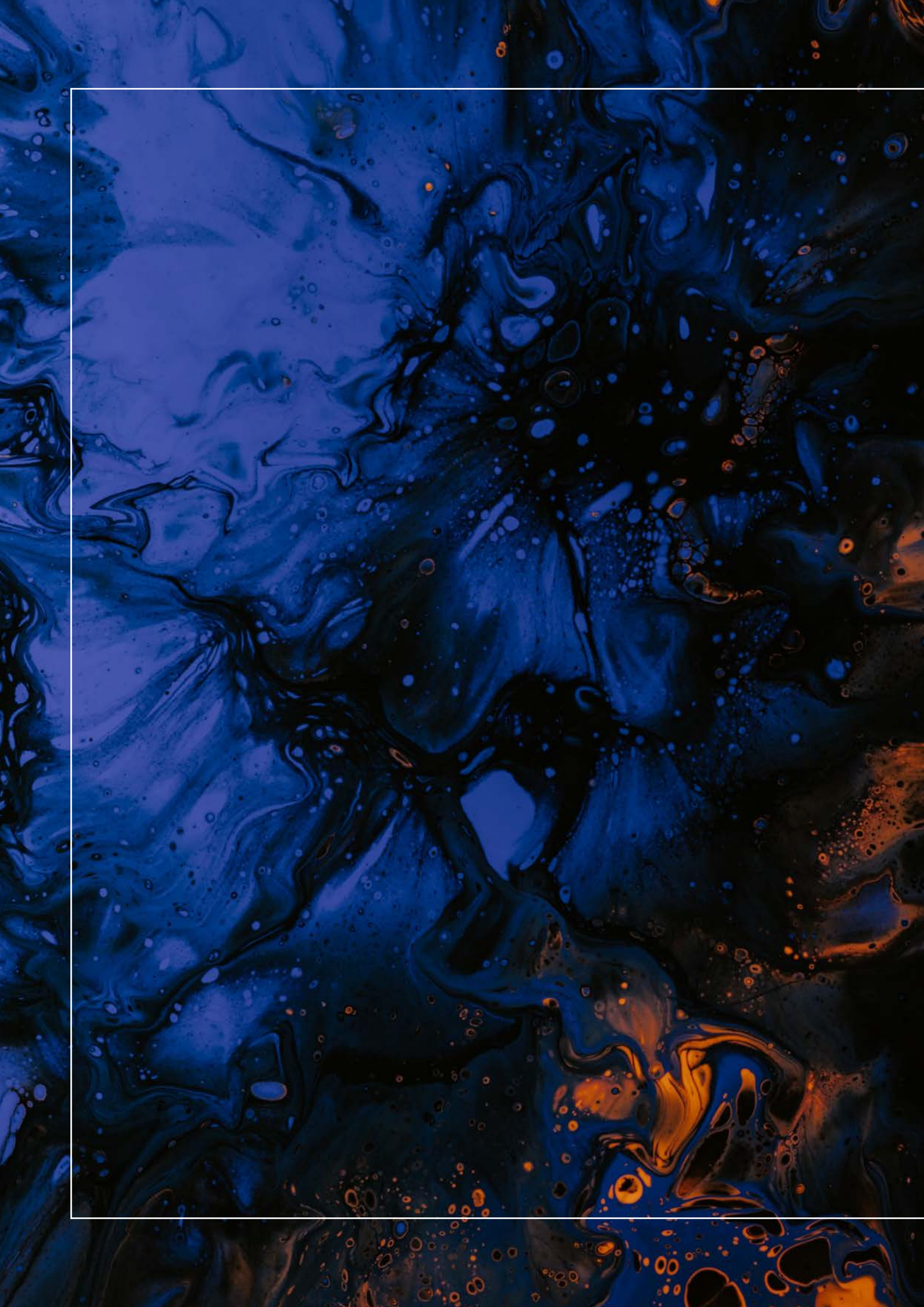
These companies supplied Iranian entities with goods and services, but needed to be paid in order to continue their operations; the Iranian oil money laundered through Bank A was their payment. In one illustrative example, Individual X’s companies made several international transfers – at the direction of Iranian banks and apparently on behalf of NIOC – to a Turkmenistan-based energy company that was supplying gas to Iran.

“Second, the scheme relieved financial pressure on Iran between 2012 and 2016, amidst multilateral negotiations to limit Iran’s nuclear programme that resulted in the 2015 Joint Comprehensive Plan of Action (JCPOA). The pressure from sanctions provided critical leverage to the US and its partners during negotiating with Iran. The financial back-channel provided by Individual X and Bank A may have lessened this leverage.

Figure 6 – The gold scheme in seven steps

The Gold Scheme: In Seven Steps







Typologies

Typologies

Trade prohibitions and embargos are in place to restrict goods or services that, upon dealing, facilitate and support regimes. For example, the Islamic Revolutionary Guard Corps (IRGC) is subject to such restrictions, and more recently Russia, where embargos have been put on luxury products coming out of Russia such as vodka and high-end chocolates. Restrictions on the purchase of strategic or significant goods is economically damaging to the country and key industries, thereby putting pressure on the sanctioned regimes. In regard to exports, goods and services provided to these countries can aid regimes and companies or bad actors in furthering their own advancement, as evidenced by the US technology ban on supply to certain Chinese telecom and military companies, intended to prevent them from using the technology in their products. Various tactics are used to evade trade restrictions or embargoes. These tactics can be used on their own or in combination with other tactics, as listed in Appendix IV, in order to engage in TBFC.

Risks Associated with Documentation

Certain types of trade documents, used in the delivery of goods as well as the payment for goods, are used and abused in order to hide illicit activity. Below are some examples of how certain documents can be misused to facilitate certain crimes or illicit activities mainly in relation to sanctions evasion.

Switch Bill of Lading

Financial Institutions that allow switch B/Ls in trade finance products face several risks relating to money laundering and/or sanctions evasions. As noted earlier, a switch B/L is a second set of B/Ls that are often requested when there has been a change in the original trading conditions.

Financial Institutions need to be aware of the risks associated with this kind of B/L, which can include disguising the main seller of the goods; disguising the ultimate beneficiary and/or end-user of the goods; and disguising the origin of the goods, which may involve sanctioned countries, ports, entities or parties, etc.¹¹⁷

Blank Endorsed Bill of Lading

As noted earlier, a "blank endorsement on a bill of lading is an indication that there is no specified recipient of the endorsed bill."¹¹⁸ A money launderer may choose to use a blank endorsed B/L as it acts similarly to a bearer cheque in that it obfuscates the ultimate beneficiary/beneficial owner, meaning that Financial Institutions will not be able to apply standard customer due diligence procedures.

Fraudulent Bills of Lading and Other Falsified Documents

B/Ls play an important role in trade, however they can be abused:

Because there are so many players involved with a B/L from start to finish, fraudulent B/Ls can appear at any point during the shipping process. The main motivation behind fraudulent B/Ls is to obtain a valuable cargo.

¹¹⁷Aliona Yurlova, "Switch Bill of Lading: A Complete Manual and Word of Advice," iContainers, October 30, 2018, <https://www.icontainers.com/us/2018/11/01/switch-bill-of-lading-complete-manual/>.

¹¹⁸"Blank Endorsement on a Bill of Lading."

One of the more common fraudulent B/L is a forged document. The forgeries themselves can vary, from the signatures on the forms, to the specific items listed; but one of the most common forgeries is the impersonation of the authorised receiver of the shipment. This enables disguising the ultimate beneficiary from the goods or the end user especially for sensitive and dual-use goods. In some cases, this will enable the criminal to steal everything in that shipment. If the B/L is "to order"—meaning the B/L is in someone's name specifically—and is transferable, the criminal may forge the person's signature to steal the shipment.

Depending on the type of B/L that accompanies a shipment, there may be several people involved in the process who can be held legally liable for a shipment never reaching its destination. This unfortunately involves otherwise innocent bystanders who had nothing to do with the crime but, as the nature of the B/L would suggest, are responsible for the contents of the shipment just the same.¹¹⁹

Back-to-Back Letters of Credit

One sanctions evasion technique that may be encountered is back-to-back letters of credit. Based on multiple sources, the technique takes the following structure:

In this situation, Bank A issues a LC as collateral to Bank B in order to issue a separate LC to the beneficiary. This often happens when the underlying agreement between the applicant and beneficiary contains restrictions about the credit quality of the bank that is issuing the LC, the location of the issuing bank, or other stipulations that prevent the applicant's bank from issuing a direct LC to the beneficiary.

A sanctions evader can use a back-to-back LC to remove the name of a sanctioned bank from the documentation more effectively than would be possible with a transferred LC. With a back-to-back LC, the beneficiary receives a letter of credit from an unsanctioned bank without mention of the original issuing bank. The beneficiary may not even know that a sanctioned institution is involved in the transaction.

An organization can avoid taking part in this type of sanctions violation by watching out for these red flags: instructions to amend the terms, alter the destination of goods, change the name of a vessel, remove a bank or applicant name, or change a financial institution or applicant name. Any of these directions requires further investigation.

The bank named as beneficiary on the initial LC would need to be complicit in this arrangement, or at least negligent, to remove all mention of the sanctioned institution from the outgoing LC. It's crucial for Financial Institutions that operate in multiple jurisdictions to understand the sanctions that apply to the local jurisdiction as well as those that apply to other jurisdictions where customers transact, and where the institution may also have responsibilities.¹²⁰

¹¹⁹"Bill of Lading."

¹²⁰"ICA Specialist Certificate in Trade Based Money Laundering," International Compliance Association, 75–77, accessed March 22, 2022, <https://www.int-comp.org/programme/?title=ICA-Specialist-Certificate-in-Trade-Based-Money-Laundering>.

Misuse of Standby Letter of Credit

Like back-to-back LCs, SBLCs can also be misused. The following is an explanation of how an SBLC can be used in a money laundering scheme:

The use of the SBLC for money laundering involves collusion between both applicant and beneficiary, as the two ensure that the terms and conditions of the SBLC are violated by the applicant, thereby effecting a payment to the beneficiary.

It is in the payment to the beneficiary stage that the funds are laundered, as the beneficiary is often offshore and outside the jurisdiction of the applicant's country of residence. The payment to the beneficiary can be allegedly justified by the documentation associated with the SBLC, thereby lending additional legitimacy to the transaction. For a SBLC to be of any use to a money launderer, the trigger in the agreement between both applicant and beneficiary must be pulled. Without this breach of the SBLC, no payment step is initiated.

Several triggers may be found under SBLC's. These triggers create a weakness in the application of an instrument for the money launderer. Throughout the normal course of business for a financial institution's trade finance operations, approximately five per cent of SBLC are triggered by the beneficiary, a figure based on conversations with trade-finance processing staff in various countries. If trade-finance processing staff notice that SBLCs are constantly being triggered between an applicant and a beneficiary, one of two outcomes is likely. Either the applicant is enduring a terrible streak of bad luck and poor business judgment, or both parties are conspiring to employ SBLCs to transmit vast amounts of value across borders without raising the suspicions of supervisory authorities.¹²¹

Risks Associated with Goods

Just as illicit actors exploit vulnerabilities in certain trade documents to mask illicit or illegal activity, so too do they employ tactics to obfuscate goods and/or use particular goods to engage in illicit activity. Trade finance instruments are designed to bridge the trust gap between parties on a promise to pay basis, and on occasion only move the associated documents; therefore, Financial Institutions can only rely on the details contained within the documents that outline the goods or services traded.

For goods that are shipped, of the estimated 11 million containers that enter the US each year, only 3.7% are scanned. 1% of that total are checked at overseas ports, with approximately 1.5% of containers being scanned that arrive in EU ports.¹²² Steps are being taken through the enhancement of technology to increase this number; however, as Financial Institutions rely on the description of the goods being shipped that are recorded in the documents provided and very few containers are being inspected, this enables illicit goods to move with a high probability of not being identified. Customs will not be aware of which goods a financial institution might be financing or moving documents for, and Financial Institutions will not be aware of the contents of containers being inspected by Customs. It is also important to understand the transaction and be alert for any details that might suggest non-genuine shipment details; for example, a 40ft container cannot carry twice the weight of a 20ft container.

¹²¹"ICA Specialist Certificate in Trade Based Money Laundering," 75–77.

¹²²<https://ajot.com/insights/full/ai-container-inspection-an-unsolved-need>

Evasion through Consolidation of Goods

Illicit actors may attempt to evade sanctions by concealing prohibited or restricted goods, such as dual use goods or sensitive goods, among other low-risk goods to reduce and/or evade scrutiny. The Association of Certified Anti-Money Laundering Specialists (ACAMS), in its Certified Global Sanctions Specialist Manual, discusses different evasion methods used:

There are a few types of transshipment evasion tactics. Some evaders hide prohibited or restricted goods through consolidation. In other words, they group small shipments into one larger one, or they mix restricted items with other goods like weapons and do not declare those restricted items in shipping documentation.

The Internet has made it much easier to make business contacts around the world. However, the practice of evading sanctions by hiding a restricted shipment within an unrestricted one or hiding a small amount of contraband among innocuous goods, has existed for centuries. As long as there have been smugglers, there has been consolidation.

When sanctions evaders ship something they want to go unnoticed or undetected, the key is to avoid or minimise inspection. For example, if the goods disguising the restricted shipment are heavy, difficult to move, or messy in some way, they may better conceal what evaders don't want the customs officials to see. Disguising goods may include live plants or crates of vegetables that are fragile and would break down with too close inspection. Imagine a shipment of machine parts in small boxes, concealed beneath pallets of scrap metal or gravel. It would be extremely difficult for inspectors to move those pallets and detect the restricted goods.

Technology has made consolidation easier in some ways. The anonymous and often untraceable parts of the Internet called the Dark Web can make it easier for sanctions evaders to advertise their willingness to engage in activity that breaks the law. However, sanctions evasion still requires a level of trust between parties. This trust can only be established through contact and time or through an introduction from a trusted individual.

In other ways, technology has made consolidation more difficult. Advances in merchandise marking, tracking, and technology have enhanced the security of goods in transport. These advances leave fewer openings for manipulation of the system.

There is potential for an increase in shipment consolidation to evade sanctions. Certain goods will always be subject to consolidation due to global restrictions; weapons are a prime example. Still, advances in technology for goods tracking, life cycle monitoring of merchandise, and government use of technology in the global shipment arena will present new challenges to the bad actors.

One example of evasion through consolidation is the case of David Wu. In August 2015, the US Department of Justice sentenced him to 10 months of imprisonment for violating restrictions relating to the export of arms equipment. Wu tried to arrange for the purchase of this equipment in the United States to ship it to China. He planned to conceal the equipment in another shipment that contained construction supplies for building houses.¹²³

¹²³"Certified Global Sanctions Specialist Certification," ACAMS, 89, accessed March 22, 2022, <https://www.acams.org/en/certifications/certified-global-sanctions-specialist-cgss#overview-e3b4081f>.

CASE STUDY

Use of Import-Export Front Company to Move Wildlife and Related Financial Flows¹²⁴

From April to May 2015, there were two seizures in Thailand and Singapore of a combined 6.8 tonnes of ivory, all exported from the port of Mombasa. Further financial investigations by Liberty Shared, in collaboration with relevant governments, helped to reveal the larger syndicate behind these seizures. By following the import/export data for the seizures, investigators were able to identify that the syndicate had established a legitimate tea trading company in Kenya to conceal ivory shipments and financial flows between east Africa and east Asia. The syndicate set up a tea trading front company (company A) to buy from a larger unwitting tea company and freight forwarder (company B) to obfuscate the true tea buyers. The syndicate also set up a third company (company C) to transport the tea to the port. Prior to the container being shipped, company C arranged for the trucks to be diverted and for the tea sacks to be filled with ivory before returning to the port. The “tea” shipments then changed destination locations twice and consignee name while en route. This was most likely an attempt to confuse port officials. One risk indicator for this case was that the final destination was East Asia that is not a major export market for tea from Africa.

High Risk Goods

Certain commodities pose a higher risk for use in TBFC due to their high and/or subjective value, high demand, and ease of conversion to cash, among other factors. Such goods include precious metals and stones like gold and diamonds, vehicles, tobacco products, and consumer electronics.

Terrorists Use Gold to Move Value

The following case study was submitted by the US and is taken directly from the FATF’s 2008 report *Terrorist Financing*:

During the invasion of Afghanistan in 2001, it was widely reported that the Taliban and members of al-Qaeda smuggled their money out of the country via Pakistan using couriers that handled bars of gold.

In Karachi, couriers and hawala dealers transferred the money to the Gulf Region, where once again it was converted to gold bullion. It has been estimated that during one three-week period in late November to early December 2001, al Qaeda transferred USD 10 million in cash and gold out of Afghanistan. An al-Qaeda manual found by British forces in Afghanistan in December 2001 included not only chapters on how to build explosives and clean weapons, but on how to smuggle gold on small boats or conceal it on the body.

Gold is often used by hawala brokers to balance their books. Hawala dealers also routinely have gold, rather than currency, placed around the globe. Terrorists may store their assets in gold because its value is easy to determine and remains relatively consistent over time. There is always a market for gold given its cultural significance in many areas of the world, such as Southeast Asia, South and Central Asia, the Arabian Peninsula, and North Africa.¹²⁵

CASE STUDY

¹²⁴FATF report June 2020” Money Laundering and the Illegal Wildlife Trade – page (19) / Source: liberty shared.

¹²⁵Financial Action Task Force, *Terrorist Financing* (Paris: Financial Action Task Force, 2008), 24, <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>.

Risks Associated with Actors

There are certain actors involved in trade and trade finance that can serve as “gatekeepers” to the international trade and financial system, placing them in a position that can facilitate TBFC.

Freight forwarders and customs brokers

The FATF and the Egmont Group under their 2020 TBML report specifically highlight freight forwarders and customs brokers due to the important role they play in facilitating trade transactions.¹²⁶ They may be put at risk of engaging in TBFC:

The most significant risk that freight forwarders and customs brokers may be exposed to is that they become participants in a trade transaction and could unwittingly be exposed to the risk of facilitating the crimes of money laundering or financing of terrorism. Any subsequent investigation or legal proceedings could lead to significant disruption of business and, depending on the circumstances, potential criminal liability.

The likelihood is that it would not be limited to a single trade transaction but could form part of a scheme which would be systematically exploited over a prolonged period once it was deemed to be viable by those responsible.¹²⁷

Freight forwarders and customs brokers are unregulated for AML purposes; however, as the TBFC schemes are becoming more sophisticated they could unknowingly become caught up in such schemes. To prevent this, such entities should make themselves aware of the associated ML/TF risks to their business, and review policies and procedures and internal controls to assess whether there are any gaps that could be exploited by criminals. Employees should be trained on the relevant risk indicators and red flags and be given guidance on what they should do if they identify a red flag. An assessment should be undertaken of the customer base to identify potential high-risk customers, and consideration should be given to undertaking desktop scenario exercises to stress test their vulnerabilities to being inadvertently engaged in TBFC schemes. Though such entities may not be prosecuted, any investigation by a regulator or law enforcement agency can be very disruptive and have a detrimental impact on the businesses’ reputation.¹²⁸

Front and Shell Companies

Front and shell companies, particularly anonymous versions, play an important role in facilitating TBFC by insulating illicit actors from their activities. In the case of anonymous companies, this can include obfuscating the identity of the company’s ultimate beneficial owners. In relation to the use of front and shell companies in TBFC and sanctions evasion:

The FATF-Egmont TBML 2020 report discussed the possibility that TBFC in some cases may involve sanctions evasion techniques especially front and shell companies. Sometimes, documents presented to Financial Institutions may involve sanctions evasions techniques. Sanctions evaders often falsify commercial invoices, bills of lading, and cargo manifests to conceal shipment contents or destinations that would arouse suspicion or trigger sanctions controls.

The physical merchandise is seen only when packaged and unpackaged, or if authorities make a random inspection. At all other times, the documentation (whether in hard copy or electronic) representing the shipment is taken at face value. So when an evader falsifies details, shipments “fly below the radar,” with the contraband goods or sanctioned parties involved passing unnoticed.

¹²⁶Financial Action Task Force and Egmont Group, TBML: Trends and Developments, 25–26.

¹²⁷“Trade Based Money Laundering (TBML) Risk in the Freight Forwarding and Customs Broking Sectors,” Clyde & Co, accessed December 20, 2021, <https://www.clydeco.com/insights/2020/12/trade-based-money-laundering-tbml-risk-in-the-frei>.

¹²⁸“Trade Based Money Laundering (TBML) Risk in the Freight Forwarding and Customs Broking Sectors.”

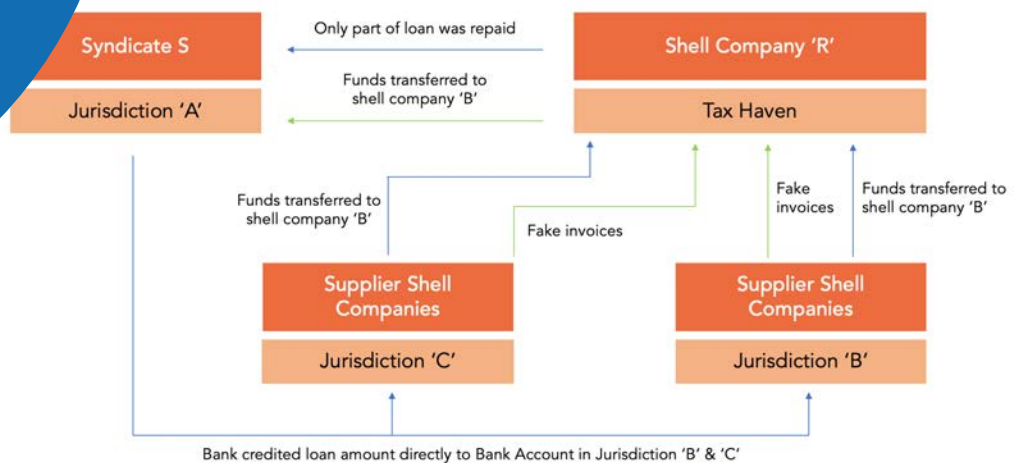
Spot checks by customs authorities identify some fraud. However, thousands of containers of goods pass through ocean ports around the world daily. Therefore, authorities rely on every party involved in a trade transaction to consider all other parties and all details involved in the transaction and to identify when something seems out of place.¹²⁹

CASE STUDY

Shell Companies and Trade Fraud

The below case study, shown in Figure 7, is an example of how shell companies were used to procure high value loans from banks through fraudulent invoices.

Figure 7 – Shell companies and trade fraud



The scheme occurred as follows:

1. Syndicate S registered a Shell Company R in a tax haven jurisdiction
2. Syndicate S set up a number of supplier shell companies in Jurisdiction B and Jurisdiction C
3. Syndicate S opened accounts in 8 banks in Jurisdiction A and applied for high value loans
4. Shell Company R claimed it dealt with cross border trading activities and purchased goods from Supplier Companies in Jurisdiction B and Jurisdiction C
5. Shell Company R obtained trade credit from the banks in Jurisdiction A on the strength of invoices for the purchases made from Jurisdictions B and C
6. The banks in Jurisdiction A directly credited loan amounts on instruction of Company R into the bank accounts of the shells in Jurisdiction B and C
7. On receipt of funds the supplier shells immediately transferred the funds to Shell Company R
8. Shell Company R used the funds for part repayment of loans

¹²⁹"Certified Global Sanctions Specialist Certification," 90-91.

Risks Associated with Transport

Approximately 90% of global trade involves maritime transportation. Malign actors constantly seek novel ways to exploit global supply chains for their benefit. For red flags associated with these typologies, see **Appendix IV**.

Transshipment

As previously mentioned, transshipment is the transport of goods through a territory where the goods are unloaded from one means of transport and loaded onto another means of transport (e.g. from a vessel to a train). OFAC, which is responsible for implementing the US's unilateral sanctions regime, has made it clear that they will fine entities using the Iran overland route even if the origin or destination of goods is not a sanctioned country.

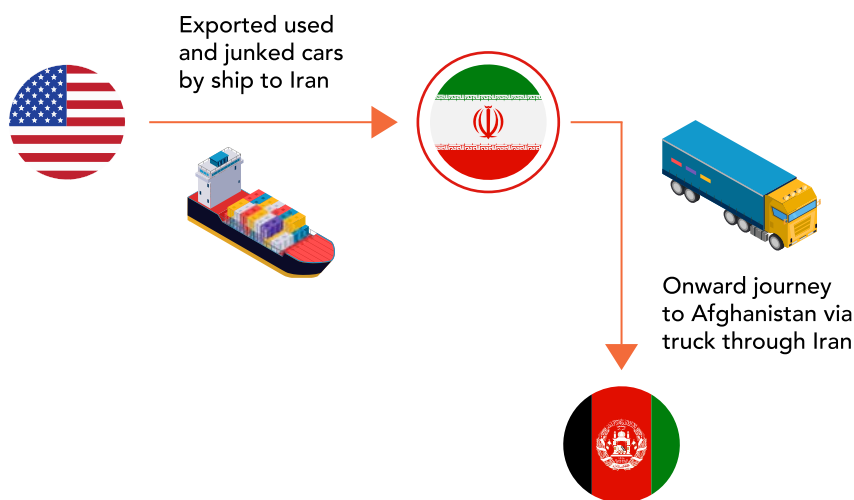
The MENA region has an amplified transshipment risk due to:

- Proximity to sanctioned countries such as Iran and Syria
- Iran's geographical location, which makes it a natural conduit for international trade

Sanctions Evasion Via Transshipment

In 2017, American Export Lines was fined more than USD518,000 for shipping cars to landlocked Afghanistan via Iran. American Export Lines transshipped used and junked cars and parts from the United States via Iran to Afghanistan on 140 occasions from 2010-2021 (Figure 8).¹³⁰

Figure 8 – American Export Lines sanctions evasion via transshipment



Concealing the Final Destination of Goods

By obscuring the final destination of goods, individuals are able to export goods to destinations without facing any additional questions or rejected payments from Financial Institutions or port authorities. Changing B/Ls or layering the sales through front companies can result in dual use or sensitive goods being exported for terrorism or for companies to sell goods to regimes to use for military purposes.

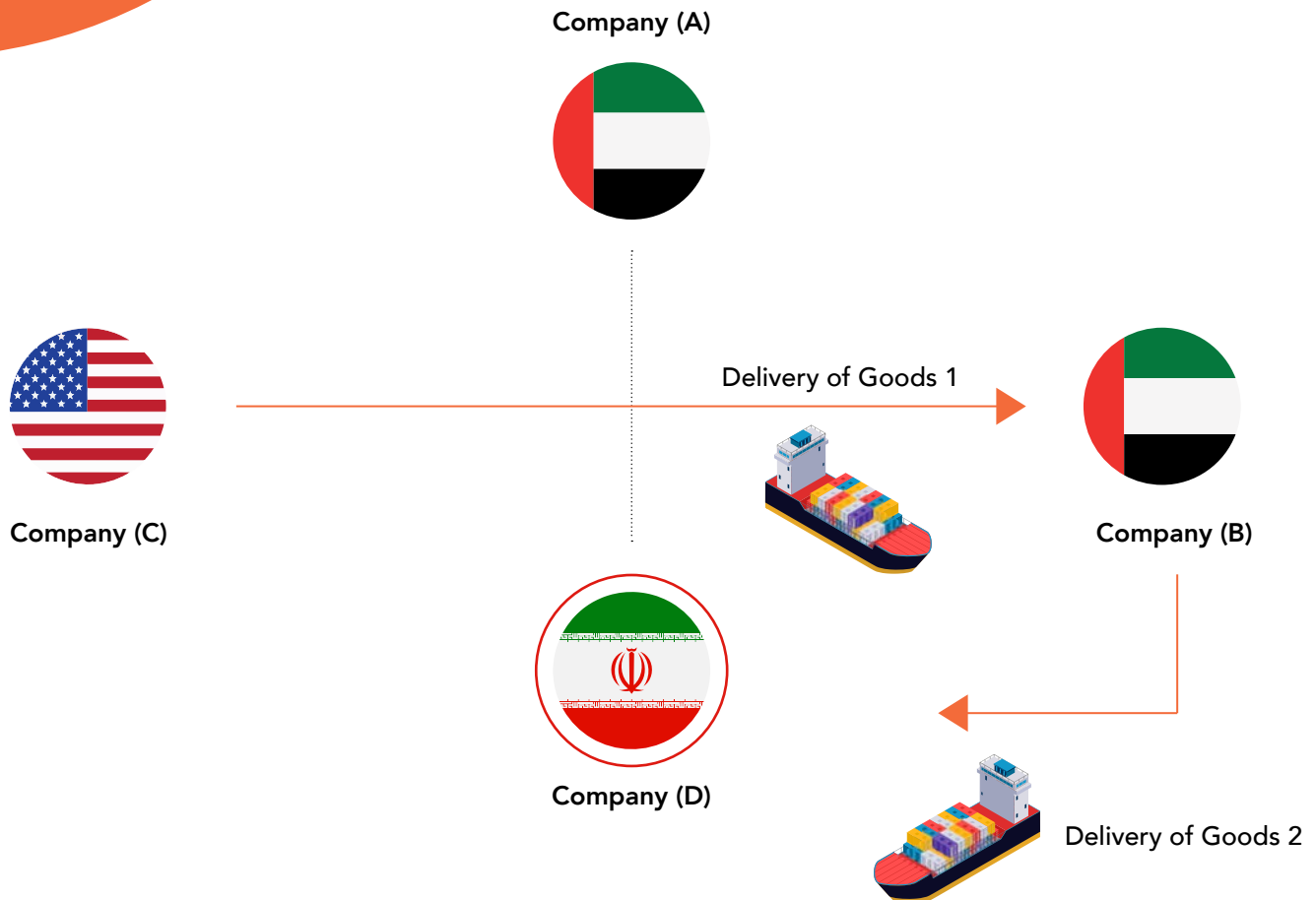
¹³⁰"Settlement Agreement between the US Department of the Treasury's Office of Foreign Assets Control and Blue Sky Blue Sea, Inc., Doing Business as American Export Lines and International Shipping Company (USA)," US Department of the Treasury, August 17, 2017, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20170817_33.

CASE STUDY

Sanctions Evasion Through Destination Concealment

In the below case study, a Dubai-based company sourced goods from the US for an Iran-based company, routing the sales through another Dubai-based company in order to obfuscate the final destination of the goods.

Figure 9 – Sanctions evasion via destination concealment



- Company (A), located in Dubai-UAE, sells fluid handling and other equipment for the energy industry and other sectors. It exported storage tank cleaning units from the US to Iran
- In 2015, an Iranian distributor of oil products, one Iranian Oil Company (company D) contacted Company (A) to inquire about purchasing cleaning units, explicitly stating the company was based in Iran and enquiring about the possibility of delivery to Iran
- In order to evade sanctions, company (A) agreed to route the sales (of US goods from company C) to Iran through the Dubai-based company (B) with which company (A) already had an existing distributor relationship
- Company (A) falsely listed Company (B) as the end user on its export documentation. Instead the Iranian Oil Company - Company (D)

International and National Responses to TBFC

Everyone has a responsibility to mitigate TBFC; if there were no market for counterfeit goods, then the supply would cease in the same way as the narcotics trade. Governments, government agencies, associated bodies and the financial services all play a part in endeavouring to identify and mitigate TBFC. Governments need to recognise that there is a problem and support the other players by providing clear and robust regulation which is globally consistent, along with guidance. Government agencies need to engage with the financial services industry through PPPs, sharing intelligence and typologies and the financial services industry needs to take steps to enhance their control frameworks in a thoughtful manner to that assess their customers' activity in a holistic manner whilst enabling trade to continue.

United Nations

The United Nations (UN) has approved a number of sanctions and other resolutions to address some of these TBFC threats. These impose mandatory obligations on all UN Member States under Chapter VII of the UN Charter. At present, the relevant such resolutions relate to WMD proliferation, specifically Iran, DPRK and non-State actors,¹³¹ and terrorism.¹³²

Security Council resolutions usually set out what Member States *should* do, but Member States need to decide for themselves how to do so. In many cases, international or regional organisations have drawn up requirements, standards, or best practices for implementation of relevant Security Council resolutions for their members.

Financial Action Task Force

In the current context, the most relevant responses are those of the FATF. The FATF Recommendations are intended to address threats from international money laundering, the financing of terrorism or the proliferation of weapons of mass destruction, and include recommendations specific to the implementation of Security Council resolutions.¹³³ The two following recommendations are most relevant to targeted financial sanctions:

Recommendation 6. Targeted financial sanctions related to terrorism and terrorist financing

Countries should implement targeted financial sanctions regimes to comply with UNSC Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the UNSC including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

Recommendation 7. Targeted financial sanctions related to proliferation

Countries should implement targeted financial sanctions to comply with UNSC resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other

¹³¹"Resolution 2231 (2015) on Iran Nuclear Issue," United Nations Security Council, accessed December 17, 2021, <https://www.un.org/securitycouncil/content/2231/background>; "Security Council Committee Established Pursuant to Resolution 1718 (2006)," United Nations Security Council, accessed December 17, 2021, <https://www.un.org/securitycouncil/sanctions/1718>; resolution 1540 (2004) and successor resolutions.

¹³²"Security Council Committee Pursuant to Resolutions 1267 (1999) 1989 (2011) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities," United Nations Security Council, accessed December 17, 2021, <https://www.un.org/securitycouncil/sanctions/1267>; United Nations Security Council, "Resolution 1373 (2001), Adopted by the Security Council at Its 4385th Meeting, on 28 September 2001," S/RES/1373 (2001) § (2001), [https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373\(2001\)](https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373(2001)).

¹³³"The FATF Recommendations," Financial Action Task Force, October 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.

assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UNSC. At present such resolutions relate only to two countries: Iran (resolution 2231 (2015)) and North Korea (resolution 1718 (2006) and successor resolutions).

Countries that are members of FATF, or one of the FATF Style Regional Bodies (FSRBs) such as MENAFATF, need to implement all 40 FATF Standards. In addition to Recommendations 6 and 7 described above, those Standards specific to terrorist or proliferation financing include:

Recommendation 1. Assessing risks and applying a risk-based approach

Countries should identify, assess, and understand money laundering, terrorist financing and proliferation financing risks and take action to ensure such risks are mitigated.

Recommendation 2. National cooperation and coordination

Countries should have national AML/CFT/CPF policies, informed by risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Recommendation 5. Terrorist financing offence

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

The FATF has published several informative guidance documents relating to terrorist and proliferation financing including, including best practices and guidance as well as indicators (See Appendix I: Additional Resources for a list of these documents).

Risk-Based Approach to Money Laundering

There should be a risk-based approach to the measures and control environment in the identification and mitigation of TBFC.

According to the EU's regulations, all EU member states must conduct national risk assessments (NRAs). By adopting a risk-based approach, States can prepare their national risk assessments according to the country's circumstances.

The NRA process includes:

- Determining the most revenue-generating criminal activities in the country.
- Assessing the financial and private sector's vulnerability to money laundering identifying the controls and weaknesses of the criminal justice system.
- Evaluating the effectiveness of the fight against money allocation to resources according to the level of risk.¹³⁴

¹³⁴"National Risk Assessment | What Is NRA?," Sanction Scanner, accessed March 22, 2022, <https://sanctionsscanner.com/knowledge-base/national-risk-assessment-of-money-laundering-321>.

Governments conduct NRAs to better detect and prevent money laundering and terrorist financing. Risk environments are increased due to globalisation as well as the growing engagement of governments in joint activities across many sectors, and therefore, the NRA is implemented to properly manage risk and support the risk environment's decisions emerging with globalization.¹³⁵

Dual-Use and Sensitive Goods

Restrictions on export or import of certain categories of shipments are a key element of many proliferation-related sanctions regimes, both multilateral or unilateral, and national trade-related legislation. "Dual-use goods" include materials, equipment and technology used for legitimate civilian purposes that can also be used in (or may be a necessary component of) military and WMD programmes. For example, corrosion-resistant pumps are needed in the oil industry (where hydrogen sulphide is a problem) and in some uranium enrichment plants (where uranium hexafluoride is the problem). Potassium nitrate is a well-known dual use good, as it is frequently used as a fertiliser by the agricultural industry, but can also be used in making explosives. Table 6 provides additional examples.¹³⁶

In practice, the development and trade of dual-use goods are monitored by four different multilateral export control regimes:

- The [Nuclear Suppliers Group](#) that deals with nuclear related items
- The [Australia Group](#) that deals with chemical and biological warfare-related items
- The [Missile Technology Control Group](#) that deals with delivery systems
- The [Wassenaar Arrangement](#) that deals with conventional weapons-related items.

Each of these regimes publishes lists of materials, equipment and technology that need to be controlled for export/import. The lists are updated on an annual basis, reflecting the speed of technological developments in these areas. Monitoring and incorporating updates into national regulations can be resource-intensive. The EU's control list combines all four regime lists and their annual updates and, for this reason, some non-EU countries base their export control legislation on the EU's list.

Some, but not all, States in the MENA region have incorporated dual-use lists into their import/export legislation. The controls are implemented in practice usually in the form of requirements to obtain licences from the appropriate licensing authority. Imports/exports of materials, equipment and technology are illegal without a licence, but few States in the region require Financial Institutions to carry out related checks. However, dual-use export/import control lists are common in many other jurisdictions, in particular the US and Europe, and other countries with advanced manufacturing capabilities.

Some of the import/export controls in these countries may extend to financial transactions and in these cases Financial Institutions need to ensure they meet local regulatory expectations. Institutions involved in documentary trade finance may find this easier than those not so involved. They have access to invoices, licences, shipping documentation or other material which enable some degree of checks to be carried out for the presence of dual-use goods in the underlying shipments. Institutions facilitating "open-account" transactions will not have detailed information available on the underlying shipment and may have to demonstrate to regulators that they deploy other methods, such as customer-monitoring, to mitigate the risk of illicit shipments of dual-use goods.

¹³⁵"National Risk Assessment."

¹³⁶Financial Action Task Force, Proliferation Financing Report, 7.

Table 6 – Dual use goods and sensitive goods¹³⁷

Dual Use Goods				Dual Use & Sensitive Goods	Sensitive Goods	
Nuclear	Chemical	Biological	Missile & Delivery	Minerals & Chemicals	Military Weapons	Precious Metals
High-speed cameras	Heat exchange	Bacterial strain	Aluminium alloys	Potassium nitrate	Weapons including rifles, pistols, and ammunition	Gold in all forms
Composites	Reactors	Fermenter	Aluminium powders	Chlorine	Missiles ammunition	Rough diamonds
Maraging Steel	Precursors	Spray dryer	Accelerometers	Phosgene	Bombs	Precious stones
Centrifuges	Scrubbers	Filters	Gyroscope	Cyanide	Combat vehicles include tanks and armoured cars	Jewellery
Pulse generators	Mixing vessels	Mills	Isostatic press	Hydrogen	Defense equipment	
Ignitions	Elevators	Presses	Composites	Chloropicrin	Aircrafts, ships/vessels and transport trucks	
Vacuum pumps	Condensers	Pumps	Maraging steel	Chemical mixture	Navigation and radar equipment	
Pressure gauges	Connectors	Tanks	Oxidant	Certain natural resources such as ore and crude oil	Equipment for military, police or foreign governments	
Mass spectrometers	Coolers	Growth media	Machine tool		Classified defense articles	
X-ray flash apparatus	Pumps		Homing devices		Sensitive technical data	

¹³⁷Several items were added based on FATF 2008 report page (7) , Proliferation Financing Report Source: "Proliferation of weapons of mass destruction", Report from the Swedish Security Service.

Export Controls

Export controls are restrictions imposed by governments on the tangible (i.e. physical) and intangible (e.g. electronic) movement of certain goods, software and technology across borders, and the provision of technical assistance related to controlled items.

International policies, agreements and commitments underpin the principles of export controls:

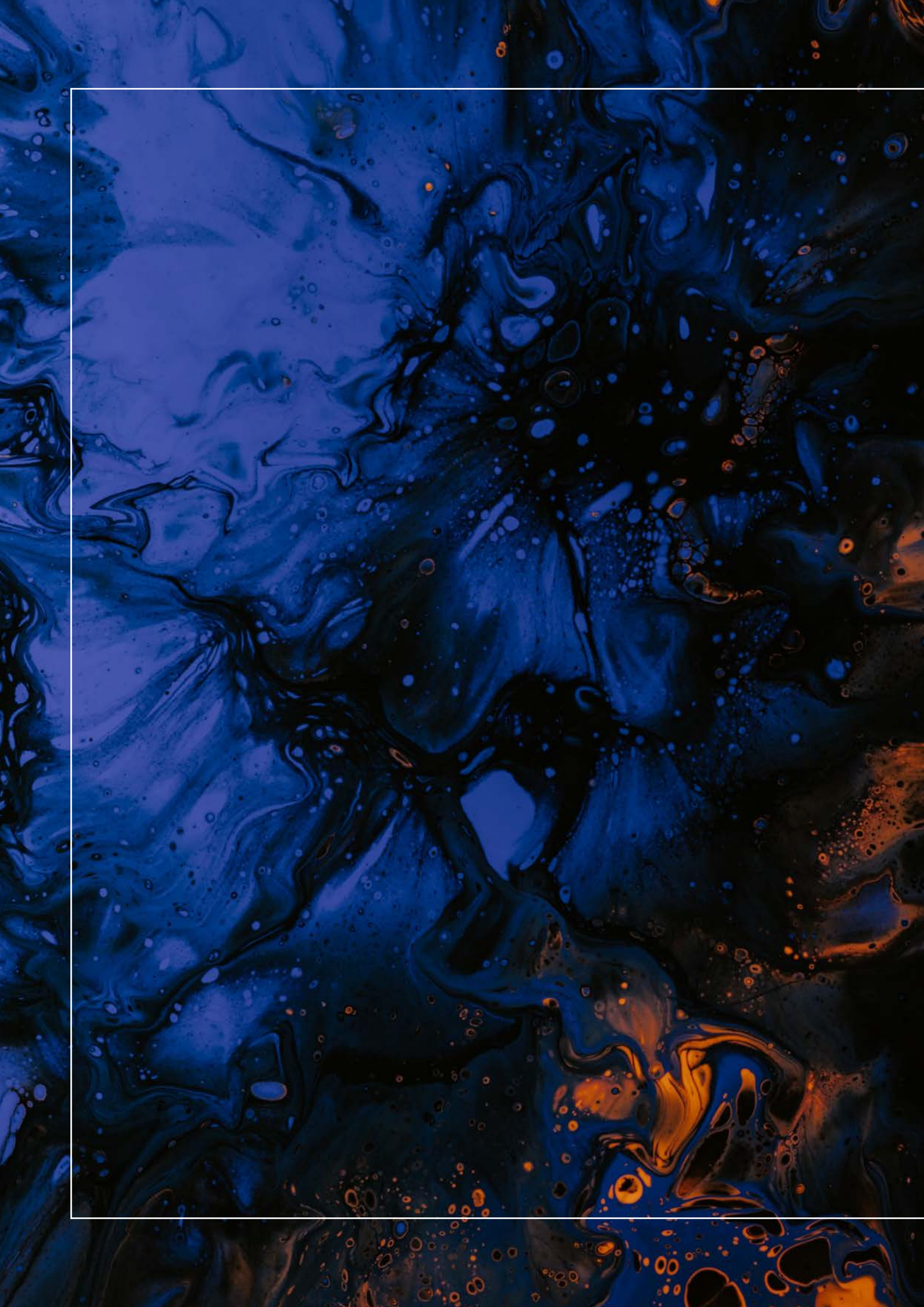
- Conventional arms & Dual-use goods are governed by the Wassenaar Arrangement
- WMD Non-Proliferation are governed by Missile Technology Control Regime (Missiles), Nuclear Suppliers Group (Nuclear) and Zanger Committee (Nuclear)
- Many countries maintain their own export control lists including EU, China, HK, Japan, the UK, and US. Some countries base their lists on the EU list which is updated on an annual basis.

Key concepts of Export Controls:

- Items: Governments publish lists of controlled goods, software and technology which require an authorisation to be exported.
- End Use: "Catch all" controls can be placed on the export of items if the exporter knows or suspects that they will be used in a weapon of mass destruction (or another restricted end use)
- End User: Exports to specific entities or persons may be prohibited or subject to a licence requirement if they are listed on a government sanctioned party list.
- Destination: Trade sanctions and embargoes are tools to implement trade restrictions against target countries

Enforcement Action:

- May 2021 – The US Department of State reached a settlement with Honeywell International Inc amounting to USD13m, to resolve alleged violations of the Arms Export Control Act (AECA), 22 USC. § 2751 *et seq.*, and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130. The offences committed by Honeywell included unauthorised exports and retransfers of ITAR-controlled technical data that contained engineering prints showing dimensions, geometries, and layouts for manufacturing castings and finished parts for multiple aircraft, gas turbine engines, and military electronics to and/or within Canada, Ireland, Mexico, the People's Republic of China, and Taiwan.





**Financial
Institutions
and TBFC:**
Vulnerabilities
and Responses

Financial Institutions and TBFC: Vulnerabilities and Responses

TBFC schemes can consist of a large number of components, including front companies, funds transmitted between several banks, goods being transhipped etc., meaning each of the Financial Institutions involved may only see a small part of the network. Other parties to the trade, for example customs agencies, may not have an understanding of the financial flows and may only see invoices and not the actual goods. This fragmentation of TBFC schemes makes it inevitably difficult for Financial Institutions to identify potential TBFC schemes based on the lack of analysis of the whole chain, and in many cases limits their ability to detect discrepancies in supplementary documentation and customer profiles.

All parties in a trade transaction have a responsibility to mitigate TBFC, whether it be the Financial Institutions, customs agencies, shipping companies, insurers etc. In some cases, a proactive approach is required which may include intelligence-led reviews. These would need to be led by government and would be based on information shared by Law Enforcement or other Agencies. A mechanism would need to be devised and implemented by Financial Institutions for this purpose. The financial services sector has a wealth of data relating to their customers, which is essential for analysis; however, it has been estimated that the cost of financial crime compliance reached USD213.9 billion in 2021.¹³⁸ There is a need to establish a cost effective and efficient solution to mitigate and detect TBFC along with the other trends and typologies for money laundering. To fully understand whether something is unusual relating to the customer, an assessment is required of the entire customer activity, their associated parties, and the countries involved.

Vulnerabilities

As previously mentioned TBFC is complex, and those involved have a wealth of financial services products to choose from to carry out illegal activity. Those involved in TBFC maybe involved in other illicit activity, for example mortgage fraud or insurance scams, so Financial Institutions and those responsible for mitigating such behaviour have to understand that each product can be used in different ways to either mask or facilitate financial crimes. There has been a lot of focus by regulators and industry forums commenting on the risks associated with trade finance products and their use in TBFC as they are associated with trading; however, it is also true that these products can act as a mitigant to TBFC.

As outlined in this guidance and other industry papers, some trade finance products require numerous documents to be presented sometimes at different stages of the trade cycle; as previously mentioned (see "Payment of Goods") this provides Financial Institutions with a lot more information than a simple wire payment. Utilising the data contained within these documents in an analytical way may go some way in the mitigation of financial crime.

The financial service industry needs to be careful that only the controls that are commensurate to the risks that may arise are deployed, which is in line with the regulatory expectation of risk-based controls. The industry must undertake a balancing act, taking into consideration the client journey

¹³⁸Tauren Corsinie, "Counting the Cost (Cost of Compliance vs Cost of Non-Compliance)," *1RS* (blog), October 11, 2021, <https://1rs.io/2021/10/11/counting-the-cost-cost-of-compliance/>.

and risk mitigation; should the controls be too onerous or restrictive, then the products will not suit the needs of the client. For example, if every wire payment was subjected to pre-transaction AML checks the global movement of funds would cease.

Those involved in financial crime and wanting to move illicit funds or value whether domestically or internationally will find loopholes in an organization’s control framework, or other ways to circumvent controls in order to succeed. Vulnerabilities will exist, and it is only through a continued cycle of assessment, refinement, trials, testing and training will any control framework evolve to successfully mitigate financial crime.

Responses

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. A number of these are outlined below.

Risk Assessments

The Wolfsberg Group states that “financial crime risk assessments are one element of the financial crime compliance (FCC) toolkit available to Financial Institutions/firms (FIs) which can be used to strengthen a FI’s compliance framework. The assessments highlight key risk areas... as well as the establishment of strategic (more long term) and tactical (immediate workaround) actions plans for managing the identified risks.”¹³⁹

There are several ways to carry out a risk assessment with the “convention/standard methodology” being the most widely used approach. The following diagram (Figure 10) illustrates conventional components of a money laundering risk assessment.

Figure 10 – Components of a financial crime risk assessment

Inherent Risk	Control Effectiveness	Residual Risk
Clients	Governance	Strategic Actions
	Policies & Procedures	
Products & Services	KYC/Due Diligence	
	Other Risk Assessments	Tactical Actions
Countries	Management Information	
	Record Keeping/Retention	
Channels	AML Unit	Risk Appetite
	SAR Filings	
Others	Monitoring & Controls	
	Controls	
	Training	
	Independent Testing	

Source: The Wolfsberg Group, “The Wolfsberg FAQs on Risk Assessments”

¹³⁹The Wolfsberg Group, “The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption” (Ermatingen, Switzerland: The Wolfsberg Group, 2015), 1, <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf>.

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.¹⁴⁰ Since Wolfsberg guidance was produced, regulators' expectations have increased on the assessment segments to not only consider the inherent risk of money laundering but also to include terrorist financing, fraud, bribery and corruption, cybersecurity, tax evasion and sanction evasion. These may be included in an overarching risk assessment or individually; for example, an independent cybersecurity risk assessment as defined by the National Institute of Standards and Technology Framework (NIST).¹⁴¹

Wolfsberg outlines that the risk assessment can be considered in three phases:

- **Phase 1** – Determine the Inherent Risk: Inherent Risk represents the exposure an FI has to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied
- **Phase 2** – Assess the Internal Control Environment: Once the inherent risks have been identified and assessed, internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies or activities put in place by the FI to protect against the materialisation of a money laundering risk, or to ensure that potential risks are promptly identified
- **Phase 3** – Derive the Residual Risk: Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management/controls. The residual risk rating is used to indicate whether the money laundering risks within the FI are adequately managed.¹⁴²

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.

There are usually three levels of due diligence:

- **Standard CDD:** This involves identifying the customer, and ensuring the identification is based on a reliable independent source. The purpose and intended nature of the business relationship or transaction must be assessed and further information obtained where appropriate
- **Simplified CDD:** This can be applied when a risk assessment has shown a negligible or low risk of money laundering. The only requirement is to identify the customer, and there is no need to verify the customer's identity.
- **Enhanced CDD:** This level is applied when the risk of money laundering is high, such as when the customer is identified as a PEP. EDD measures can include:
 - Additional identification information from the customer
 - Information on the source of funds or source of wealth
 - Subjecting the customer to additional ongoing monitoring procedures.¹⁴³

¹⁴⁰The Wolfsberg Group, 7.

¹⁴¹The Wolfsberg Group, "Wolfsberg Statement: Guidance on a Risk Based Approach for Managing Money Laundering Risks" (Ermatingen, Switzerland: The Wolfsberg Group, 2006), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf.

¹⁴²The Wolfsberg Group, "Wolfsberg FAQs on Risk Assessments," 7,10,12.

¹⁴³"Anti-Money Laundering – a Guide to Customer Due Diligence," VinciWorks Blog (blog), June 27, 2018, <https://vinciworks.com/blog/anti-money-laundering-a-guide-to-customer-due-diligence/>.

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 check¹⁴⁴.

Sanction Screening

In regard to terrorism financing, the FATF explains:

Recommendation 6 requires each country to implement the targeted financial sanctions regimes to comply with the UNSC resolutions relating to the prevention and suppression of terrorism and terrorist financing. These resolutions require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any person or entity either (i) designated by or under the authority of, the UN, including in accordance with the Al-Qaida/Taliban sanctions regimes; or (ii) designated by that country or by a supra-national jurisdiction pursuant of UNSCR 1373.¹⁴⁵

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.¹⁴⁶ 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.¹⁴⁷

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.¹⁴⁸

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

¹⁴⁴Byrne, James E., and Justin B. Berger. *Trade Based Financial Crime Compliance*. Montgomery Village, MD: Institute of International Banking Law & Practice; London Institute of Banking & Finance, 2017. – Page (108).

¹⁴⁵Financial Action Task Force, *International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)* (Paris: Financial Action Task Force, 2013), 3, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf>.

¹⁴⁶The Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening" (Ermatingen, Switzerland: The Wolfsberg Group, 2019), <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf>.

¹⁴⁷For more information, see The Wolfsberg Group, 2.

¹⁴⁸For more information, see The Wolfsberg Group, "Monitoring Screening and Searching: Wolfsberg Statement" (The Wolfsberg Group, September 2003), https://ms.hmb.gov.tr/uploads/sites/2/2019/04/monitoring_statement.pdf.

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.

In 2013, the UK Financial Conduct Authority (FCA) issued a Thematic Review document titled “Banks’ control of financial crime risks in trade finance” which outlined good and bad practices. The review highlighted several failings by Financial Institutions with regards to the lack of controls over trade finance transactions. It highlighted that many Financial Institutions were unable to demonstrate that money laundering, terrorist financing and sanctions risks had been considered when processing trade transactions. In addition, many Financial Institutions only conducted manual screening of the trade documents in isolation of the associated payment for the trade transaction.¹⁴⁹

It is very important that the assessment of the trade documents must be considered in conjunction with the payment. In addition, Financial Institutions should implement a procedure to ensure that payments are not completed in instances where the trade finance transaction is rejected from a document perspective and the documents returned to their customer.¹⁵⁰

The findings of the review had quite an impact on the trade finance departments, with many Financial Institutions reassessing their control frameworks. Following the publication of the FCA report, the Wolfsberg Trade Finance Principles guidance document was updated to outline certain controls for different trade finance products as well as potential red flags to consider when processing trade finance transactions.

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.

¹⁴⁹For more information, see UK Financial Conduct Authority, Banks’ Control of Financial Crime Risks in Trade Finance, Thematic Review TR13/3 (London: Financial Conduct Authority, 2013), <https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf>.

¹⁵⁰If goods are in transit, then settlement by way of payment will have to be made.

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.

Trade Finance, Tax Evasion, and Oversight

An individual (Buyer) in Country A purchases a car from someone (Seller) in Country B. The Buyer and Seller agree on a fair market value of USD20,000. The Buyer obtains a letter of credit (LC) from a financial institution (FI) in order to purchase the car, however, in order to evade high import duties, the Buyer secures the LC for a price much lower than the fair market value of the car (e.g. USD10,000).

Upon import, the customs agency will inspect the commercial invoice, the bill of lading and certificate of origin; however, they will not be aware of the arrangement for payment. The Buyer will now have a car but still needs to pay the Seller for the remaining amount of the value outside of the LC (USD10,000), which they do via a SWIFT payment to the Seller's account.

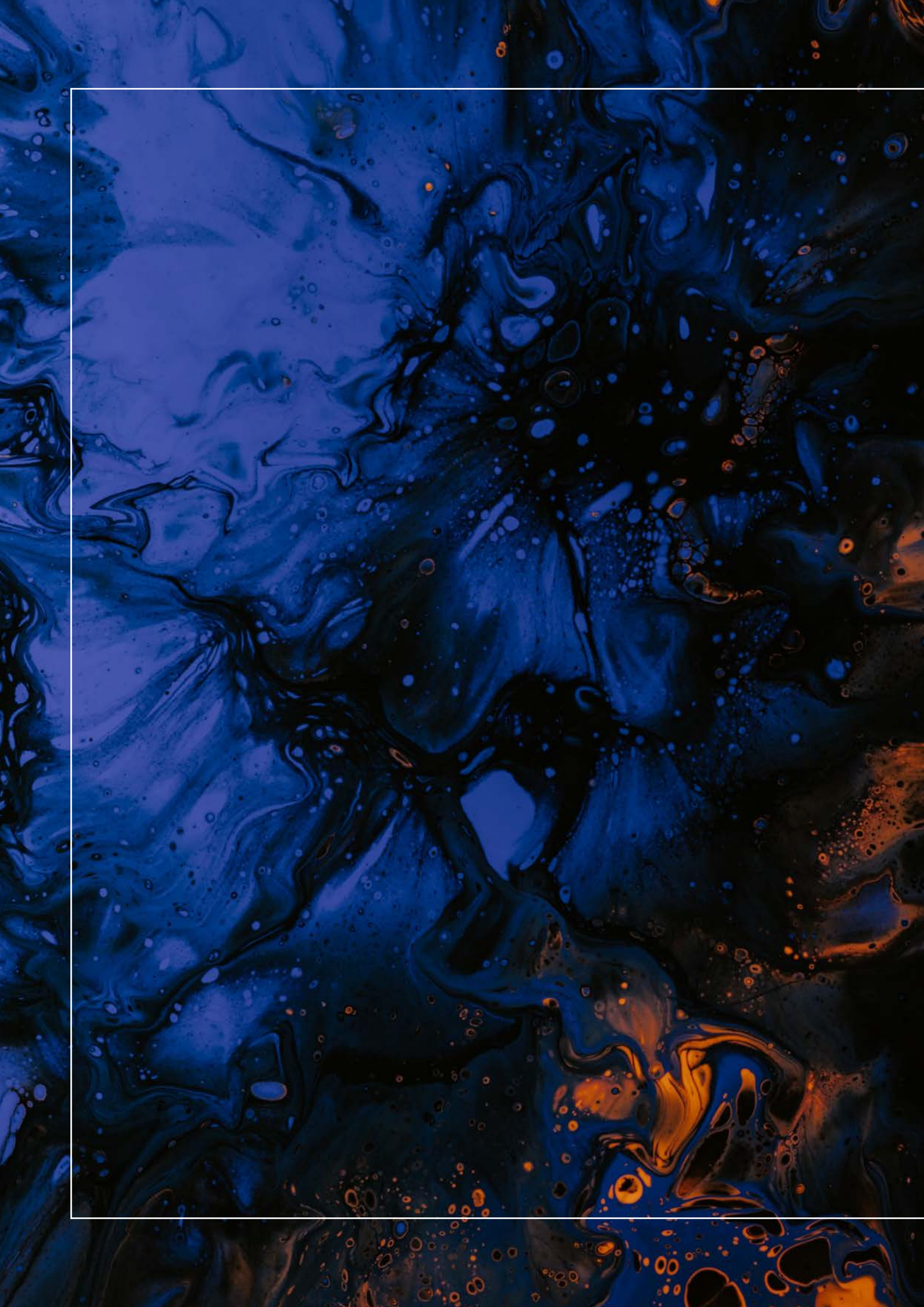
Assuming the Buyer and Seller bank with the same FI, and the LC was issued by this FI, the FI's trade finance operations department will review the finance documents but may be unaware of the true value of the car. They may process the trade finance transaction due to the fact that the LC will be of the same value as the commercial invoice. The department may not, depending on thresholds set within their scenarios, even detect the excess SWIFT payment alert, so no review will be undertaken. This clearly requires collusion between the Buyer and Seller.

If the Buyer and Seller bank with different FIs, one FI may process the LC and another FI may receive the excess funds, no analysis can be undertaken over both transactions.

This case study outlines potential gaps within a FI should they bank both Buyer and Seller, as well as the fact that two separate FIs may not see both transactions, both of which present challenges in identifying TBFC.



CASE STUDY





**Digitalisation
of Trade**

Digitalisation of Trade

With the enhancements of technology comes benefits. Trade and in particular trade finance products would benefit from becoming digital, and the evolution of digital ledger technology (DLT) provides an opportunity to pursue this goal. A consortium of Financial Institutions came together under the banner of Marco Polo Network with the vision of digitalising trade and producing smart contracts, eBill of lading and financing within its own ecosystem. This is still being progressed, but the vision is a step forward.

Several vendors have embarked on a journey to offer optical character recognition (OCR), which extracts data from documents, real time vessel tracking, red flag monitoring along with price checking in a solution. Several countries have developed, or are developing, digital invoicing systems giving legal recognition of digital systems. If universally used, then this should reduce certain types of financial crime, for example double invoicing. Considering the complexity of TBFC, any solution that has been designed to mitigate financial crime must have a holistic view of both internal and external data to fully reach its potential.

TBFC and Technology

Risk mitigation controls combining people, training, processes, systems, data, and governance, along with new technologies seeking to digitalise banking, provide Financial Institutions the means to detect and protect against TBFC. Appropriate risk assessments, know your customer (KYC)/customer due diligence (CDD) procedures, and an understanding of the trading activity of its clients and counterparties should form the heart of an FI's defence.

Financial Institutions sit on a wealth of data. Further, there are a number of FinTech and Data Aggregators deploying advanced techniques to gather external data now increasingly available via application programming interface, better known as API. Financial Institutions are more often collaborating with platform providers, vendors and data aggregators to connect their own customer data and transactional data in order to form a more holistic picture of the activity performed, across value chains and across time periods. Such data may include customers, counterparties, products, and geographies (taking into consideration the transaction activity and trade finance data), third-party providers with a particular focus on trade, which may include shipping data, Companies House data, primary and secondary sanctions exposure (direct and indirect), PEPs, and adverse media. Combining internal and external data provides a richer overview of the customer and its counterparties.

Trade-specific data can be as follows:

- **Vessels:** Information about ownership, type, capacity, and chartering companies
- **Ports:** Locations and sanctions status
- **Dual-Use Goods:** Goods that have both civilian and military applications
- **Detailed shipping information and tracking:** Routes, current locations, goods carried, off- or on-loading at sea and container information

Data about the vessels provides a wealth of information including true ownership and usage. If applied intelligently, this data can be used to assess contracts and additional risk factors, such as ownership by any sanctioned parties and whether the vessel is capable of carrying the goods it is meant to be carrying.

Network Analytics

Analysing data holistically across all data sets can create a network (or graph) database of entities and connections. This form of analysis can identify the linkages between entities to build patterns of ownership, hidden relationships, networks, and map transaction flows between entities. Through the use of advanced data analytics and vast data storage capabilities, the network expands, creating further linkages and providing Financial Institutions with a holistic view of the client's activity, related association and transaction patterns. The output of such analysis forms a spider web picture of linkages which can be investigated with a view of identifying TBFC.

However, trade finance has inherently been largely paper-based and resource intensive. The digitalisation of key documents, such as LCs, improving monitoring and detection processes, reducing costs, and improving efficiency are some of the key areas being addressed by digital ledger technology (DLT) and will continue to be fundamental to combatting financial crime in this space.

According to Quantexa (a software firm headquartered in the UK), advanced analytics and network generation are just some methods being used by several vendors to improve risk coverage across the trade lifecycle, increase speed and automate certain processes/red flag detection, improve risk scoring and alerting, and monitoring. International consortiums and PPPs have been established across a number of countries to share expertise in TBFC and include DLT as a central topic. Regulations will ensure that TBFC controls continue to develop as an intrinsic part of any financial institution's trade finance tool solution.

Digitalisation

The commercial world is making significant efforts to drive digitalisation of trade processes to remove the need for paper documents and manual data entry as part of the trade cycle. This makes sense from a cost and operational effectiveness perspective, but it also benefits AML controls. For example, if data can be accurately extracted from trade documents and automatically entered into screening systems, as opposed to being entered manually, human error can be eliminated, breaks in the process can be avoided, and false positives may be reduced. This not only can lead to straight-through processing and streamlined trade transactions but also it enhances risk management.

Data

Data is key. It is the basis of actional intelligence and the means to understanding the parties in the trade (whether customers or not), the relationships, and the trade transactions. Using additional third-party data, firms can enhance the identification of activity that may warrant further review. The FI's own internal data needs to be of good quality, accurate, and up to date to ensure robust matching and processes are undertaken, avoiding subsequent false positives. All FIs should seek to develop a robust data standards policy outlining to employees the minimal requirements for the quality of data to be input into systems.

Innovation

Clearly the approach to combating TBFC cannot, and should not, rely on one technique; it should encompass people, processes, training and an understanding of specific trends and typologies, as well as making the best use of available data, systems, and technology. There is now a clear case to enhance current systems with new machine learning and AI techniques. This may be through the ability to read and interpret documents, and extract specific data. The use of advanced data analytics on large data sets will identify new threats, highlight new typologies and the creation and interrogation of networks of connected parties will produce a more meaningful overview of the customers' activity. Technology has advanced in a way that can make certain process more efficient, for example the automation of Suspicious Activity Reporting. Couple all this with information sharing across all parties and the responsibility to mitigate TBFC, and technology will go some way in making trade a safer mechanism to undertake global business.

Distributed Ledger Technologies¹⁵¹

The cross-border nature of transactions, settlements, wide pricing margins for certain goods, extended trade cycles (i.e. shipping across multiple jurisdictions), and the difficulties for customs authorities in examining goods; all of these factors make TBML an attractive model for illicit trade and money laundering.

FIs rely primarily on infrastructure and data available in their own organization by implementing their own governance, process and technologies. Duplication of efforts and inconsistency of application are common in the industry in terms of interpreting regulations, defining processes and procedures, building systems and setting up the infrastructure to combat illicit finance. The high costs of meeting AML and KYC requirements is seen as a significant impediment for trade finance growth.

While some of the solutions may exist to help banks identify TBML, typically these systems are not populated with timely, trusted and rich data sets to fully benefit from today's existing solutions. And, as a result, they are often very manual, paper-based, inefficient, and costly to manage.

¹⁵¹R3 and Quantexa contributed extensively to drafting this section

Blockchain or DLT enables secure information sharing to deliver shared facts and the automation of AML controls at the industry level—both inter-bank and inter-firm. It is also financially attractive for market participants, allowing the mutualisation of costs within a business network, while allowing parties to remain in control of their data.

Blockchain technology enables everyone involved in a transaction to know with certainty what happened, when it happened, and confirm other parties are seeing the same thing without the need for an intermediary providing assurance, and without a need to reconcile data afterwards. TBML is an excellent use-case for blockchain because it allows parties such as banks to help build trust by allowing them to validate the authenticity and integrity of documents, all while mutualizing the cost of implementing TBML solutions through common industry platforms.

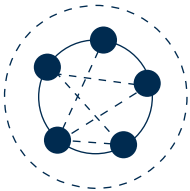
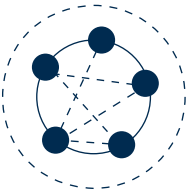
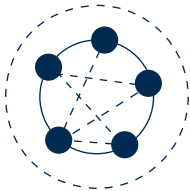
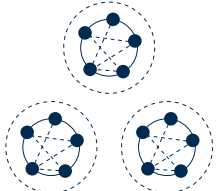
According to R3, developers of the Corda blockchain platform, over 100 trade networks are now on the Corda DLT platform (as of Nov 2021) including banks, corporates, shipping companies and customs departments. Regulatory expectations to improve digitisation and build advanced controls have accelerated DLT usage in Asia. The focus in blockchain over the last five years has been on the digitisation of trade processes, and now there is increased interest in TBFC use-cases. There is a clear change, especially in Asia, amongst regulators and FIs to collaborate to fight financial crime. For example, around 65 banks formed a consortium in Singapore as part of the DLTledgers initiative to evaluate and run PoCs to assess 13 data-fields in a typical B/L to combat double financing.

‘Confidential computing’ refers to new technology which allows interpreting and using data at a point in time without actually letting the data asset move out of its core place. It enables businesses to pool private data sets and jointly perform calculations on them while keeping their data private. It provides transparency on how data is being processed and confidence that data is protected. This is highly important to technology companies and institutions to enable more private to private collaboration and bridge the gap between data privacy and data availability.

Traditionally, collaboration within the financial crime space has been limited, due to data privacy laws and related challenges. Recently, however, Financial Institutions have increased collaboration to advocate for regulatory changes that are better for the industry as whole, defining and sharing best practices or publishing emerging TBML typologies. The pace of new typologies, increasing internal costs and regulatory fines, especially during COVID-19, is forcing banks to rethink how they tackle financial crime in new ways.

Vendors and Financial Institutions are increasingly sensing opportunities to introduce new tools and common industry platforms to spread the cost of solving common industry problems. There is a clear desire to shift from siloed infrastructure to common platforms, which would also force data standardisation and availability.

Figure 11 – Four emerging archetypes to commercialise TBFC solutions

ARCHETYPE	Single Bank Business Network	AML Solution Provider Business Network	Jurisdiction - based Business Network	Network-of-Networks
				
PARTICIPANTS	Single bank (multiple branches)	Customers belonging to one AML Solution Provider	Banks & FIU operate nodes within a jurisdiction	Multiple, connected business networks
BUSINESS NETWORK OPERATOR (BNO)	Bank or Trusted Third Party	AML Solution Provider	New Co or Existing Trusted Third Party	Multiple independent BNO's
BENEFITS OF TRUST TECHNOLOGY	Limited benefits for trust tech at a single bank for TBML	DLT enables secure data sharing, data provenance, mutualisation of cost of building and implementing TBML solutions. Confidential computing enables greater protection for data in use.	Greater mutualisation of cost (at a jurisdiction-level) and scale, Encouraging reuse, avoid data siloes, bespoke integration. Easier to have adoption (regulatory-driven)	Most effective means of combatting TBML. Bridges the gap between data availability and privacy/ data residency/ bank secrecy at an international scale.

Source: Picture courtesy of R3



Risks

Whilst DLT technologies could significantly improve financial crime control frameworks in TBFC, privacy, security protocols and integration with legacy systems remain as key risks and challenge. Without standardisation of trade information/data and mass adoption, the ability to transmit information to parties outside the system will remain a challenge. Keeping shared data safe might remain a significant hurdle; well-designed controls need to be developed to ensure data sharing especially in the context of systems and data accessed cross-border. Further, preventing collusion, and the risk of information leading to commercial risks for Financial Institutions, need to be considered in the context of anti-competition regulations.

Tech companies are now closer than ever to the financial world. With great opportunity, also comes great responsibility. Tech companies need to appreciate the strict rules based on the pillars of finance that were built over decades, and support the maintenance and improvement of these pillars for aiding sustainable prosperity.

The future of DLT adoption

Whilst it is still uncertain how DLTs and advanced technologies may evolve, there are two likely possibilities:

- Regulation-driven adoption, potentially operating infrastructure at a local level (for example, connecting the trade eco-system in a country)
- With more scale and technology adoption, core DLT developers could work with software and platform providers in AML / TBFC and build be-spoke solutions



Conclusion

All economic activity needs to be funded or financed in some form, and growing national economies reflect increasing economic activity, including domestic and international trade. Most such activity is legitimate, laudable and highly desirable. Some, however, is not. The funding and financing of illegitimate activity is clearly a risk that jurisdictions and the financial sector need to assess. Equally, funding and financing of legitimate economic activity and its related trade may carry risks of financial crime that need to be assessed and mitigated.

This document is focused on TBFC; illegitimate activity in this respect may include but is not restricted to, money laundering, terrorist financing, drugs trafficking, human trafficking, trafficking in conventional weapons or weapons of mass destruction and related materials, fraud, or theft. Many different types of actors may be involved and identifying them is a challenge for both jurisdictions and the financial sector. The good news, however, is that many of the methods involved are relatively well known. This document describes most of the techniques related to trade, many of which revolve around the falsification of trade-related documentation, including over- and under-invoicing of goods, false descriptions of goods, and fictitious shipments. TBFC can be complex, involving multiple parties, probably in different jurisdictions, possibly with different legal standards.

The responsibility of combating and countering TBFC fundamentally lies at the feet of jurisdictional authorities. Here, the FATF has a very important role to play; it has published clear global standards designed to combat money laundering and the financing of terrorism and proliferation of weapons of mass destruction. Many of these relate to TBFC. Jurisdictions need to ensure that, where it does not already exist, effective legislation to combat TBFC, in line with FATF standards, is enacted and enforced.

Authorities also need to publish guidance for the financial sector on standards expected in terms of compliance and reporting, as well as share information on typologies. In turn, financial sector entities need to ensure they have appropriate compliance procedures in place to meet regulatory requirements and that staff are trained accordingly. TBFC risk assessments, tuned to the full range of possible threats and regularly updated, should be standard practice. As most international trade is inherently cross border, regulatory requirements may extend to those of foreign countries in addition to those of the local jurisdiction.

Combating TBFC successfully, as with other types of financial crime, depends on information sharing, and where PPPs do not already exist, the public and private sectors in each jurisdiction should consider creating effective mechanisms to share intelligence. In so doing, jurisdictions and private sector entities will not only help to defend their own interests in terms of meeting compliance standards, but will also support the efforts of the international community more generally to combat TBFC.

Bibliography

- US Department of the Treasury. "486. What Is an Example of Goods Otherwise Coming into Contact with Iran?," December 22, 2016. <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/486>.
- Affaki, Georges, Karin Bachmayer, Roeland Bertrams, Rolf J. Breisig, Maximilian Burger-Scheidlin, Mohammad M. Burjaq, Carlo Calosso, et al. *Guide to ICC Uniform Rules for Demand Guarantees (URDG758)*. E702E. Paris: International Chamber of Commerce, 2010. https://2go.iccwbo.org/guide-to-icc-urdg-config+book_version-eBook/.
- VinciWorks Blog. "Anti-Money Laundering – a Guide to Customer Due Diligence," June 27, 2018. <https://vinciworks.com/blog/anti-money-laundering-a-guide-to-customer-due-diligence/>.
- Asia/Pacific Group on Money Laundering. "APG Typology Report on Trade Based Money Laundering." Sydney: Asia/Pacific Group on Money Laundering, 2012. http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf.
- BAFT. *Combatting Trade Based Money Laundering: Rethinking the Approach*. Washington, D.C.: BAFT, 2017.
- Legal Dictionary. "Bill of Lading." Accessed December 20, 2021. <https://legaldictionary.net/bill-of-lading/>.
- Investopedia. "Blank Endorsement on a Bill of Lading." Accessed December 20, 2021. <https://www.investopedia.com/ask/answers/032615/what-endorsement-blank-bill-lading.asp>.
- Bou Mansour, Mark. "\$427bn Lost to Tax Havens Every Year: Landmark Study Reveals Countries' Losses and Worst Offenders." Tax Justice Network, November 20, 2020. <https://taxjustice.net/2020/11/20/427bn-lost-to-tax-havens-every-year-landmark-study-reveals-countries-losses-and-worst-offenders/>.
- Brewer, Jonathan. *Study of Typologies of Financing of WMD Proliferation*. London: King's College London, 2017. <https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf>.
- Byrne, James E., James G. Barnes, and Gary W. Collyer. *International Standby Practices (ISP98)*. E590E. Paris: International Chamber of Commerce, 1998. https://2go.iccwbo.org/international-standby-practices-isp98-config+book_version-eBook/.
- Byrne, James E., and Justin B. Berger. *Trade Based Financial Crime Compliance*. Montgomery Village, MD: Institute of International Banking Law & Practice; London Institute of Banking & Finance, 2017.
- Cassara, John. "Service-Based Money Laundering: The Next Illicit Finance Frontier." Foundation for Defense of Democracies, May 19, 2016. <https://www.fdd.org/analysis/2016/05/19/service-based-money-laundering-the-next-illicit-finance-frontier/>.
- Caves III, John P., and Meghan Peri Crimmins. *Major Turkish Bank Prosecuted in Unprecedented Iran Sanctions Evasion Case*. Iran Watch Report. Madison, WI: Wisconsin Project on Nuclear Arms Control, 2020. <https://www.wisconsinproject.org/wp-content/uploads/2020/04/Major-Turkish-Bank-Prosecuted-Unprecedented-Iran-Sanctions-Evasion-Case.pdf>.
- ACAMS. "Certified Global Sanctions Specialist Certification." Accessed March 22, 2022. <https://www.acams.org/en/certifications/certified-global-sanctions-specialist-cgss#overview-e3b4081f>.
- Corsinie, Tauren. "Counting the Cost (Cost of Compliance vs Cost of Non-Compliance)." 1RS (blog), October 11, 2021. <https://1rs.io/2021/10/11/counting-the-cost-cost-of-compliance/>.
- Dictionary.com. "Definition of Tax." Accessed December 17, 2021. <https://www.dictionary.com/browse/tax>.
- Dunne, Aaron. "The Role of Transit and Transshipment in Counterproliferation Efforts." SIPRI Good Practice Guide. Stockholm: SIPRI, September 2016. https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2006_Dunne.pdf.
- European Parliament. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, PE/30/2018/REV/1 § (2018). <https://eur-lex.europa.eu/eli/dir/2018/1673/oj>.
- European Union. Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, Pub. L. No. No. 2271/96 (1996). <http://data.europa.eu/eli/reg/1996/2271/2018-08-07/eng>.
- US Bureau of Industry and Security. "Examples of Boycott Requests." Accessed March 21, 2022. <https://www.bis.doc.gov/index.php/enforcement/oac/7-enforcement/578-examples-of-boycott-requests>.
- Executive Office of the Committee for and Goods Subject to Import and Export Control. *Typologies on the Circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction*. Dubai: Government of the United Arab Emirates, 2021. <https://www.centralbank.ae/sites/default/files/2021-08/Typologies%20on%20circumvention%20of%20Targeted%20Sanctions%20agst%20Terr.%20and%20the%20Prolif.%20of%20WMD%20-%20Ex.Office%20IEC%20May2021.pdf>.

- Financial Action Task Force. "FATF President Juan Manuel Vega-Serrano's Remarks at the Meeting of the UN Security Council, December 15, 2016," December 15, 2016. <http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-vega-serrano-un-security-council-meeting-dec2016.html>.
- Financial Action Task Force. "FATF Steps up the Fight against Money Laundering and Terrorist Financing," February 16, 2012. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html>.
- Financial Action Task Force. *Best Practices on Trade Based Money Laundering*. Paris: Financial Action Task Force, 2008. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bestpracticesontradebasedmoneylaundering.html>.
- . *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*. Paris: Financial Action Task Force, 2010. <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>.
- . *FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*. Paris: Financial Action Task Force, 2018. <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf>.
- . *International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)*. Paris: Financial Action Task Force, 2013. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf>.
- . *Proliferation Financing Report*. Paris: Financial Action Task Force, 2008. <https://www.fatf-gafi.org/media/fatfdocuments/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>.
- . *Terrorist Financing*. Paris: Financial Action Task Force, 2008. <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>.
- . *Trade Based Money Laundering*. Paris: Financial Action Task Force, 2006. <https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf>.
- Financial Action Task Force and Egmont Group. *Trade-Based Money Laundering: Risk Indicators*. Paris: Financial Action Task Force, 2021. <https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-indicators.html>.
- . *Trade-Based Money Laundering: Trends and Developments*. Paris: Financial Action Task Force, 2020. <https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html>.
- Internal Revenue Service. "Foreign Account Tax Compliance Act (FATCA)." Accessed December 17, 2021. <https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca>.
- Global Compliance Institute. "Certified Compliance Manager Manual." Spring Hill, Australia: Global Compliance Institute, 2020. <https://www.gci-ccm.org/node/4>.
- . "Sanctions Compliance Specialist Manual." Spring Hill, Australia: Global Compliance Institute, 2020. <https://www.gci-ccm.org/certificate/scs-sanctions-compliance-specialist>.
- Eurostat. "Glossary: Transshipment." Accessed December 20, 2021. <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Transshipment>.
- Hong Kong Association of Banks. "Guidance Paper on Combating Trade-Based Money Laundering." Hong Kong: Hong Kong Association of Banks, 2016. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/Guidance_Paper_on_Combating_Trade-based_Money_Laundering.pdf.
- University of Maine. "Hot Topics: Terrorism in the Middle East: Terrorist Groups." Accessed December 16, 2021. <https://libguides.library.umaine.edu/c.php?g=144444&p=2961556>.
- International Compliance Association. "ICA Specialist Certificate in Trade Based Money Laundering." Accessed March 22, 2022. <https://www.int-comp.org/programme/?title=ICA-Specialist-Certificate-in-Trade-Based-Money-Laundering>.
- Institute for Economics & Peace. *Global Terrorism Impact 2020: Measuring the Impact of Terrorism*. Sydney: Institute for Economics & Peace, 2020. <https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf>.
- International Chamber of Commerce. *Uniform Rules for Documentary Credit (UCP600)*. E600E. Paris: International Chamber of Commerce, 2007. https://2go.iccwbo.org/uniform-rules-for-documentary-credits-config+book_version-eBook/.
- Jean, Sébastien, and Cristina Mitaritonna. "Determinants of and Pervasiveness of the Evasion of Customs Duties." CEPII Working Paper Number 2010-26. CEPII, November 2010.
- iContainers. "LCL vs FCL." Accessed December 20, 2021. <https://www.icontainers.com/help/lcl-vs-fcl/>.
- League of Arab States. *The Arab Convention For The Suppression of Terrorism*, Cairo § Council of Arab Ministers of the Interior and Council of Arab Ministers of Justice (1998).

- London Institute of Banking & Finance. *Certificate of International Trade and Finance Manual*. London: London Institute of Banking & Finance, 2019. <https://www.libf.ac.uk/study/professional-qualifications/trade-finance/certificate-in-international-trade-and-finance>.
- Manaadiar, Hariesh. "What Is a Switch Bill of Lading and When and Why Is It Used.???" Shipping and Freight Resource, February 1, 2019. <https://www.shippingandfreightresource.com/what-is-a-switch-bill-of-lading-and-when-and-why-is-it-used/>.
- Menon, Hari. "What Is Seaway Bill in Shipping?" *Marine Insight* (blog), December 21, 2021. <https://www.marineinsight.com/maritime-law/what-is-seaway-bill-in-shipping/>.
- Mills-Sheehy, Jeremy, and James Kane. "Trade: Freeports and Free Zones." The Institute for Government, July 22, 2021 <https://www.instituteforgovernment.org.uk/explainers/trade-freeports-free-zones>.
- Moiseienko, Anton, Alexandria Reid, and Isabella Chase. *Improving Governance and Tackling Crimes in Free-Trade Zones*. London: Royal United Services Institute, 2020. https://static.rusi.org/20201012_ftzs_web_2.pdf.
- Monetary Authority of Singapore. *Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking*. Singapore: Monetary Authority of Singapore, 2015. <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Guidance-on-AML-CFT-Controls-in-Trade-Finance-and-Correspondent-Banking.pdf>.
- Financial Action Task Force. "Money Laundering." Accessed December 13, 2021. <https://www.fatf-gafi.org/faq/moneylaundering/>.
- United Nations Office on Drugs and Crime. "Money Laundering." Accessed December 13, 2021. <https://www.unodc.org/unodc/en/money-laundering/overview.html>.
- Sanction Scanner. "National Risk Assessment | What Is NRA?" Accessed March 22, 2022. <https://sanctionscanner.com/knowledge-base/national-risk-assessment-of-money-laundering-321>.
- Organisation for Economic Co-operation and Development. "OECD Recommendation on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones," October 21, 2019. <https://www.oecd.org/gov/risk/recommendation-enhancing-transparency-free-trade-zones.htm>.
- Organisation for Economic Co-operation and Development. *Standard for Automatic Exchange of Financial Information in Tax Matters: Implementation Handbook; Second Edition*. Paris: OECD, 2018. <https://www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-information-in-tax-matters.pdf>.
- Reich, Walter. *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Woodrow Wilson Center Press, 1998.
- United Nations Security Council. "Resolution 2231 (2015) on Iran Nuclear Issue." Accessed December 17, 2021. <https://www.un.org/securitycouncil/content/2231/background>.
- SWIFT. "RMA and RMA Plus: Managing Correspondent Connections," July 10, 2018. <https://www.swift.com/news-events/news/rma-and-rma-plus-managing-correspondent-connections>.
- United Nations Security Council. "Security Council Committee Established Pursuant to Resolution 1718 (2006)." Accessed December 17, 2021. <https://www.un.org/securitycouncil/sanctions/1718>.
- United Nations Security Council. "Security Council Committee Pursuant to Resolutions 1267 (1999) 1989 (2011) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities." Accessed December 17, 2021. <https://www.un.org/securitycouncil/sanctions/1267>.
- US Department of the Treasury. "Settlement Agreement between the US Department of the Treasury's Office of Foreign Assets Control and Blue Sky Blue Sea, Inc., Doing Business as American Export Lines and International Shipping Company (USA)," August 17, 2017. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20170817_33.
- European Commission. "TARIC Consultation." Accessed March 23, 2022. https://ec.europa.eu/taxation_customs/dds2/taric/taric_consultation.jsp?Lang=en.
- Wolters Kluwer. "Tax Avoidance Is Legal; Tax Evasion Is Criminal," November 6, 2020. <https://www.wolterskluwer.com/en/expert-insights/tax-avoidance-is-legal-tax-evasion-is-criminal>.
- World Bank. "Taxes & Government Revenue." Accessed December 17, 2021. <https://www.worldbank.org/en/topic/taxes-and-government-revenue>.
- Teichmann, Fabian M., and Madeleine Camprubi. "Money Laundering Through Consulting Firms." *Compliance Elliance Journal* 5, no. 2 (2019): 60–72.
- Financial Action Task Force. "The FATF Recommendations," October 2021. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.
- Sohatoos. "The Middle East Free Zones." Accessed March 22, 2022. <https://sohatoos.com/en/the-middle-east-free-zones>.

- The Wolfsberg Group. "Monitoring Screening and Searching: Wolfsberg Statement." The Wolfsberg Group, September 2003. https://ms.hmb.gov.tr/uploads/sites/2/2019/04/monitoring_statement.pdf.
- . "The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption." Ermatingen, Switzerland: The Wolfsberg Group, 2015. <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf>.
- . "Wolfsberg Guidance on Sanctions Screening." Ermatingen, Switzerland: The Wolfsberg Group, 2019. <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf>.
- . "Wolfsberg Statement: Guidance on a Risk Based Approach for Managing Money Laundering Risks." Ermatingen, Switzerland: The Wolfsberg Group, 2006. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf.
- The Wolfsberg Group, International Chamber of Commerce, and BAFT. *The Wolfsberg Group, ICC and BAFT Trade Finance Principles: 2019 Amendment*. Paris: The Wolfsberg Group; International Compliance Association; BAFT, 2019. <https://iccwbo.org/content/uploads/sites/3/2019/03/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf>.
- Clyde & Co. "Trade Based Money Laundering (TBML) Risk in the Freight Forwarding and Customs Broking Sectors." Accessed December 20, 2021. <https://www.clydeco.com/insights/2020/12/trade-based-money-laundering-tbml-risk-in-the-frei>.
- Global Financial Integrity. "Trade-Related Illicit Financial Flows in 134 Developing Countries 2009-2018," December 16, 2021. <https://gfintegrity.org/report/trade-related-illicit-financial-flows-in-134-developing-countries-2009-2018/>.
- US Department of the Treasury. "Treasury Sanctions Those Involved in Ballistic Missile Procurement for Iran," January 17, 2016. <https://www.treasury.gov/press-center/press-releases/pages/jl0322.aspx>.
- UK Financial Conduct Authority. *Banks' Control of Financial Crime Risks in Trade Finance*. Thematic Review TR13/3. London: Financial Conduct Authority, 2013. <https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf>.
- UK Government. "UK Integrated Online Tariff: Look up Commodity Codes, Duty and VAT Rates." Accessed March 23, 2022. https://www.trade-tariff.service.gov.uk/find_commodity.
- United Nations. International Convention for the Suppression of the Financing of Terrorism (1999). https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en.
- . United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988). https://www.unodc.org/pdf/convention_1988_en.pdf.
- United Nations Security Council. Resolution 1373 (2001), Adopted by the Security Council at its 4385th meeting, on 28 September 2001, S/RES/1373 (2001) § (2001). [https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373\(2001\)](https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1373(2001)).
- US Department of State. *Money Laundering and Financial Crimes Country Database*. Washington, D.C.: US Department of State, 2015. <https://2009-2017.state.gov/documents/organization/239329.pdf>.
- US Government Accountability Office. *Trade-Based Money Laundering: US Government Has Worked with Partners to Combat the Threat, but Could Strengthen Its Efforts*. Washington, D.C.: US Government Accountability Office, 2020. <https://www.gao.gov/assets/gao-20-333.pdf>.
- Waerzeggers, Christophe, and Cory Hillier. "Introducing a General Anti-Avoidance Rule (GAAR)." Washington, D.C.: International Monetary Fund, 2016.
- NYC Supply Chain Solutions Inc. "What Is Bill of Lading?" Accessed March 17, 2022. <https://nycscs.com/what-is-bill-of-lading/>.
- World Customs Organization. "What Is the Harmonized System (HS)?" Accessed February 17, 2022. <http://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx>.
- World Trade Organization. *World Trade Statistical Review 2021*. Vienna: World Trade Organization, 2021. https://www.wto.org/english/res_e/statis_e/wts2021_e/wts2021_e.pdf.
- Yansura, Julia, Channing Mavrellis, Lakshmi Kumar, and Claudia Helms. *Financial Crime in Latin America and the Caribbean: Understanding Country Challenges and Designing Effective Technical Responses*. Washington, D.C.: Global Financial Integrity, 2021. <https://gfintegrity.org/report/financial-crime-in-latin-america-and-the-caribbean/>.
- Yurlova, Aliona. "Switch Bill of Lading: A Complete Manual and Word of Advice." iContainers, October 30, 2018. <https://www.iconainers.com/us/2018/11/01/switch-bill-of-lading-complete-manual/>.
- Zangari, Ernesto, Antonella Caiumi, and Thomas Hemmelgarn. "Tax Uncertainty: Economic Evidence and Policy Responses." Taxation Papers. Brussels: European Commission, 2015. https://ec.europa.eu/taxation_customs/system/files/2017-04/taxation_paper_67.pdf.

Appendices

Appendix I: Recommended Resources

Cross Subject

- UNODC and IMF, [Model legislation on money laundering and financing of terrorism](#) (2005)

Trade Finance

- [Uniform Customs and Practice for Documentary Credits, 2007 Revision](#) (ICC publication No. 600, also known as UCP600): The UCP has been published in several editions since 1933. The current edition, UCP 600, came into effect on 1 July 2007. These rules are primarily intended for documentary credits but can be used for standby letters of credit. Some banks frequently issue standby letters of credit incorporating UCP 600. The rules are not designed to be used with demand guarantees, but one might occasionally see a demand guarantee incorporating UCP 600. However, this is not recommended.
- [International Standby Practices, 1998 edition](#) (ICC publication No. 590, also known as ISP98): These rules are primarily intended for use with standby letters of credit. They may also be used with demand guarantees but are not appropriate for documentary credits. The rules were initially prepared and promoted by the Institute of International Banking Law & Practice (IIBLP). The rules were then adopted and published by the ICC. IIBLP remains active in supporting the use of ISP98 in standby letters of credit.
- [Uniform Rules for Demand Guarantees, 2010 revision](#) (ICC publication No. 758, also known as URDG758): These rules are intended for demand guarantees but may be used for standby letters of credit. They are not appropriate for documentary credits. The first edition of the rules, URDG 458, came into effect in April 1992. The second edition, URDG 758, came into effect on 1 July 2010.
- [International Standard Banking Practice for the Examination of Documents under UCP 600](#) (ISBP 745): International Standard Banking Practice — 2013 edition is the most up-to-date guide for the examination of documents under documentary credits which reflects practices agreed by ICC national committees. It also serves as an aid to a beneficiary of a documentary credit in its creation and presentation of documents to a nominated bank or issuing bank. The publication should always be read in conjunction with UCP 600.
- [Uniform Rules for Collection](#) (ICC Publication No. 522, also known as URC 522): The ICC Uniform Rules for Collections were first published by the ICC in 1956. Revised versions were issued in 1967 and 1978; this present revision was adopted by the Council of the ICC in June 1995.

Proliferation Financing

- FATF, [Typologies Report on Proliferation Financing](#) (2008)
- FATF, [FATF Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction](#) (2018)
- FATF, [Guidance on Proliferation Financing Risk Assessment and Mitigation](#) (2021)

- US Department of the Treasury, [National Proliferation Financing Risk Assessment](#) (2018)
- King's College London, [Study of Typologies of Financing of WMD Proliferation](#) (2017)
- Royal United Services Institute (London), [Guide to Conducting a National Proliferation Financing Risk Assessment](#) (2019)
- Center for New American Security (Washington, D.C.), [The Financing of WMD Proliferation: Conducting Risk Assessments](#) (2018)

Terrorism and Terrorist Financing

- FATF, [Terrorist Financing](#) (2008)
- FATF, [International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing \(Recommendation 6\)](#) (2013)
- FATF, [Guidance on Criminalising Terrorist Financing](#) (2016)
- FATF, [Terrorist Financing Risk Assessment Guidance](#) (2019)
- Wilson Center, [Report: Terrorism on Decline in Middle East and North Africa](#) (2019)
- FATF, [Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing](#) (2020)
- Government of UAE, "[Maintaining safety and security](#)"

Appendix II: Additional Information on Payment Messages / Trade SWIFT messages

As explained by the Global Compliance Institute, "when the Applicant Bank (Importer) issues the letter of credit to the Beneficiary Bank (Exporter), they use the Banking Authenticated Message System (SWIFT). This means that if there is an integration tool between the SWIFT system (such as SWIFT Alliance Access)¹⁵² and the Name Screening System, then all data within the SWIFT message will be checked. If there is any potential match between the data mentioned within the SWIFT message and a Sanctions Target, then the SWIFT will be stopped, to allow the alert to be investigated."¹⁵³

There are many different types of documentary credit and letter of guarantees messages used within SWIFT. Some examples include:

- **MT700:** Issue of a Documentary Credit - Indicates the terms and conditions of a documentary credit
- **MT720:** Transfer of a Documentary Credit - Advises the transfer of a documentary credit, or part thereof, to the bank advising the second beneficiary¹⁵⁴
- **MT710:** Advice of a Third Bank's or a Non-Bank's Documentary Credit
- **MT760:** Issue of a Demand Guarantee / Standby Letter of Credit

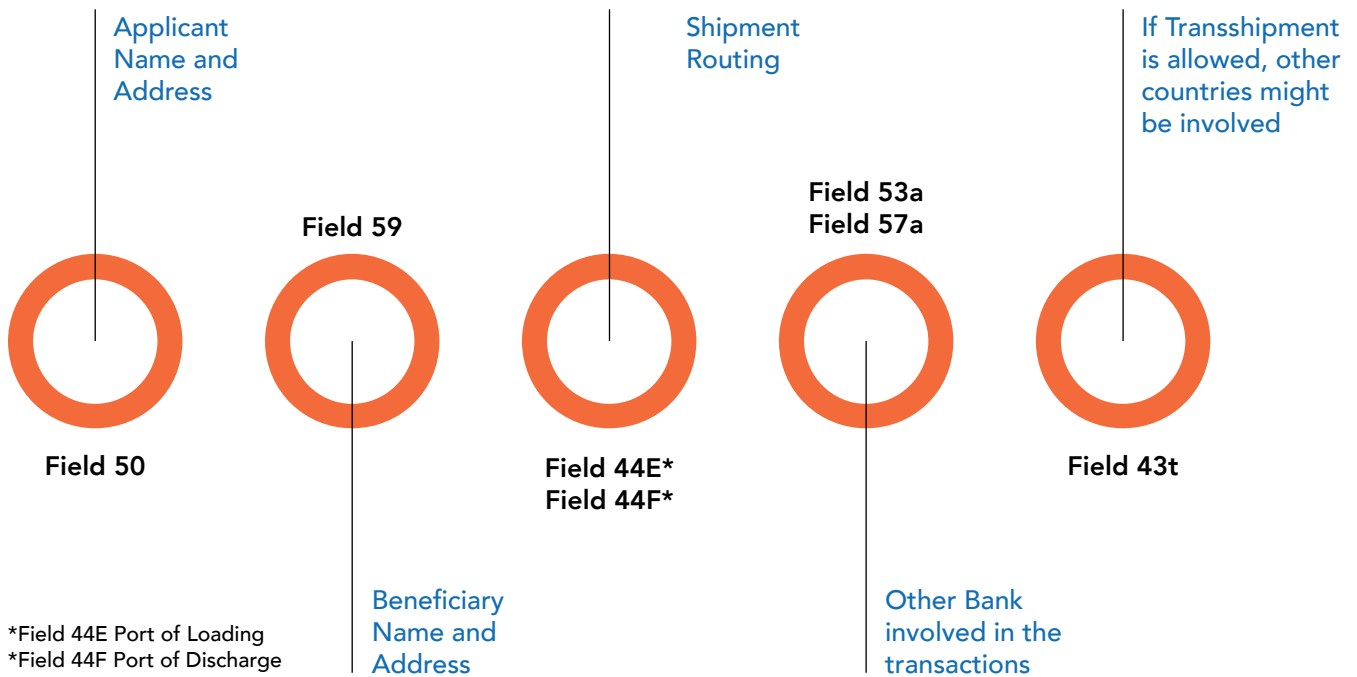
The data available on a SWIFT message should be examined for sanctions risks. Figure 12 is an example of the main fields which need to be examined for an MT700 message.

¹⁵²Alliance Access, SWIFT's market-leading messaging interface, allows banks and market infrastructures to connect to SWIFT.

¹⁵³Global Compliance Institute, "Sanctions Compliance Specialist Manual" (Spring Hill, Australia: Global Compliance Institute, 2020), 39–40, <https://www.gci-ccm.org/certificate/scs-sanctions-compliance-specialist>.

¹⁵⁴In regards to transferable LC's, Article (38) of UCP 600 states that transferable credit means a credit that specifically states it is "transferable". Transferred credit means a credit that has been made available by the transferring bank to a second beneficiary.

Figure 12 – Key fields within an MT700 message



Source: Global Compliance Institute, "Sanctions Compliance Specialist Manual" Page 40.

Appendix III: Harmonised System Codes

The following discussion of the harmonised system (HS) codes is provided by the World Customs Organization:

The Harmonised Commodity Description and Coding System generally referred to as "Harmonised System" or simply "HS" is a multipurpose international product nomenclature developed by the World Customs Organization (WCO).

It comprises more than 5,000 commodity groups; each identified by a six-digit code, arranged in a legal and logical structure and is supported by well-defined rules to achieve uniform classification.

The system is used by more than 200 countries and economies as a basis for their Customs tariffs and for the collection of international trade statistics. Over 98% of the merchandise in international trade is classified in terms of the HS.

The HS contributes to the harmonization of Customs and trade procedures, and the non-documentary trade data interchange in connection with such procedures, thus reducing the costs related to international trade.

It is also extensively used by governments, international organisations and the private sector for many other purposes such as internal taxes, trade policies, monitoring of controlled goods, rules of origin, freight tariffs, transport statistics, price monitoring, quota controls, compilation of national accounts, and economic research and analysis. The HS is thus a universal economic language and code for goods, and an indispensable tool for international trade.¹⁵⁵

¹⁵⁵What Is the Harmonized System (HS)?," World Customs Organization, accessed February 17, 2022, <http://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx>.

Based on the risk profile of the transaction, Financial Institutions may need to compare the description and/or HS code of the traded goods if available in the supporting trade and transport documentation with the official commodity codes. However, it is important to note that HS codes are only harmonised to the six-digit level; each country or jurisdiction has their own unique designation for eight-, nine-, and/or ten-digit HS codes (what are sometimes referred to as “tariff-level” codes). Therefore, when verifying the commodity code provided on trade documentation, it is important to use the correct source, which typically involves reviewing a country’s tariff classifications. For example, if a financial institution is looking at documentation concerning an import of goods into France, they need to ensure they review the EU’s customs tariffs to get an accurate description, such as visiting the European Commission’s TARIC Consultation portal.¹⁵⁶ Or if goods were exported from the UK, the financial institution should use the UK Integrated Online Tariff portal.¹⁵⁷

Appendix IV: TBFC Red Flags and Risk Indicators

The following are key red flags and risk indicators for TBFC collected from the FATF¹⁵⁸, BAFT¹⁵⁹, US Federal Financial Institutions Examination Council (FFIEC)¹⁶⁰, The Wolfsberg Group¹⁶¹, UK Financial Conduct Authority¹⁶², APG¹⁶³, Hong Kong Association of Banks¹⁶⁴, Monetary Authority of Singapore¹⁶⁵, and ICC.¹⁶⁶

Table 7 – Red Flags and Risk Indicators Related to Documentation

No.	Risk Indicators
1	Re-presentation of an official document immediately after a turn-down for discrepancy
2	Documents accepted as presented with indication of falsely described of goods or services that are inconsistent with the letter of credit (LC), letter of guarantee (LG) or documentary collection (DC)
3	Import LCs issuance involve presenting one of the following: delivery note, delivery order, cargo receipt, forwarder’s certificate of receipt, forwarder’s certificate of shipment, forwarder’s certificate of transport, forwarder’s cargo receipt, and mate’s receipt
4	Request a bill of lading (B/L) or any documents allowing a third party
5	Documents issued by a person rather than the applicant or the beneficiary under LG are in another language

¹⁵⁶See “TARIC Consultation,” European Commission, accessed March 23, 2022, https://ec.europa.eu/taxation_customs/dds2/taric/taric_consultation.jsp?Lang=en.
¹⁵⁷See “UK Integrated Online Tariff: Look up Commodity Codes, Duty and VAT Rates,” UK Government, accessed March 23, 2022, https://www.trade-tariff.service.gov.uk/find_commodity.
¹⁵⁸Financial Action Task Force, Best Practices on Trade Based Money Laundering (Paris: Financial Action Task Force, 2008), <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bestpracticesontradebasedmoneylaundering.html>; Financial Action Task Force, Trade Based Money Laundering; Financial Action Task Force and Egmont Group, TBML: Trends and Developments; Financial Action Task Force and Egmont Group, Trade-Based Money Laundering: Risk Indicators (Paris: Financial Action Task Force, 2021), <https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-indicators.html>.
¹⁵⁹BAFT, Combatting Trade Based Money Laundering: Rethinking the Approach (Washington, D.C.: BAFT, 2017).
¹⁶⁰<https://www.ffiec.gov/>
¹⁶¹<https://www.wolfsberg-principles.com/sites/default/files/wb/Trade%20Finance%20Principles%202019.pdf>
¹⁶²<https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf>
¹⁶³Asia/Pacific Group on Money Laundering, “APG Typology Report.”
¹⁶⁴Hong Kong Association of Banks, “Guidance Paper on Combating Trade-Based Money Laundering” (Hong Kong: Hong Kong Association of Banks, 2016), https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/Guidance_Paper_on_Combating_Trade-based_Money_Laundering.pdf.
¹⁶⁵Monetary Authority of Singapore, Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking (Singapore: Monetary Authority of Singapore, 2015), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Guidance-on-AML-CFT-Controls-in-Trade-Finance-and-Correspondent-Banking.pdf>.
¹⁶⁶See Appendix I: Additional Resources

6	A condition under LCs or LGs additional terms and conditions text allowing switch B/L or blank endorsed B/L or a copy from them, and the customer makes a trade-related claim on a stand-by L/C before or a short period of time after its issuance
7	Indication that transshipment has taken place in transport documents
8	Indication of intended vessel under B/L without a named vessel or B/L with a future date
9	Unusual codes, markings or stamps appearing on monetary instruments such as drafts or bills of exchange (e.g. country codes such as SY, SD, IR, IRISL, RU). Where SY refers to Syria, SD refers to Sudan, IR refers to Iran, RU refers to Russia, for the abbreviation IRISL it could be referred to shipping lines for the Islamic Republic of Iran
10	Many discrepancies in the documents' merchandise descriptions, e.g. quantities, weights, etc.
11	The LC contains non-standard clauses or phrases or has unusual characteristics
12	Trade-related documentation under an LC or DC appears illogical, altered, fraudulent, or certain documentation is absent that would be expected given the nature of the transaction
13	The payment terms or tenor are inconsistent with the type of goods
14	The LC is frequently significantly amended for extensions, changes to the beneficiary, and/or changes to payment location/instructions
15	Indication that vessel loitering and/or spoofing took place based on vessel tracking
16	There are indications of double invoicing in conjunction with export/import documents that have yet to be presented
17	Service locations or description of services that are inconsistent with the SBLC
18	Indication that documents have been reused due to sanctions
19	LC or collection purportedly covers the movement of goods but fails to call for presentation of transport documents or 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
20	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
21	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

22	Contracts supporting complex or regular trade transactions appear to be unusually simple
23	Commodities imported into a country within the framework of temporary importation and inward processing regime are subsequently exported with falsified documents
24	B/L describes containerised cargo but no container numbers are evidenced
25	Charter Party B/L shows clause "Always Afloat" then tracking the vessel should be conducted carefully

Table 8 – Red Flags and Risk Indicators Related to the Customer

No.	Risk Indicators
1	The customer engages in transactions that are inconsistent with the customer's business profile (e.g. a steel company that starts dealing in paper products) or overly complex transaction structure without a clear and legitimate commercial purpose or some reasonable justification
2	A customer deviates significantly from their historical pattern of trade activity
3	Customer conducts business in jurisdictions that are at higher risk for money laundering, terrorist financing, sanctions evasion or other financial crimes
4	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
5	Advance waivers provided or pre-accepted discrepancy(s) by the applicant and/or the applicant is over-keen to waive discrepancy(s)
6	The customer has no experience in the goods in question, or the size or frequency of the shipments appear inconsistent with the scale of the customer's regular business activities (e.g. a sudden surge in transaction volume)
7	The 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.
8	The 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
9	The customer reacts aggressively to Know Your Customer questions and requests
10	The customer offers to pay unusually high charges and fees to process any trade finance products or open account transactions basis

11	Unclear identity or connections
12	Payment instructions are changed at the last minute
13	Transactions are conducted from residential addresses, jurisdictions at high risk for money laundering, or non-cooperative countries identified by FATF
14	A trade entity is registered or has offices in a jurisdiction with weak AML/CFT compliance

Table 9 – Red Flags and Risk Indicators Related to the Shipment

No.	Risk Indicators
1	Obvious misrepresentation of quantity of goods shipped: over-shipment or significantly overdrawn LC
2	B/L describing containerised cargo but without container numbers, with sequential numbers, non-standard numbers or indicates Islamic Republic of Iran Shipping Lines ("IRISL") or IRISL-affiliated entity container numbers (i.e. numbers containing the prefixes of "IRSU", "SBAU", or "HDXU")
3	Trade transactions where the quantity of goods exceeds the known capacity of the shipping containers or tanker capacity, or where abnormal weights for goods are suspected
4	Container numbers lacking, or are sequential, or are incompatible with size of shipment, indication for container(s) fraud with indication of high value and volume of shipping charges
5	Negative report from IMB on the underlying shipment
6	Import LC's with letter of indemnity (LOI) documentation and indication with high seas sales condition
7	Trade activity done from port which is far from the importer's/exporter's base location; for example, the importer is in one location and the goods are imported through a port at a distant location
8	Shipment of goods inconsistent with normal geographic trade
9	Repeated importation and exportation of same high-value commodity
10	The origin of goods/shipment are not in line with the normal import/export of goods associated with the countries involved
11	Transaction structure and/or shipment terms appear unnecessarily complex or unusual and designed to obscure the true nature of the transaction
12	Shipment locations or description of goods not consistent with LC

13	Shipping something other than what is invoiced; for example, shipping more or less goods than invoiced
14	Phantom shipping, i.e. shipping nothing at all with false invoices and fraudulent transport documents
15	Goods not supplied within reasonable timeframe
16	HS code differs from international identification system for goods
17	Complex shipment terms are used to conceal the true nature of the transaction
18	Shipments of commodities are routed through a number of jurisdictions without economic or commercial justification

Table 10 – Red Flags and Risk Indicators Related to Goods Traded

No.	Risk Indicators
1	Customers transacting in activities/goods that potentially involve a high risk of money laundering and other financial crimes, including activities/goods that may be subject to export/import restrictions
2	The unit price of items is abnormally higher/lower than the market price
3	The quantity of the good is over- or under- declared
4	False reporting, such as commodity misclassification
5	Transaction involves obvious dual use goods
6	Underlying goods involved in the trade transaction are of sensitive nature (i.e. sensitive goods)
7	Transactions related to acquisition or sale of intangibles like specialised software, etc.
8	Packing inconsistent with the commodity or shipping method

Table 11 – Red Flags and Risk Indicators Related to the Payment

No.	Risk Indicators
1	Funds received but goods not exported (advance for exports, mainly used with open account basis)
2	Funds sent out but goods not imported (advance for imports)
3	Advance for supply of goods is a major part / percentage of the total value of goods
4	Amount of advance is not in line with normal international trade for the kind of goods
5	Payments/fund transfers made through economic/exchange centres even when account is held with Financial Institutions
6	Non-resident's payments to companies/natural persons who have accounts with offshore Bank
7	Import payments being made against old bills after lapse of considerable period of time from import of goods, without appropriate justification and documentation
8	Importer of goods not from the same country from where wire (payment for import) originated

Table 12 – Red Flags and Risk Indicators Related to the Structure of the Trade Entity

No.	Risk Indicators
1	A trade entity is registered at an address that is likely to be a mass registration address, especially when there is not reference to a specific unit (e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes)
2	The business activity of a trade entity does not appear to be appropriate for the stated address; for example, a trade entity appears to use residential properties, without having a commercial or industrial space and with no reasonable explanation
3	A trade entity lacks an online presence or the online presence suggests business activity inconsistent with the stated line of business
4	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)
5	Owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners (ultimate beneficial owner)
6	A trade entity, or its owners or senior managers, appear in negative news (e.g. past money laundering schemes, fraud, tax evasion, etc.)

7	A trade entity maintains a minimal number of working staff that is inconsistent with its volume of traded commodities
8	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
9	Unexplained periods of dormancy for the trade entity
10	An entity is not compliant with regular business obligations, such as filing VAT returns

Table 13 – Red Flags and Risk Indicators Related to the Counter Party

No.	Risk Indicators
1	Assignment of proceeds issued to a party not in line of business of the beneficiary relevant where the assignee is not a bank (for both LCs and LGs)
2	Trade transactions where multiple parties are involved in the LC besides the principal parties, such as applicant and beneficiary
3	A trade transaction involves multiple countries in the sourcing and movement of goods
4	Transferable credit allowing transfer between the same parties or belonging to the same group
5	Transacting parties appear to be affiliated
6	Transacting parties conduct business out of a residential address
7	Transacting parties only provide a registered agent's address
8	Customer requests payment of proceeds to an unrelated third party
9	Transactions involving third parties which may not be contract parties (consignee and remitter are different)
10	Related party transactions including transfer pricing
11	Possible indication of back to back LCs
12	Transaction not in-line with normal international trade for the given kind of goods & parties involved
13	Front or shell companies appear to be used for the purpose of hiding the true parties involved
14	A trade entity engages in complex trade deals involving numerous third-party intermediaries in incongruent lines of business

Table 14 – Red Flags and Risk Indicators Related to Account and Transaction Activity

No.	Risk Indicators
1	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
2	An account displays frequent deposits which are subsequently transferred to persons or entities in free trade zones or offshore jurisdictions without a business relationship to the account holder
3	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
4	Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reason
5	Cash deposits or other transactions of a trade entity are consistently just below relevant reporting thresholds
6	Transaction activity associated with a trade entity increases in volume quickly and significantly, and then goes dormant after a short period of time
7	Payments are sent or received in large round amounts for trade in sectors where this is deemed as unusual
8	Payments are routed in a circle, i.e. funds are sent out from one country and received back in the same country, after passing through another country or countries
9	Transaction involves boycott clauses (ABCO language)
10	Transaction involves deleting of sanctions clause under trade finance terms and condition

Table 15 – Red Flags and Risk Indicators Related to Trade Activity

No.	Risk Indicators
1	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 the purchase price)
2	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)
3	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)

Appendix V: Trade Finance Check Lists

Table 16 – Check List for Letter of Credit Issuance

No.	Item
1	Does the LC cover movement of goods but fails to call for presentation of transport? (e.g. LC documents cover steel shipment but allows a forwarder's cargo receipt)
2	Does the account party, beneficiary, or any of the involved banks fit one of the blocking profiles or are they list under international or national blacklists?
3	Has the compliance screening been performed?
4	Is the underlying trade transaction prohibited?
5	Does the LC include a condition for a switch B/L? (e.g. allowing cargo to be switched on the open sea)
6	Does the trade product financing have unusual (overvalued or undervalued) pricing suggestive of invoice manipulation?
7	Does the LC not provide description of goods/services being furnished?
8	Does the certificate of origin show goods originating from a sanctioned and/or high-risk country?
9	Does the LC application request shipment/transshipment to or from a sanctioned country?
10	Does the transaction include high-risk products or high-risk business?
11	Does the transaction cover the shipment of dual-use and/or sensitive goods?
12	Does the LC include a condition for a letter of indemnity (LOI) – high seas sale?
13	Does the LC contain "available with any bank" condition? Or "accepted as presented" condition?
14	Does the LC contain any boycott clauses?
15	Are the parties involved in trade transaction part of an identifiable group, network, or family?
16	Are the parties involved reputable? Have they been engaged in previous verifiable business?
17	Is there any law enforcement, financial intelligence, internal, or publicly available derogatory information on any of the parties involved?
18	Are the goods imported commonly imported from sanctioned countries?

-
- 19 Does the B/L indicate that goods will be shipped by a blocked shipping company or aboard a blocked vessel appearing on the SDN list?
-
- 20 Does the LC allow presentation of stale documents?
-

Table 17 – Check List to Evaluate Shipments for Suspicious Activity

No.	Item
1	What are the items being shipped? Where are they manufactured or produced?
2	What is the shipment route (port of loading and ultimate destination)? Is the routing logical? Is the origin and destination logical or suspect?
3	Do any of the shipping documents contain unusual codes, markings or stamps appearing on monetary instruments such as drafts or bills of exchange (e.g. country codes such as SY, SD, IR, IRISL, RU)? where SY refers to Syria, SD refers to Sudan, IR refers to Iran, RU refers to Russia, for the abbreviation IRISL it could be referred to shipping lines for the Islamic Republic of Iran
4	Do any of the provided phone numbers have country codes for sanctioned countries?
5	Is the provided HS code for the goods accurate?
6	Was one of the containers utilised in the shipment related to Iran Container Suffixes? Or subsidiaries to IRISL shipping lines?
7	Is the container check digit valid?
8	Does the B/L describe containerised cargo but without container numbers or with sequential numbers or non-standard numbers?
9	Were there many discrepancies found under transport documents?
10	Who is the shipper, broker, and/or freight forwarder? What is their relationship(s) to the buyer/seller?
11	Does the content and cost of the shipment (shipment or freight charge) match the description in the accompanying documents?
12	Is the price of the goods in question standard market value? (There will be many variables involved in determining price.)
13	Are the size, weight, and packaging consistent with the contents?
14	What kind of payment is involved (e.g. cash, advance payment, LC, direct wire transfer, etc.)?
15	Is this a regularly scheduled shipment of goods? Does it match the business of the parties involved with the transaction?

-
- 16 Does the B/L indicate that the goods will be shipped by a blocked shipping company or aboard a blocked vessel appearing on the SDN list?
-
- 17 Do the transport documents showed the name of the intended vessel?
-
- 18 Do the transport documents show a future B/L date?
-
- 19 Do LC indicate a geographical area of ports of Loading/Discharge such as European Port/ Black sea Ports/ Caspian Sea/ Persian Gulf?
-

The following information and recommendations were taken from the Global Compliance Institute's Certified Compliance Manager Manual.

When reviewing trade documentation, trade operations employees, MLRO's and sanctions specialists need to be aware of a considerable amount of information, such as the consignee, consignor, and vessel name, among others.

Some of the above information will not be available on the SWIFT message, therefore it is recommended to add a "Sanctions Clause" to the letter of credit in the body of the (SWIFT) stating that payment will not be made if the other party becomes listed on a sanctions list (mainly the UN List) at the due date of payment and, that the relevant sanctions regulations will apply if any of the parties are affected.

In addition, when the applicant bank receives the bill of lading (B/L), the vessel name and its flag beside the shipping company name should be examined. In B/L, the vessel name is not mentioned; instead, you will find the vessel IMO number.¹⁶⁷ Through using the public domain (Internet), you can easily find information about the vessel. Tailored solutions for sanctions monitoring purposes can provide a set of data that helps the compliance manager, or the sanctions specialist, investigate the validity and the sanctions risk of the transaction. The following lists includes important information to collect and what that information should be screened.¹⁶⁸

Table 18 – Check List for Trade Transport documents in relation to Vessel and Ownership information

No.	Item
1	<p>Vessel Name: What is the vessel name? How many times has the vessel name been changed? If applicable, what were the previous names of the vessel?</p> <p>Vessels under sanctions or managed by a sanctioned country will try continuously to change their names.</p>
2	<p>Vessel Flag: What is the current flag? What were the previous flags, and how many times has it been changed?</p> <p>Vessels under sanctions (or managed by a sanctioned country), will attempt to continuously change their flag.</p>

¹⁶⁷The International Maritime Organization (IMO) number is a unique identifier for ships and for registered ship management companies. For ships, it consists of the three letters "IMO" followed by the seven-digit number.

¹⁶⁸Global Compliance Institute, "Certified Compliance Manager Manual" (Spring Hill, Australia: Global Compliance Institute, 2020), 346–49, <https://www.gci-ccm.org/node/4>.

Vessel Picture and Class: Vessel picture and class help determine what the vessel is used for.

3 Compliance managers and sanctions specialists should ensure that the type of vessel is consistent with the commercial transaction that they are investigating. Checking this data can lead to the discovery of forged or incorrect B/Ls. For example, if the commercial transaction is related to livestock transportation but the vessel class is “container ship”, then this indicates that there is something wrong.

4 **Vessel location and route:** Both the origin and destination locations of the voyage, plus the estimated time of arrival (ETA), should be checked.

5 **Ports and Passage:** This gives an indication of the ports visited by the vessel in the past (e.g. 6 months) and how long it spent there.

This can give a good indication whether a vessel is visiting sanctioned countries, and if it is, then you will need to investigate the transactions further.

6 **Sanctions Violations:** Information on whether the vessel is under sanctions or owned by a sanctions target. Also, if it has been connected with any sanctions violations.

7 **Ownership Information:** Information about the registered owners, commercial operator, beneficial owners and how many times the names of the owners have been changed.

8 **Vessel Status Information:** Information on whether the vessel is operational/in service/ in commission or has been decommissioned (reached the end of its usable life) or is lost or scrapped.

Appendix VI. Proliferation Financing Indicators

FATF's 2018 Guidance on Counter Proliferation Financing included the following two lists of possible indicators (noting that they were “not uniquely determinative of proliferation financing, and proliferation financing activities may share similar traits with money laundering (especially trade-based money laundering) and terrorist financing activities”).¹⁶⁹

List 1 – Indicators of possible proliferation financing from the 2008 FATF Proliferation Financing Report:

- Transaction involves person or entity in foreign country of proliferation concern
- Transaction involves person or entity in foreign country of diversion concern
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of “denied persons” or has a history of export control contraventions
- Customer activity does not match business profile, or end-user information does not match end-user’s business profile
- A freight forwarding firm is listed as the product’s final destination
- Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry)

¹⁶⁹Financial Action Task Force, FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (Paris: Financial Action Task Force, 2018), 32–34, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf>.

- Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators)
- Transaction demonstrates links between representatives of companies exchanging goods (i.e. same owners or management)
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws
- Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?)
- Transaction involves Financial Institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried
- New customer requests letter of credit transaction awaiting approval of new account
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

List 2 – Additional potential indicators of sanctions evasion activity mentioned in third-party reports (e.g. UN Panel of Experts’ Reports, academic research)

- Involvement of items controlled under WMD export control regimes or national control regimes
- Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background
- Use of cash or precious metals (e.g. gold) in transactions for industrial items
- Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business
- Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business
- Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions
- Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated)
- Involvement of a university in a country of proliferation concern
- Description of goods on trade or financial documentation is nonspecific, innocuous or misleading
- Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent
- Use of personal account to purchase industrial items.

Appendix VII. Indicators of Laundering the Proceeds for Illegal Wildlife Trade

FATF June 2020 “Money Laundering and the Illegal Wildlife Trade” report included the following lists of possible indicators related to trade activity client profiles (individuals and corporates) and trade activity client profiles (transactions and client account activity)¹⁷⁰.

List 1 – Red Flags and Risk Indicators Related to Trade Activity Client profiles (individuals and corporates)

- Involvement of international trade companies, including import-export, freight forwarding, customs clearance, logistics, or similar types of companies operating in the following commodities long high-risk corridors or ports⁸² for IWT supply and demand: raw or squared wooden logs, plastic waste or pellets, frozen food, fish maws, various kinds of beans, stone or quartz blocks.
- Use of common containers, consignees, transporter, clearing agents, or exporters as seen in other cases believed to involve IWT.
- Activity involving PEPs and wealthy businessmen/women, particularly those with environmental, game, or forestry oversight or environmental or wildlife related businesses.
- Involvement of legal wildlife-related entities such as private zoos, breeders, (exotic) pet stores, safari companies, pharmaceutical companies making medicines containing wildlife and wildlife collectors or reserves.
- Individual or beneficial owner(s) of a corporate domiciled in jurisdiction that is a prominent transit or demand country for illegal wildlife.

List 2 – Red Flags and Risk Indicators Related to Trade Activity Client profiles (Transactions and client account activity)

- Large cash deposit by government officials working in wildlife protection agencies, border control or customs and revenue officials.
- Large cash or other deposits, wire transfers, multiple cash deposits and withdrawals, and/or unexplained wealth from government officials working in forestry agencies, wildlife management authorities, zoo and wildlife park employees, or CITES Management Authorities (CMAs).
- Large cash or other deposits, multiple cash deposits and withdrawals, and/or unexplained wealth from government officials from environment or other ministries who have specific management or oversight authority of government stockpiles of seized ivory, rhino horn, timber, or other illegal wildlife products.
- Shipments of legal wildlife (fauna and flora) with anomalous, incomplete, or otherwise suspicious CITES certificates.
- Transactions using names of ingredients or products in the traditional medical trade that refer to CITES species.
- Illogical or anomalous loans between trading or import/export companies in key IWT source or transit countries.
- Switched bills of lading by traders previously implicated in criminal activity involving wildlife trafficking or trade fraud investigations or prosecutions.
- Transactions having discrepancies between the description or value, of the commodity in customs and shipping documents and invoice, relative to the actual goods shipped or quoted price or the actual value in payments made.

¹⁷⁰FATF June 2020 “Money Laundering and the Illegal Wildlife Trade” – pages (60-62).

- Illogical or anomalous purchases, payments, or other transactions related to gold trading from business accounts of clients. Payments for wildlife shipping are often masked as payment for gold or to gold trading business.
- Escrow-type transactions from/to accounts and companies with same beneficial owner in particular for payment of cross-border and transcontinental shipments.
- Transactions from known traffickers to individuals who then pay for couriers or packages via the post.
- Transactions for hired vehicles and domestic accommodation from known members of a trafficking syndicate who are not present in the country or region within a country.
- Third-party wire transfers/cash deposits to, or withdrawals by, known wildlife poachers and traffickers.
- Transactions between licenced pet shop suppliers/breeders and known wildlife poachers and traffickers.
- Transactions to licenced pet shop suppliers/breeders that originate from Overseas, and/or incommensurate with stated business activities.

TBFC Project Team, GCFFC MENA Chapter



Nishanth Nottath
Project Lead
Executive Vice President –
Head AML, ABC and RegTech,
Mashreq Bank



Channing Mavrellis
Lead Editor
Illicit Trade Director,
Global Financial Integrity



Graham Baldock
Author
Chief Compliance Officer/
MLRO, Anglo-Gulf Trade Bank



Amjad Batayneh
Author
Special Investigations Unit
Manager, Group Regulatory
Compliance, Arab Bank



Jonathan Brewer
Author
Visiting Professor, King's
College, London



Fahad Haque
Author
Regional Head of Sanctions -
MENAT, HSBC

Title: Trade Based Financial Crime - Middle East and North Africa: A reference guide for the anti-financial crime community

Compiled by: TBFC Project Team, GCFFC MENA Chapter



secretariat@gcffc.org



info@menafccg.com



www.gcffc.org

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, synched audio, hyperlinks, or otherwise without prior permission of GCFFC MENA Chapter.

Disclaimer: Whilst every effort has been taken by GCFFC MENA Chapter to avoid errors or omissions in this document, any mistake or omission is not intended. The information contained in this document is only for reference / educational / awareness purposes and liable to change without notice. It should be noted that GCFFC MENA Chapter or its parent organisation, GCFFC Global or any affiliates thereof, will not be responsible for any damage or loss, or any other consequences whatsoever, that may result from activities undertaken based on the information provided in this document.

Cover image: Pawel Czerwinski, Unsplash licence

Languages: English and Arabic

Number of pages: 112

Edition: 1st edition

Month and year of publication: October 2022

Supporting Organisations:

التصميمي و مشاركون
AL TAMIMI & CO.



Design and type-setting:



Shriya Sanjeev
shriyasanjeev@hotmail.com

Design sponsored by:



Arabic translation sponsored by:



This document is not for sale. This document shall be distributed by GCFFC MENA Chapter or MENA FCCG or their affiliates to individuals and entities as they deem fit.



Attribution-NonCommercial-
NoDerivatives 4.0 International
(CC BY-NC-ND 4.0)



**GLOBAL COALITION
TO FIGHT
FINANCIAL CRIME**



MENA FCCG
Making a Collective Impact

www.gcffc.org • www.menafccg.com