



# Economic Sanctions following Russia's Military Aggression against Ukraine: Typologies and case studies

*Niki Charilaou*

*Manager Financial Crime & Sanctions Compliance Department*

October-November 2023

# 1. Sanctions - General

Sanctions are a tool used by governments / intergovernmental organizations (UN, EU) to exert their foreign policy in a non-forceful way to punish, deter or prevent a nation's behavior.

Sanctions can target geography or activities.

- Geographic sanctions target specific countries or regions.
- Sanctions targeting activities concentrate on international criminals and can be imposed to influence actions that lead to a reduction of money laundering, terrorist financing, and the trafficking of illegal goods by reducing the flow of funds.

In general, sanctions are imposed to prevent terrorism, arms proliferation, human rights violations, deliberate destabilisation of a sovereign country, annexation of territories, or cyber-attacks.

# 1. Sanctions - Types

There are different types of sanctions as follows:

- **Diplomatic Sanctions:** Measures such as cutting off diplomatic relations with a targeted country or the coordinated recall of diplomatic representatives.
- In the narrower sense:
  - **Arms embargo**
  - **Travel Bans:** targeted persons cannot enter the EU (for example)
  - **Asset freezes** of targeted persons or entities: all their assets in the EU (for example) are frozen, while EU person and entities cannot allocate funds to those targeted.
  - **Economic Sanctions** or restrictions which relate to specific sectors of economic activity, such as export / import prohibitions, prohibitions of investments, prohibitions in the provision of services, etc

# Most sanctioned countries





# U.S. Primary vs Secondary Sanctions

- Primary Sanctions: Activities within OFAC's jurisdiction:
  - Activities by a US person or by a person in the USA.
  - Activities involving the US financial system (including the clearing of US dollars through US intermediary Banks.)
- Secondary Sanctions: Activities outside OFAC's jurisdiction:
  - The USA seeks to persuade those outside its jurisdiction to act in accordance with US foreign policy objectives.
  - In this respect, it may impose sanctions measures against foreign individuals / entities, even where there is no US jurisdiction.
  - Secondary sanctions do not apply to all OFAC sanctions regimes.
  - Secondary Sanctions may include designations of foreign individuals / entities or prohibiting correspondent and other accounts with US banks, as a penalty for providing support / facilitating transactions with SDNs.

SDN= Specially Designated National

# U.S. Primary vs Secondary Sanctions

PRIMARY SANCTIONS (any jurisdiction)		SECONDARY SANCTIONS (currently – US ONLY)
>> <u>jurisdictional</u> nexus (US, EU, UK, etc.) 		>> jurisdictional nexus 
<p>A) Direct breach of sanctions by DOMESTIC persons</p> <p><b>Example:</b> The US Treasury's OFAC orders New York-headquartered XYZ Corp to pay a \$10mn penalty for having contracted with the Government of Venezuela.</p>	<p>C) Facilitation of sanctions evasion/ circumvention by FOREIGN persons</p> <p><b>Example:</b> The EU Council lists Individual A, a Chinese national resident in Shanghai, for facilitation of export control violations involving EU-origin controlled items for the benefit of the Russian military.</p>	<p>E) Provision of material support by FOREIGN persons</p> <p><b>Example:</b> OFAC designates Individual B, a Cypriot national resident in the UK, for having provided material support outside of the US to a Belarusian SDN.</p>
<p>B) Sanctions evasion/ circumvention by DOMESTIC persons</p> <p><b>Example:</b> Canada's OSFI finds Toronto-headquartered Bank ABC guilty of secretly funneling funds to several designated persons in Myanmar in a complex lending arrangement. Bank ABC is subject to civil and/or criminal domestic enforcement.</p>	<p>D) Direct listing of a DOMESTIC or FOREIGN person</p> <p><b>Example 1:</b> The UK Treasury's OFSI lists UK-registered ABC Limited as being controlled by a sanctioned Iranian official. It is subject to an asset freeze.</p> <p><b>Example 2:</b> The EU Council lists ABC SA for its role in Russia's invasion of Ukraine. It is subject to an EU-wide asset freeze.</p>	<p>F) Significant transactions involving FOREIGN persons</p> <p><b>Example:</b> OFAC designates Malaysian-based XYZ Bhd for having deceptively facilitated a significant transaction in EUR for the benefit of a 60%-owned subsidiary of a Russian oil company (subject to US sectoral sanctions).</p>

# War in Ukraine – Sanctions by the EU

Since March 2014, the EU has gradually imposed restrictive measures against Russia in response to:

- ❑ The illegal annexation of Crimea
- ❑ Russia's aggressive war against Ukraine
- ❑ The illegal annexation of Donetsk, Luhansk, Zaporizhia and Kherson

The measures are intended to weaken Russia's economy, depriving it of vital technologies and markets and limiting its ability to wage war.

The EU has also imposed sanctions against:

- Belarus, in response to its involvement in the invasion of Ukraine
- Iran, in response to the supply to Russia of unmanned aerial vehicles (drones)

# War in Ukraine – EU Sanctions

The first sanctions relating to Ukraine were imposed in 2014 and have been amended and strengthened since Russia stepped up its attack on Ukraine, with a first package of sanctions in February 2022.

The EU has imposed several types of sanctions:

- Diplomatic measures
- Asset freezes and travel restrictions
- Restrictions on economic activity in Crimea and Sevastopol, and in the non-government-controlled regions of Donetsk, Luhansk, Kherson, and Zaporizhia.
- Economic sanctions (export / import prohibitions, prohibitions in the provision of services, etc)
- Media restrictions

Since the outbreak of the Ukraine war, 11 packages of sanctions have been issued to date.



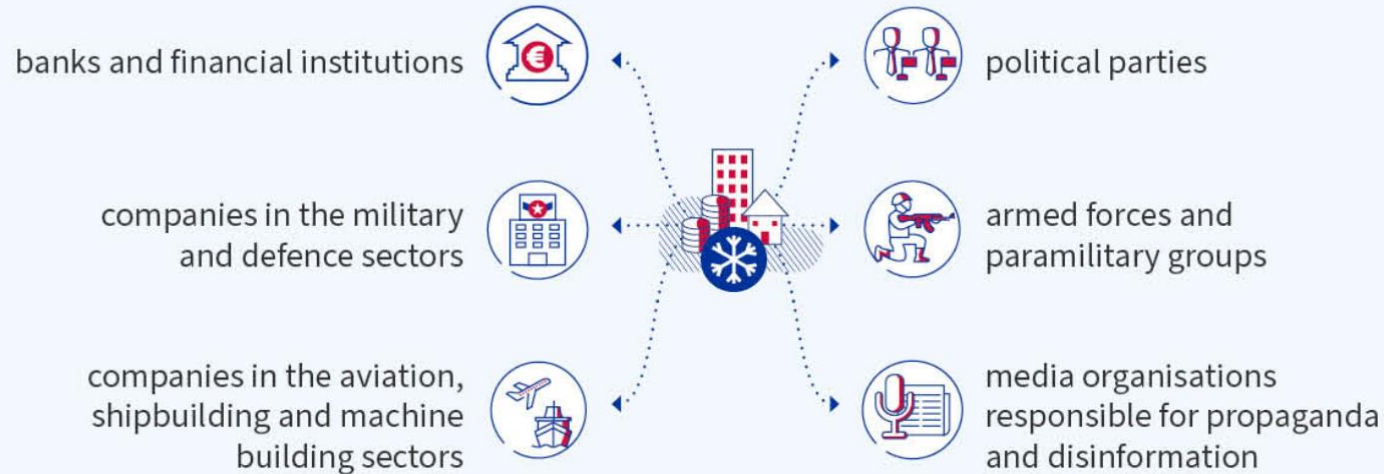
# EU Sanctions – Asset Freeze / Travel Bans against individuals & entities

## → Assets freeze / travel ban against



# EU Sanctions – Asset Freeze / Travel Banks against individuals & entities

## → Assets freeze against



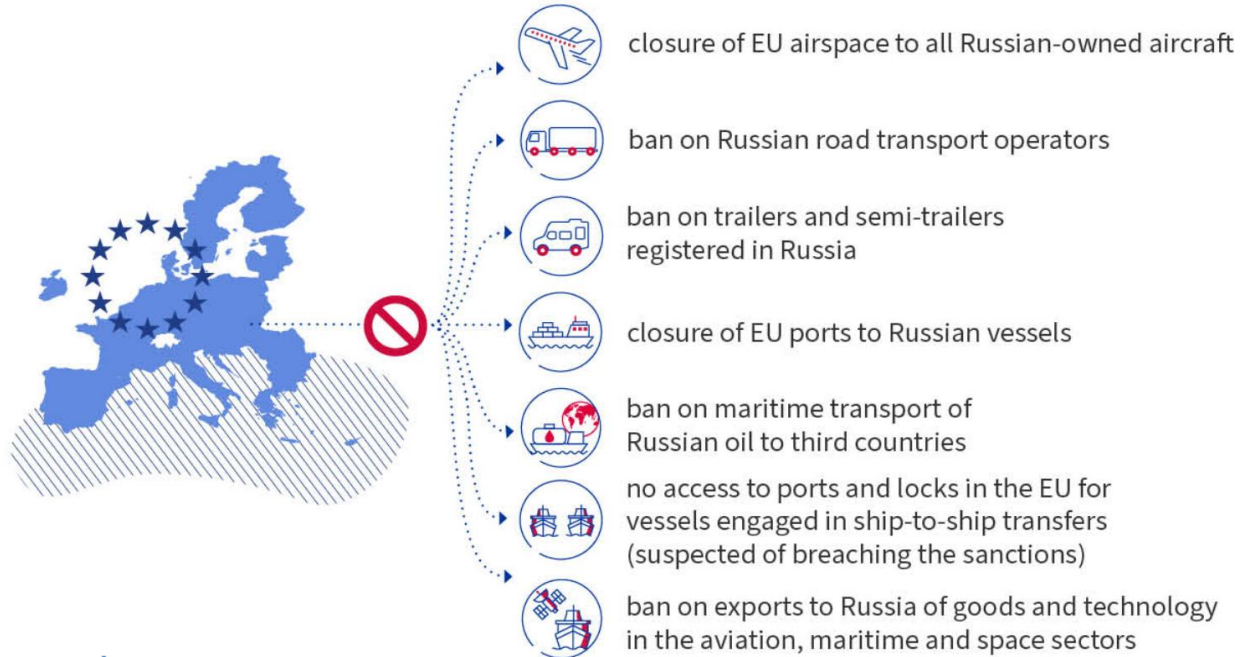
# EU Sanctions – Economic Sanctions

## → Finance



# EU Sanctions – Economic Sanctions

## → Transport



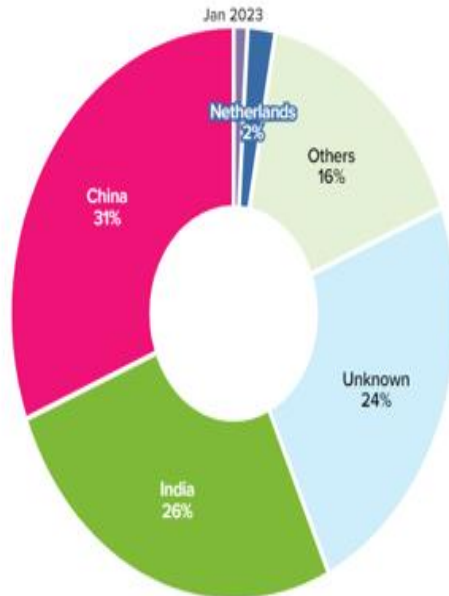
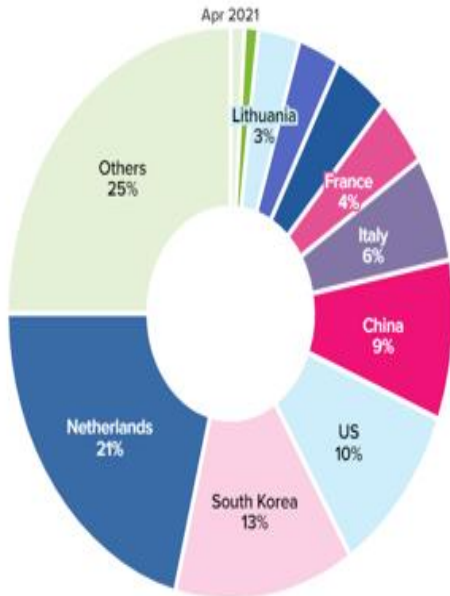
# EU Sanctions – Economic Sanctions

## → Energy



# EU Sanctions - Energy

Russian crude oil condensate exports



- Since the invasion of Ukraine began, Russia's oil exports have become less diversified and more dependent on India and China. In 2021,
- Europe was the primary destination for Russian oil exports.
- In 2023, India and China together will now account for 57% of Russian oil exports, making Russia vulnerable to fluctuations in demand in the two markets. Russia now has less bargaining power, as the oil price cap gives buyers more leverage to negotiate prices below the cap. In addition, the cost of transporting oil to many more destinations further erodes Russian margin.

Source: TankerTracker.com, Ellen Wald, PhD

# EU Sanctions – Economic Sanctions

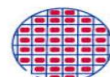
## → Defence



Ban on exports to Russia of:



dual-use goods and technology for military use



semiconductor materials  
electronic and optical components



navigational instruments



drone engines



arms and civilian firearms and their parts



ammunition, military vehicles and  
paramilitary equipment



other goods which could enhance  
Russian industrial capacities

# EU Sanctions – Economic Sanctions

## → Raw materials and other goods

Ban on exports to Russia of:



luxury goods



Ban on imports from Russia of:



steel, iron, cement and asphalt



wood, paper, synthetic  
rubber and plastics



seafood, spirits, cigarettes  
and cosmetics



gold, including jewellery



# EU Sanctions – Economic Sanctions

## → Services



Ban to provide to Russia or Russian persons:



architectural and engineering services



Audit and accounting services

IT consultancy and legal advisory services



advertising, market research and  
public opinion polling services



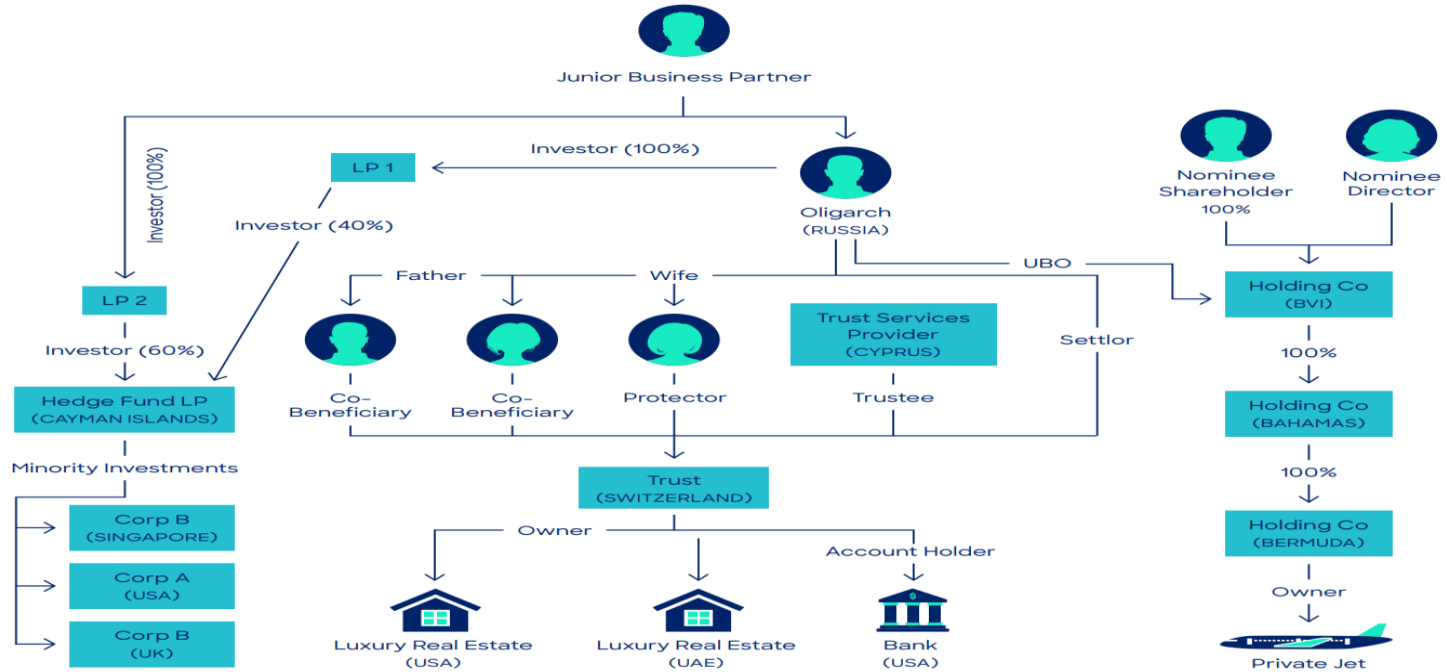
intellectual property rights of trade  
secrets (related to goods and technology  
covered by other sanctions)

# EU Sanctions – Sanction against Belarus



# Sanctions Evasion – Typologies

## Financial Sanctions Evasion by Oligarchs, Other Elites and Proxies\*



\* This is a fictional example. The jurisdictions mentioned in the above graph have been previously identified by western regulatory agencies as having been involved in fund and asset transfers on behalf and for the benefit of Russia's political and economic elites.



# FinCEN

# ALERT

FIN-2022-Alert001

March 7, 2022

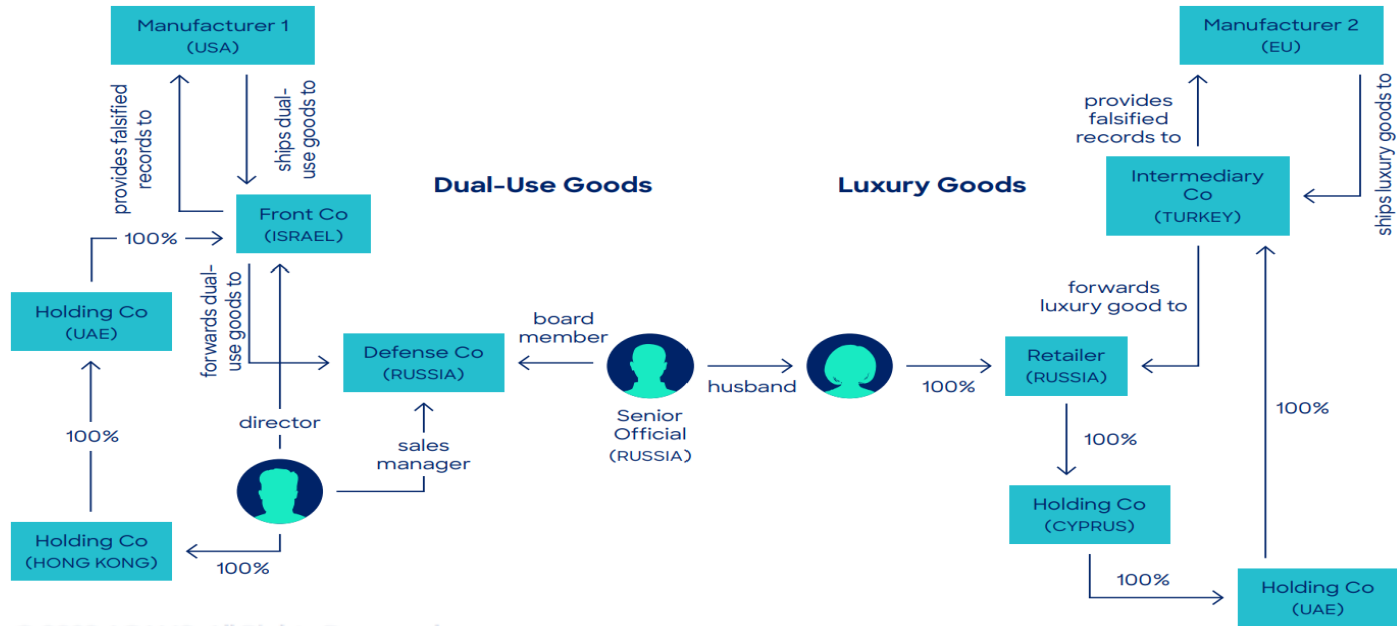
## FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts

### Select Red Flag Indicators<sup>16</sup>

- 1** Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.
- 2** Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- 3** Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.<sup>17</sup>
- 4** Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale.
- 5** Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.
- 6** Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

# Sanctions Evasion - Typologies

## Procurement of Defense Items, Dual-Use Goods and Sensitive Technologies as well as Embargoed Luxury Goods\*



© 2023 ACAMS. All Rights Reserved.

# Sanctions Evasion – Through Central Asia Companies

<https://www.rferl.org/a/central-asia-companies-russia-sanctions/32469313.html>





# Financial Trend Analysis

## Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls

September 2023

### *Suspicious Transactions Indicate Key U.S.-Origin Goods Supplied Directly and Via Transshipment Points to Russian End-Users*

Companies in intermediary countries also appear to be purchasing U.S.-origin goods on behalf of Russian end-users. These companies were mainly located in China and Hong Kong, but also in Belgium, Germany, Singapore, Turkey, the United Arab Emirates (UAE), the United Kingdom (UK), and other countries where transshipment may be occurring and payments for goods may be originating.<sup>10</sup>



# Financial Trend Analysis

## Trends in Bank Secrecy Act Data: Suspected Evasion of Russian Export Controls

September 2023

Figure 1. Top 10 Subject Countries in Suspected Export Control Evasion-Related BSA Reports<sup>11</sup>

Subject Address, By Country	Count of Subject References
United States	976
Russia	322
China	130
Hong Kong	126
Turkey	49
UAE	43
United Kingdom	33
Canada	30
Singapore	30
Cyprus	17



# Sanctions Evasion – Red Flags in Real Cases



1

## Product

Is the product at high risk of diversion because of:

- its potential end use by the Russian military or in another sanctioned sector?
- Its previous use in Russian munitions or military systems?

2

## Customer

- Is the entity found on a sanctions list?
- Does the entity have a history of shipping to Russia, even if the exported item is allegedly going to a non-sanctioned destination?
- Does the entity have any connection with the Russian military or the Russian State?
- Has the entity recently changed or reincorporated?
- Has the entity recently purchased vessels for no obvious purpose?

3

## Network

- Does the entity involved have a connection to a sanctioned entity?
- Do all entities involved have a web presence?
- Is any entity using a personal email?
- Are there common items (e.g. addresses) linking to sanctioned entities?
- Does the transaction involve offshore law firms?

# Sanctions Evasion – Red Flags in Real Cases



4

## Destination

- Is the item delivered to a common transshipment point?
- Is the Bank or freight forwarding company listed as the item's final destination?

5

## Transaction

- Does the entity prefer to pay cash?
- Does the entity attempt last minute changes to shipping instructions?
- Has the invoice or other document been altered to obscure the ultimate customer?
- Is payment coming from a 3<sup>rd</sup> party country or business?
- Does the undervalue the purchase on shipping documentation?

6

## End Use

- Does the end use match historical patterns of evasion?
- Is the client reluctant to answer questions about the end use?
- Is the item incompatible with the stated end use?
- Is the item more sophisticated than needed for the stated end use?



# Sanctions Evasion – Red Flags in Real Cases



**Case 2:** In October 2022, Estonian national Andrey Shevlyakov was indicted for illicitly procuring U.S.-origin microelectronics and high-tech products on behalf of the Russian government and military via a series of Estonian shell companies.<sup>58</sup> Shevlyakov also attempted to acquire computer hacking software (Metasploit Pro) for a Russian client, and organized frequent smuggling trips across the Estonian-Russian border to deliver goods.

**Case 4:** In March 2023, American nationals Cyril Gregory Buyanovsky and Douglas Robertson were indicted for exporting avionics equipment to Russian buyers through Buyanovsky's company, Kanrus Trading Inc.<sup>61</sup> Both men concealed the transactions by falsifying the true end users, value, and destinations of the goods, and by transshipping them through other countries.





Bank of Cyprus



Thank you

# Anti-Money Laundering & Combating the Financing of Terrorism – Theoretical and Practical Considerations for Compliance

PRESENTED BY HAIG ASSADOURIAN

24 & 26 OCTOBER 2023

7 & 8 NOVEMBER 2023

**What is expected of us and what if we don't comply?**

**How do we comply?**

**Compliance Culture**

**Common findings from Regulator review visits**

# Haig Assadourian - Profile

- ❑ Involved in the Financial Services Sector from 2001
- ❑ Over 22 years' experience in AML/CFT compliance
- ❑ Formerly Board Member of ASP regulated by CySEC
- ❑ Co-Founder of Aequus Business Consulting
- ❑ Qualifications: BA(Hons) Economics, ACAMS, CySEC AML, CySEC Advanced, ACSI, Certified Data Protection Practitioner
- ❑ ACAMS Certified Cryptoasset Anti-Financial Crime Specialist (in process)

## Contact Details:

Email: [haig@aequus.cy](mailto:haig@aequus.cy)

# WHAT IS EXPECTED OF US AND WHAT IF WE DON'T COMPLY?



# Legal Framework - EU

- The Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('The 4th EU Directive') <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN>
- The Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('The 5th EU Directive') <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>
- The Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN>



# Legal Framework - Cyprus

- ❑ The Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2021 (“The Law”)
- ❑ The Law Regulating Companies Providing Administrative Services and Related Matters (“The Fiduciaries Law”)
- ❑ The Combating of Terrorism Law of 2019 L75(I)/2019
- ❑ Internal Guidelines and Directives issued by CySEC, ICPAC and CBA



# Why is Compliance so Important?

- ✓ Avoid risk of facilitating/assisting criminal activity, terrorist financing, and/or sanctions circumvention
- ✓ Protect yourself (job, reputation, qualifications)
- ✓ Protect your firm
- ✓ Protect other clients



# “But I Know all my Clients.....”

“.....why do we need all this extra work and inconvenience?”



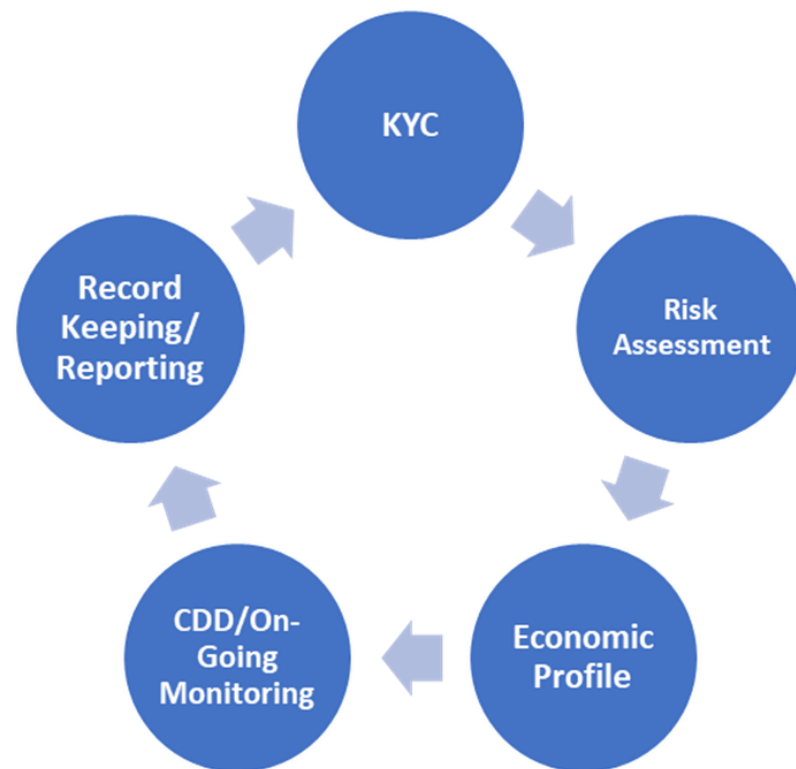
# What is Expected of Us?

- ✓ Identify clients & other stakeholders/counterparties
- ✓ Understand business activities
- ✓ Identify, assess, manage/mitigate risks
- ✓ Ongoing monitoring
- ✓ Proper record keeping & reporting



# In Other Words.....

- KYC – Client & counterparty/stakeholder identification
- Risk Assessment
- Economic Profile
- CDD/Ongoing monitoring
- Proper record keeping & reporting



# What Should we be Looking for?

- ✓ Money Laundering
- ✓ Terrorist Financing
- ✓ Sanctions Circumvention
- ✓ Proliferation Financing



# What is Money Laundering (ML)

Money laundering is the process of concealing the origin of money, often obtained from illicit activities such as drug trafficking, corruption, embezzlement or gambling, by converting it into a legitimate source

A “predicate offence” is an offence whose proceeds may become the subject of money-laundering offences, e.g. narco trafficking, tax evasion, murder and grievous bodily harm, corruption, fraud, smuggling, human trafficking, illegal wildlife trafficking, forgery





# What is Terrorist Financing (TF)

“Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources.”  
(International Monetary Fund website)

Money Laundering and Terrorist Financing are two separate crimes, though they sometimes use similar methods:

- ❑ Both need to disguise links to origin of funds
- ❑ Both target countries or service providers with non-existent, insufficient or weak AML/CFT controls and regulations



# Sanctions

Sanctions that apply in Cyprus by law are:

- EU Council Decisions and Regulations (“Restrictive Measures”)
- UN Security Council Resolutions or Decisions (“Sanctions”)

However, due to the power of the USA to black-list and block the use of USD\$ by individuals, companies and financial institutions, obliged entities are strongly advised to also take into consideration US Economic and Trade Sanctions imposed by **The Office of Foreign Assets Control (OFAC)**



# Sanctions – continued

- Sanctions imposed to:
  - Preserve peace & international security
  - Increase cooperation and safeguard common values and security
  - Protect human rights, democracy and the rule of law
- They target:
  - Governments
  - Companies
  - Groups/organisations (e.g. terrorist groups)
  - Individuals
- In addition to AML policies & procedures, obliged entities must implement and document policies & procedures to identify actions that are in breach, or potentially in breach of Sanctions



# Sanctions – continued

**Sanctions Avoidance Facilitation =**



# Sanctions – continued

19 April 2023 – Cyprus Government announced the establishment of a National Sanctions Implementation Unit.

Will cooperate with the respective department in the UK and will have technocratic support from its British counterpart.

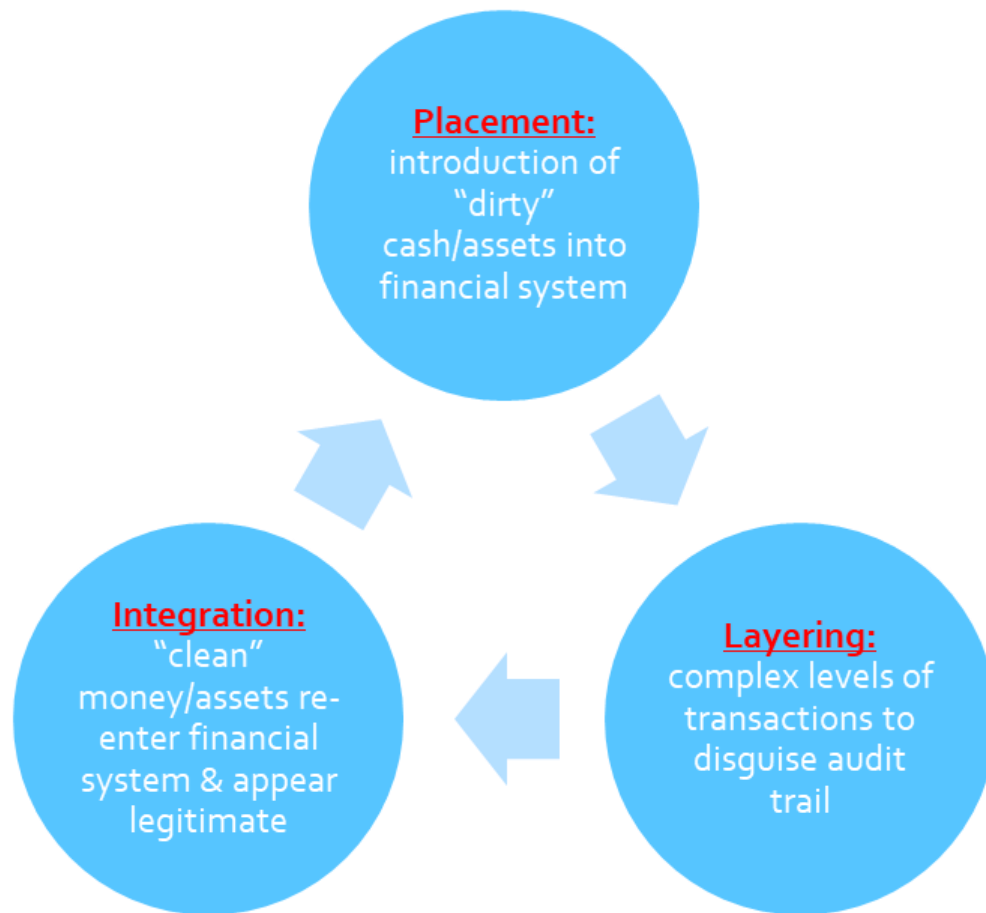
# Stages of ML

**Stage 1 – Placement**

**Stage 2 – Layering**

**Stage 3 – Integration**

*It's already too late!*



# Offences, Penalties and Criminal Liability

Money Laundering offences considered very serious in Cyprus and courts impose heavy penalties. Under the provisions of the Law, the following offences and penalties are defined:

- **Failure to comply with AML/CFT Law or directive issued by a Supervisory Authority:**

Administrative fine not exceeding EUR 1,000,000. If offender received benefit from infringement which exceeds amount of administrative fine imposed, then administrative fine of up to twice amount of benefit received may be imposed. If infringement continues, an administrative fine not exceeding EUR 1,000 for each day infringement continues may be imposed



# Offences, Penalties and Criminal Liability - continued

- **For committing a Money Laundering offence:**
  - For a person who knows: 14 years imprisonment or a penalty of up to EUR 500,000 or both
  - For a person who ought to have known: 5 years imprisonment or a penalty of up to EUR 50,000 or both
- Article 27 of the AML/CFT Law provides that a person who knows or reasonably suspects that another person is engaged in money laundering or financing of terrorism, and the information on which that knowledge or reasonable suspicion is based comes to his attention during the course of his trade, profession, business or employment, that person commits an offence if he does not report this information to MOKAS as soon as reasonably practicable after it comes to his attention – **Penalties:**
  - Imprisonment not exceeding 2 years or a penalty not exceeding EUR 5,000 or both





# Offences, Penalties and Criminal Liability - continued

- **For the offense of tipping off:**
  - Upon conviction, imprisonment not exceeding 2 years or a fine not exceeding EUR 50,000 or both
- **Violation of the United Nations Security Council Resolutions and Decisions (Sanctions) and the Council of the European Union (Restrictive Measures) Law – Penalties:**
  - Criminal prosecution can only be exercised with the approval of the Attorney General
  - For a natural person, imprisonment not exceeding 2 years or a fine not exceeding EUR 100,000 or both
  - For a legal entity a fine not exceeding EUR 300,000
- **Terrorist offenses under the Combating of Terrorism Law of 2010 (N.110(I)/2010) – Penalty:**
  - Life imprisonment
  - Imprisonment and/or financial penalty for lesser offences



# Summary of Offences

- Convert, transfer or remove property from illegitimate sources
- Acquire, possess or use property from illegitimate sources
- Conceal or disguise information relevant to property from illegitimate sources
- Participate in, cooperate, conspire/attempt to commit, provide counselling/advice to commit any of the above offenses
- Assist another person to convert, transfer or remove property from illegitimate sources to evade legal consequences from such actions
- Tipping-off\*



*\*Tipping-off is the illegal or improper act of notifying a person that he/she is the subject of a STR, SAR, or is being investigated/pursued by the authorities*

# HOW DO WE COMPLY?

*KYC is the process of collecting personal data and identifying clients at start of relationship – allows creation of risk profile*

- ✓ Identify all relevant persons & legal entities (shareholders, UBOs, directors, company secretary, signatories, Attorneys, persons with significant influence, counter-parties)
- ✓ Identify Source of Funds/Source of Wealth



# When Should CDD/KYC be Performed?

CDD/KYC should be performed:

- When establishing a new business relationship with a client, and certainly before any transactions take place
- In case of an occasional transaction equal to or higher than €15,000 irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked
- When ML/TF is suspected, irrespective of amount
- When have doubts over veracity/adequacy of CDD already obtained

**Note:** CDD/KYC should be carried out also in the case of existing clients periodically, in accordance with the client risk rating, and when the relevant circumstances of the client change, or when trigger events occur



# What do we Mean by KYC?

The purpose of KYC is to identify the client company and all the relevant related persons/entities

## ➤ Physical Persons:

- International passport, or photo ID, or driving license (photo)
- Utility bill, or bank statement, or tax assessment (less than 6 months old) or internal passport (former CIS countries)
- Source of funds **for the specific transaction** (+ supporting documents)

## ➤ Legal Entities (registered shareholders of client):

- Certificates (incorporation, registered office, directors & co secretary, shareholders, good standing)
- M&A
- Group structure (signed & dated) to include “sister companies”
- Latest audited FS
- Resolution authorising contact person



# KYC - continued

- **Direct/Indirect Ownership (Legal Entities) in Shareholder(s) of Client:**
  - Certificate of Incumbency
  - Declaration of Trust or other nominee arrangements, if any
- **Trusts, Foundations, etc:**
  - Documents confirming registration date & number
  - Trust Deed, Constitution or similar
- **Trustees, Council Members, Settlor/Founder, Protector, Beneficiaries, etc:**
  - See above “Physical Persons”
- **KYC collection should take place at start of relationship, before any services provided.**

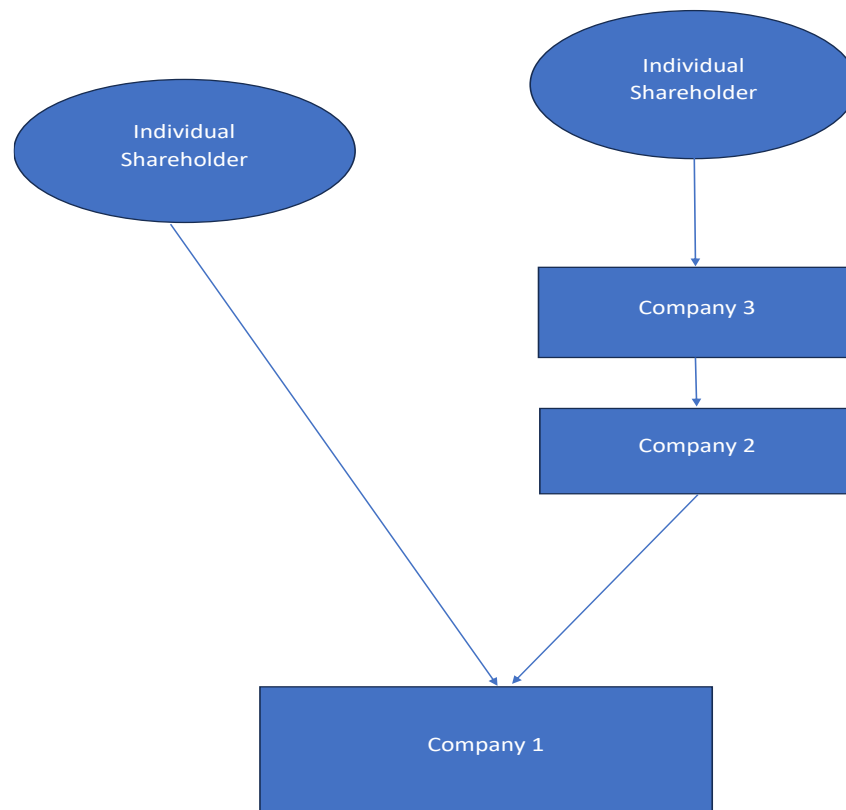


*NOTE: Each document should only be used for single purpose*

# Who Should we Check?

1. Direct shareholders of client, physical persons or legal entities – **full KYC**
2. If there is more than one layer in the ownership structure above the client – **full KYC for the UBOs** (physical persons)
3. For intermediary layers - **Certificate of Incumbency (or equivalent), Declaration of Trust or other nominee arrangements (if any)**

## Ownership Structure





# Economic Profile

The Economic Profile of a client is a snapshot summary of all the known information about the client

Purpose is to assist the Obligated Entity to identify any Red Flags regarding change of ownership or group structure, change of business activities, suspicious activity or transactions which are not normal for this client, and any other indications that there is a greater risk of ML or TF



# Constructing the Economic Profile

Needs to be a separate easily accessible document as part of client file

Should include:

- ✓ **Company Details:** name, country of registration, registered office address, identification details of UBOs, shareholders, directors, authorised signatories, group structure
- ✓ **Business Details:** nature of business, expected annual turnover, expected incoming and outgoing funds, counterparties
- ✓ **Banking Details:** names of banks where accounts held



# Risk Assessment – Risk Based Approach

*“A risk-based approach means that countries, state authorities, as well as the private sector should have an understanding of the ML/TF risks to which they are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks.”*

*“It is therefore not optional, but a prerequisite for compliance with all other requirements. A risk-based approach therefore consists of the identification, assessment and understanding of risks, as well as the consequent application of AML/CFT measures commensurate to these risks in order to ensure an effective mitigation thereof.”*

*“The FATF issued a number of guidance papers on risk-based approach in order to assist countries to implement the requirements of the FATF Recommendations, but also to help them develop their own guidance for the private sector.”*

**Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)**



# Risk Assessment & Risk Factors

RBA is cornerstone of a successful AML/CFT program

Purpose is to enable Obligated Entities to correctly identify, assess and understand the risks they face and prioritise their efforts to mitigate those risks

Obligated Entities can then focus their resources where risk of ML & TF is higher

Risk score of each client generates the level of CDD required (standard, SDD, EDD)



# Risk Assessment & Risk Factors

## RBA Risk Factors:

- Due to clients
- Due to countries/geographical areas
- Due to products & services
- Due to delivery channels/transactions



Therefore, proper Risk Assessment  
needs proper KYC!



# Risk Levels

Risk assessment results in risk rating for each client and enables Obligated Entity to decide where to focus

- Low Risk ➡ CDD + SDD
- Medium/Normal Risk ➡ CDD
- High Risk ➡ CDD + EDD



# Low Risk Factors

**Customer:** government & semi government bodies, publicly listed companies

**Product, Service, Transaction, Delivery Channel:**

life insurance with low premium, pension schemes, some financial products, products with limited value/purse limits (e.g. some types of e-money)

**Country, Geographic:** EU Member States, 3<sup>rd</sup> countries with equivalent ML/TF regime, countries with low level of crime & corruption, 3<sup>rd</sup> countries that follow FATF recommendations





# High Risk Factors

**Customer:** PEP, unusual circumstances, resident in high risk country, asset holding structures, nominee shareholders/bearer shares, cash intensive, complex structures without reason

**Product, Service, Transaction, Delivery Channel:** private banking, anonymous transactions, non-face-to-face, payments from unknown parties, new products/services/business practices/technologies (e.g. virtual assets, online gaming), extractive industries, arms/weapons/military

**Country, Geographic:** countries without effective AML/CFT regimes, countries with significant crime and corruption, sanctioned/embargoed countries, countries supporting/funding terrorism



# Medium/Normal Risk Factors

**All other clients!**



# Risk Assessment

- Client Risk Assessments
- Firm-Wide Risk Assessment (AML & Sanctions)



## ENTERPRISE - WIDE RISK ASSESSMENT



# CDD/On-Going Monitoring

KYC is process of collecting personal data and identifying clients at start of relationship – allows creation of risk profile

CDD is process for ongoing monitoring of clients and transactions, and ensuring that KYC information is correct and up to date – ongoing assurance framework

Names often used interchangeably

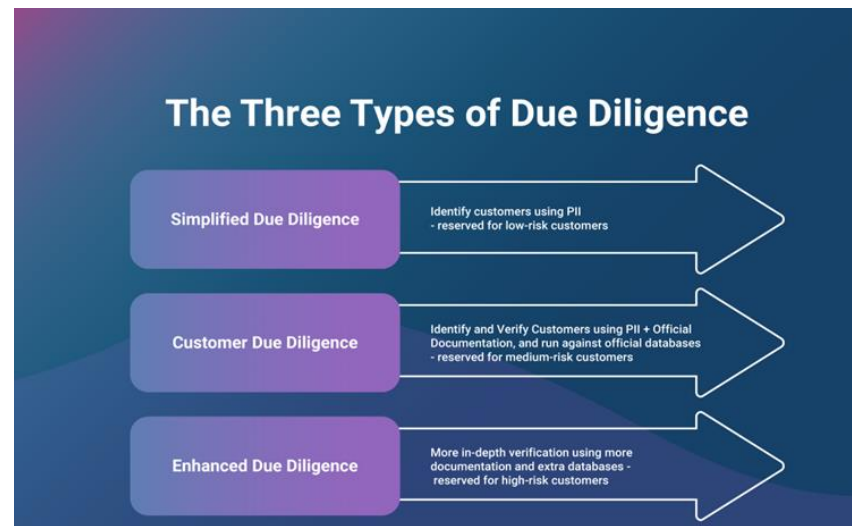


# Types of CDD

The level of CDD to be applied is determined by risk rating of client

## 3 levels of CDD:

1. Normal CDD is applied to **all** clients (low, Medium/Normal, high risk)
2. Simplified Due Diligence (SDD) is applied to low risk clients, **BUT** is not an exemption from CDD – allows adjustment on amount, timing or type of CDD
3. Enhanced Due Diligence (EDD) is applied to all high risk clients, and is in addition to CDD



# CDD

CDD is the base for all clients and must be applied in all cases, irrespective of the risk rating. **Default level**

Standard level of CDD involves:

- Collection of appropriate KYC documents/information
- Screening using recognised databases
- Transaction monitoring based on services provided to client
- Regular client reviews (e.g. every 2-3 years or when trigger event occurs)



# SDD

SDD must only be applied in cases where client risk rating is low

Must carry out CDD, but can vary:

- Quantity, source and type of documents collected
- Frequency of reviews, e.g. every 3-4 years or when \*trigger event occurs
- Frequency/intensity of transaction monitoring, e.g. transactions above certain threshold

*\*Trigger events: change of UBOs, shareholders, BoD, group structure, business activities, or when veracity of KYC documents is in doubt, or when there is a suspicion of ML/CT*



# EDD

EDD must be performed in all cases where client risk rating is high

EDD is in addition to CDD

EDD involves:

- Obtain CV, Source of Wealth & bank/professional reference as part of KYC
- Senior Management approval for onboarding & continuing relationship
- Negative media screening
- Enhanced transaction monitoring
- Annual client review and risk assessment





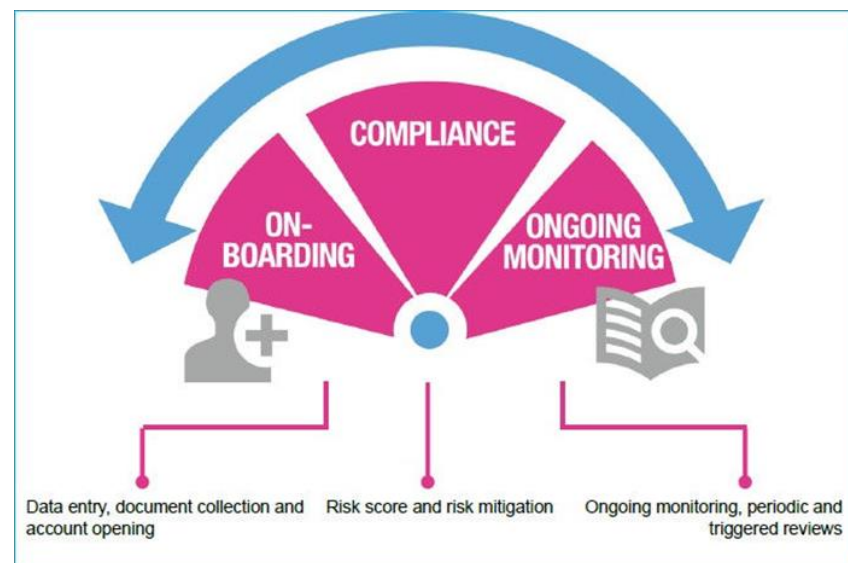
# Ongoing Monitoring

AML & CFT is a dynamic process, therefore **Ongoing Monitoring** is at the heart of AML compliance best practice

Ongoing monitoring utilises all the building blocks put in place during the onboarding, KYC and CDD processes (KYC, economic profile, risk assessment & rating)

Comprised of following elements:

- Transaction monitoring
- Periodic review of client, UBOs, directors, authorised signatories, etc



# Ongoing Monitoring - Elements

**Transaction monitoring** – aim is to verify that the business activities of the client, counterparties, sources and destination of funds, etc are as stated in the client’s economic profile, or if any changes have taken place, to re-assess the risk rating

**Periodic review of client, UBOs, directors, authorised signatories, etc** – based on the client’s risk rating a full review of the client is undertaken and KYC documents updated

**Trigger events** – also require a full review of the client, as per the previous point

**Extent of monitoring** – will depend on services provided



# Proper Documentation/Reporting

- Record keeping
- Suspicious Activity Reports (SARs)
- Suspicious Transaction Reports (STRs)



# Record Keeping

Record keeping requirements are not subject to RBA so no room for subjective assessment...**All Obligated Entities must keep records**

Records must include:

- CDD/KYC documents
- Sufficient supporting records so as to enable a transaction under investigation to be reconstructed

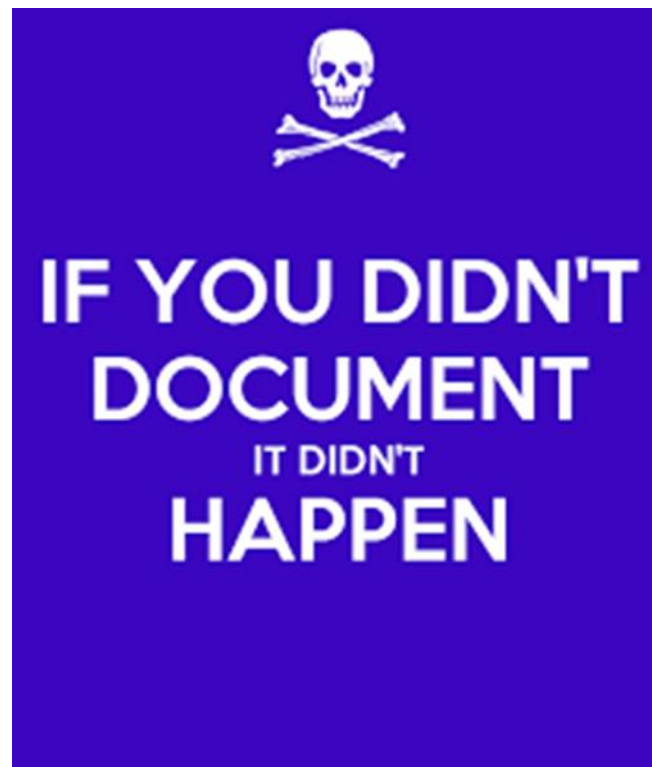
Records must be kept in a format that can easily be retrieved and provided to the investigating authority, if required, and to enable the Supervising Authority to assess the Obligated Entity's observance of AML/CFT policies & procedures, without undue delay

Records must be kept for 5 (five) years after the end of a relationship, or after the last transaction date



# Record Keeping

***If it's not documented  
it didn't happen!***



# Suspicious Activity Reports (SARs) & Suspicious Transaction Reports (STRs)

**SAR** = general suspicions due to overall behaviour of reported person(s). Behaviour creates knowledge or suspicion that person(s) may be involved in criminal activities which generated proceeds

**STR** = more targeted, comprise of suspicions based on specific suspicious transactions, generate knowledge or suspicion that person may be involved in criminal activities from which illegal proceeds were derived

AMLCO is responsible for submission of SARs and STRs to MOKAS via GoAML platform

AMLCO receives Internal Suspensions Reports from staff – evaluates, and if necessary, files SAR/STR to MOKAS

If AMLCO decides not to submit SAR/STR must clearly document reasoning behind decision



# Reliance on Third Parties/Accredited Introducers

Obligated Entities can enter into agreements with 3rd parties (credit/financial institution, auditor, external accountant, tax advisor, trust & company service provider, law firm) for carrying out all/part of client identification and CDD. BUT must immediately provide KYC documents for start of relationship with client

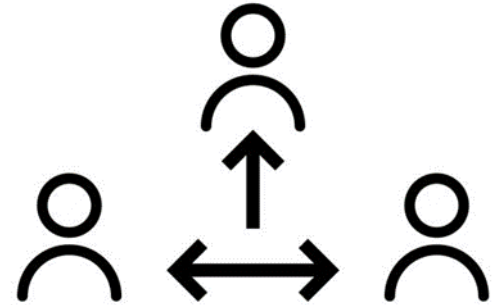
Accredited introducers must operate in EEA or 3rd country and fulfil following:

- ✓ Apply CDD & record keeping measures consistent with EU Directives
- ✓ Subject to supervision consistent with requirements of EU Directives

Obligated Entities are **prohibited** from relying on 3rd parties operating in high risk third countries

Can only rely on 3rd parties at outset not for ongoing monitoring

3rd party is in full compliance with the Personal Data Law and introduced clients are aware that their personal information will be disclosed and have no objection on this



# Reliance on Third Parties/Accredited Introducers - continued

Obligated Entities are required to apply following additional measures:

- Assess AML/CFT systems & procedures of third party (AML manuals)
- Be satisfied that third party implements KYC & CDD policies & procedures in line with The Law and The Directive
- Keep separate file for each accredited introducer with relevant assessments, KYC, etc
- Take steps to ensure that third party will provide KYC documents immediately
- Establishment of cooperation with third party and acceptance of KYC documents verified by third party subject to approval by AMLCO





# Reliance on Third Parties/Accredited Introducers - continued

The following KYC documents should be collected to accept third party as accredited introducer:

- ✓ Incorporation documents
- ✓ KYC of shareholders of firm and/or any other person who controls the firm
- ✓ Copy of License/certificate for providing its services and any other certificate confirming its supervision for AML purposes
- ✓ AML manual
- ✓ Questionnaire to assess the systems and procedures applied by the 3rd party for AML/CFT



# Beneficial Owner & Trust Registries

18 February 2021 5th EU AMLD transposed into Cyprus Law

Legislation created obligation for companies & other legal entities incorporated in the Republic of Cyprus to register beneficial owners in a national centralised register

Under the provisions of Article 61C(4)(a) of The Law, CySEC is responsible for maintaining a Beneficial Ownership Register of Express Trusts and Similar Legal Arrangements ('The Register') via the CyTBOR platform

The Registrar of Companies has the responsibility to maintain the register of beneficial owners for all companies incorporated in Cyprus



*Note: As part of an ICPAC AML review, you may be asked to present evidence that you have submitted BO Registers for each client. Other Regulators may also do the same*

# Definition of Beneficial Owner

In accordance with the law, a beneficial owner is defined as any natural person(s) who ultimately owns or controls the Obligated Entity and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

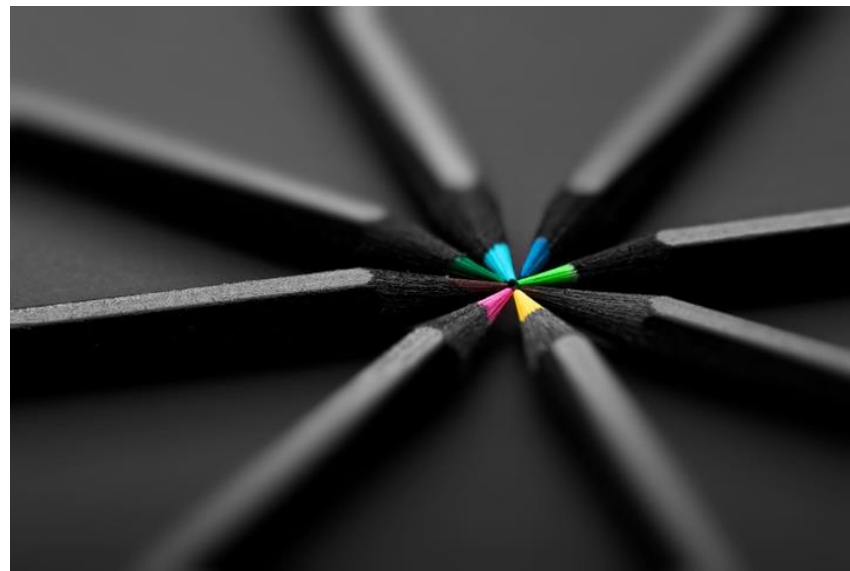
- **For corporate entities:** the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person shall be an indication of direct ownership.
- **For trusts:** the settlor; the trustee(s); the protector, if any; the beneficiaries, or where the individuals benefitting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates and any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.
- **For legal entities such as foundations and legal arrangements similar to trusts:** the natural person(s) holding equivalent or similar positions to those referred to in point (b) above.

# COMPLIANCE CULTURE

# Compliance Culture

Strong AML Compliance Culture is a “Top Down” process, with strong & clear messages and commitment from Senior Management

If successful, Obligated Entity not only meets regulatory obligations and reduces risk of failings, sanctions and reputational damage, but also results in more efficient processes as whole Company engaged in common goal



# 7 Steps to Building Strong Compliance Culture

1. Top Down – Senior Management is driving force, positive & consistent messages
2. Leadership Engagement – take responsibility
3. Monitoring & Assurance Framework – independent review
4. Profits should not take priority over compliance
5. Allocation of sufficient resources for AML Compliance program
6. AML Compliance should be viewed as integral part of business practices and not as a burden
7. Training & Communication – staff should understand the “why” of compliance and not only the “what” so they understand the real value of what they are doing





# COMMON FINDINGS FROM REGULATOR REVIEW VISITS

# Policies, Procedures & Internal Controls

- AML manual doesn't include procedures & controls
- AML manual not updated to reflect latest provisions of the Law or risk appetite of senior management
- Policies & procedures in AML manual are not proportional/relevant/accurately reflect actual procedures and nature and size of firm and its clients
- No monitoring procedures to assess compliance/effectiveness of policies & procedures
- Board member not assigned responsibility of ensuring implementation of policies & procedures
- MOKAS and Regulators not advised of name & position of AMLCO
- Responsibilities & role of AMLCO not clearly defined and documented
- AMLCO doesn't have direct/timely access to all necessary information/documents/data to perform role



# Risk Based Approach

- RBA policies & procedures not properly documented and in line with Client Acceptance Policies
- Client risk assessments not documented properly
- No firm-wide risk assessment
- RBA procedures not consistent for all clients
- Lack of risk grading system/not all client characteristics taken into consideration
- Risk assessments missing some risk categories
- Lack of proper risk factor weighting according to seriousness – unable to establish appropriate risk score, or incorrect risk scoring (e.g. low risk clients)

# Risk Based Approach – continued

- No procedure for automatic high-risk categorisation (PEP, CIP, high risk 3<sup>rd</sup> countries)
- No procedures for risk re-classification following ongoing CDD
- Lack of adverse media screening- Regulated Entities failed to flag and properly assess published adverse information, relating to the reputation of their customers and/or beneficial owners
- Adverse media not taken into consideration as affecting client risk rating
- Lack of screening of related companies/counterparties to see if affect client risk rating
- Regulated Entities have not always accounted for risks posed by UBOs related to the Cyprus Investment Program (CIP)

# KYC & CDD

- Proof of residence not obtained/or not properly certified/or out of date
- No or insufficient understanding of control structure/ownership to identify all UBOs
- KYC not completed prior to start of relationship or 1<sup>st</sup> transaction
- No evidence if copies of KYC documents made from originals at face-to-face meeting
- In no face-to-face cases, no EDD undertaken
- Where KYC supplied by 3<sup>rd</sup> party:
  - No verification if applies equivalent CDD with EU
  - Subject to supervision equivalent to EU
- Reliance on 3<sup>rd</sup> parties for ongoing CDD – *Not allowed!*
- No direct contact with UBOs, controlling parties

# KYC & CDD - continued

- Reliance on 3<sup>rd</sup> parties in absence of:
  - Assessment of their systems, policies, procedures for AML/CFT
  - Verification that 3<sup>rd</sup> party implements KYC/CDD procedures in line with the Law & Regulator Directives
  - Lack of separate files for each 3<sup>rd</sup> party due diligence
  - No evidence that AMLCO approval obtained before accepting client KYC from 3<sup>rd</sup> party
- No/insufficient or out of date economic profile to demonstrate understanding of:
  - Nature of business activities
  - Size, nature, frequency of transactions
  - Business rationale
  - Client structure including subsidiaries & related companies
  - Source of Funds, and if applicable, Source of Wealth

# EDD

- Procedures not risk based – same measures for all risk categories
- Procedures not adjusted to reflect areas of higher risk:
  - Detailed review of purpose of business relationship, client's background/ownership/financial status, counterparties
  - Systematic screening
  - Additional steps to verify if transactions consistent with purpose/nature of business
  - Procedures for increasing/adjusting transaction monitoring
- Client categories requiring EDD not recorded in AML manual
- No escalation process for approval/renewal of engagement for high-risk clients

# PEPs

- No escalation process for approval/renewal of engagement for PEPs
- Inadequate verification of size & source of Funds/Wealth
- No enhanced ongoing monitoring
- No screening
- No evidence that ex-PEPs with normal risk have no continuing high-risk characteristics

# On-Going Due Diligence

- Procedures for on-going relationship & transaction monitoring non-existent
- On-going monitoring not customised based on risk levels and type of services provided
- No procedures for ensuring KYC and CDD documents/information are up to date/relevant/properly certified
- Initial client review not updated & impact of changes on risk not considered:
  - Changes in shareholding
  - Unexplained changes in activities or turnover
  - Unexplained changes in nature of transactions
  - New entities set up in structure

# On-Going Due Diligence – Continued

- Non-existent or inadequate evidence of on-going monitoring of transactions by:
  - Review of transactions to ensure that consistent with business & risk profile
  - Failure to collect supporting documentation for transactions
  - Verify that SoF for transactions is legitimate
  - Investigate transactions that are large, complex, unusual, have no economic rationale to make sure they are not suspicious
  - Screening & background checks
- No procedures for in-depth scrutiny in cases where clients based in high-risk countries or where transact with high-risk countries



# SoF/SoW

- CDD questionnaires limited/brief/inadequate and replies not substantiated
- Face value acceptance of client explanations & lack of verification
- Lack of risk-based procedures – same measures for all risk categories
- Lack of understanding between client SoF and SoW

# Sanctions

- Non-existent/insufficient implementation & documentation of Sanctions Regulations policies & procedures
- Poor/non-existent client sanctions risk assessment
- No firm-wide sanctions risk assessment
- No sanctions screening of clients or counter-parties
- No new screening after changes to sanctions lists, or new UNSCR or EU Decision/Regulation issued
- Poor or non-existent transaction screening
- Non-existent/poor documentation of sanctions screening
- Non-existent/insufficient sanctions related training
- No procedure to investigate positive matches
- No procedure to inform AMLCO or Regulator of positive matches

# SARs & STRs – Identification & Reporting

- Non-Existent/inadequate policies & procedures for suspicious transaction reporting
- Reporting procedures not updated to reflect MOKAS online reporting via GoAML system
- Non-existent/inadequate records of SARs & STRs
- No procedure for assessment of SARs & STRs by AMLCO
- No/insufficient documented reasoning why SARs & STRs not reported to MOKAS by AMLCO
- Failure to report SARs & STRs to MOKAS – *has obliged entity really never noticed any suspicious activity?*
- Lack of understanding/knowledge/training and policies & procedures regarding tipping-off

# Documentation & Record Keeping

- Record keeping policy not properly documented
- Record keeping policy does not clarify what documents must be kept
- Non-existent or inadequate policies & procedures to ensure integrity, confidentiality and ease of retrieval/security of records/documents/information
- Retention policies not in line with provisions of all laws/regulations and lack of understanding of interaction of such laws/regulations, e.g. AML/CFT vs GDPR
- In cases where obliged entity ceased operations did not keep required records for 5 years from date when ceased

# Training & Education

- AMLCO has insufficient training and/or knowledge
- No/insufficient training of staff on obliged entity's policies & procedures and AML/CFT/Sanctions regulations
- Staff training is not tailored to job positions/roles (staff, management, Board of Directors)
- No systematic refresher training or updates on new/changes to legislation

# Key Takeaways

## ➤ **AML/CFT Compliance is important so as to:**

- ✓ Avoid risk of facilitating/assisting criminal activity, terrorist financing, and/or sanctions circumvention
- ✓ Protect yourself (job, reputation, qualifications)
- ✓ Protect your firm
- ✓ Protect other clients

## ➤ **Obligations:**

- ✓ Identify clients & other stakeholders/counterparties
- ✓ Independent verification of information/documentation
- ✓ Understand business activities
- ✓ Identify, assess, manage/mitigate risks
- ✓ Ongoing monitoring
- ✓ Proper record keeping & reporting

# Some Final Points

Proper AML and Sanctions compliance is no longer an easy task

You need to invest time, money and resources in:

- ✓ Knowledge & training
- ✓ Software
- ✓ Independent expert assistance & support

# Some Final Points - continued

And remember.....

.....No Client is worth losing your:

- License
- Business
- Career
- Reputation





# Questions...



# Contact Details



Tel: 70007599

Mobile: 99 626 843

Email: [haig@aequus.cy](mailto:haig@aequus.cy) or:  
[team@aequus.cy](mailto:team@aequus.cy)

Website: [www.aequus.cy](http://www.aequus.cy)

P O Box 27720, Nicosia 2432

The slides contained in this seminar are the property of Aequus Business Consulting Ltd. The reproduction, transmission, sharing or publishing of all or part of this work, whether by photocopying or storing in any medium by electronic means or otherwise without the written permission of the owner is strictly prohibited.

Aequus Business Consulting Ltd ©

# CYPRUS FIDUCIARY ASSOCIATION

---

## **CYFA 2023 Seminar #9:** “How Theory becomes Practice?”



**Speaker: Mrs Athena Yiallourou**  
Risk and Compliance Director  
Trident Trust Company (Cyprus)  
Limited

Anti-money laundering (AML) refers to laws and regulations intended to stop criminals from disguising illegally obtained funds as legitimate income.

Counter Terrorist Legislation and practices refer to measures which prevent money (sometimes legitimate) to be used for terrorist activities.

# How theory/Legislation is linked with Practice

- Policies
  - AML Manual
  - Acceptance Policy
  - Sanction Policy
  - Approval Policy
- Procedures – Onboarding Procedure
  - Monitoring Procedure
  - Departmental Procedures
  - Job Description

# How theory/Legislation is linked with Practice (2)

- Training
  - General Training /Induction
  - Specific Training
  - Repeated Offenders Training
- Monitoring Program
  - Compliance Monitoring
  - Assessment of results
  - Report to Board

# 1. Can I accept this Client ?

- Company Acceptance Policy
- Legislation
- Sanctions
- Risks
- Provided information
- Risk assessment
- Cost V Benefit

# Case 1

- A new client requires the registration of a new entity and the ASP to offer full services
1. How would you avoid the management of an entity related with Bribery funds ??



# Case 2

- A new request for a managed entity.
- All KYC and information submitted in line with legislation.

Q. How do we deal with Geographical Risk ?

## 2. Client Profile

- Include :
  - Business Activities and any changes
  - Structure
  - Updated KYC records
  - Banking details and records
  - Main relations
  - Source of Funds
  - Source of Wealth
  - Memos and Communication with client (meetings, calls, updates)
  - Screening and other searches

# How is Client profile useful

- Monitoring
- Assessment
- Meetings
- Promotion
- Reminder
- Monitor regulatory obligations
- Prevention /Comparison/Reporting

# 3. Monitoring

- Regulatory Periodic reviews
- Day to day transactions
- Compliance monitoring Program ( 2<sup>nd</sup> level of defense)
- Risk monitoring
- Screening
- Banking transactions
- Accounting
- FATCA/DAC6 etc

- Business Activities V Transactions
- Risks – Geographical, Sectoral, Client
- Legal implications
- Sanctions
- Timing
- Update records

- Regulatory Obligation
- Protection
- Risk mitigation tool
- External reporting
- Investigation
- Critical thinking
- Knowledge

- Internal Suspicious reporting
- Clear line of reporting
- Investigation – further details
- External Reporting
- Mitigation measures
- Exit relation.

# Sanction Considerations

- Why/How/What/When?
- Policy
- Risk assessment
- Impact on Company
- External Advice



# Issues to consider in cases of possible sanction related transactions

- The Client Business Activities-  
Geographical/Sectoral restrictions
- The Source/Flow of Funds
- The Shareholding/Ownership risk
- PEP and any other Business relations
- Past and proposed transaction assessment and monitoring
- Updated KYC records – review the logic and the evidence
- Client Profile information /Historical records.

# Do I think compliant?

- One way Street
- Ethical Dilemmas
- Business V Compliance
- Risks of non – Compliance
- Prevention V Mitigation of Risks
- De- risking
- Practical considerations
- Policies and Procedures
- Logical
- Empathy

# Practice makes perfect

Learn and Grow

Think

Analyze and assess

Transaction V Profile

Communication

Information

Record keeping

# Ethics and Culture V Practice

- Tax evasion
- Bribery
- Unethical behavior
- Slavery /Child abuse
- War
- Equality
- Drags
- Terrorism
- Safe environment
- Greenwashing

# Tips for a Culture

- Relate procedures with real life scenarios
- Do not underestimate the results of a Compliance Culture
- Use Meetings and other communication to get information
- Short sessions on deficiencies found
- Deal with any deviation on the spot
- Reporting line
- Group therapy
- Include compliance subject in company activities
- Automation

# Mitigating Risks

- Reputational Risk
- Financial Risk
- Legal Risk
- Regulator Penalty Risk
- License Risk
- Imprisonment Risk

# My role

- Important at any level
- Know General Policies
- Know Departmental Procedures
- Address issues on the spot
- Report any red flag or suspicion
- Participate in Training – Implement at least one new thing after each training session.
- Make suggestions
- Get involved – Participate

Athena Yiallourou  
Risk and Compliance Director  
Trident Trust Company (Cyprus) Limited  
[ayiallourou@tridenttrust.com](mailto:ayiallourou@tridenttrust.com)  
tel. 24820650

*Thank You!*





# Thank you.

---



## CYPRUS FIDUCIARY ASSOCIATION

### **Business Address:**

6 Emmanuel Roide Street,  
Office 402, 1095 Nicosia, Cyprus

Tel.: +357 22 256263

Fax: +357 22 256364

**E-mail:** [info@cyfa.org.cy](mailto:info@cyfa.org.cy)

**Website:** [www.cyfa.org.cy](http://www.cyfa.org.cy)