

## AML Quality & Control

### Effective Anti – Money Laundering



# Schedule:

---

## Money Laundering Defined

Effective Due Diligence – Know your Client

## Politically Exposed Persons - Private Banking

Trusts – Foundations - Complex Structures

## ML in Real Estate – Trade Based ML

Professional Intermediaries – Business Associates

## Terrorist Financing

Sanctions Compliance

## Effective Transaction Monitoring

Customer Review Process

## Suspicious Activity Reports

Closing Remarks – Conclusion



# Money Laundering Defined

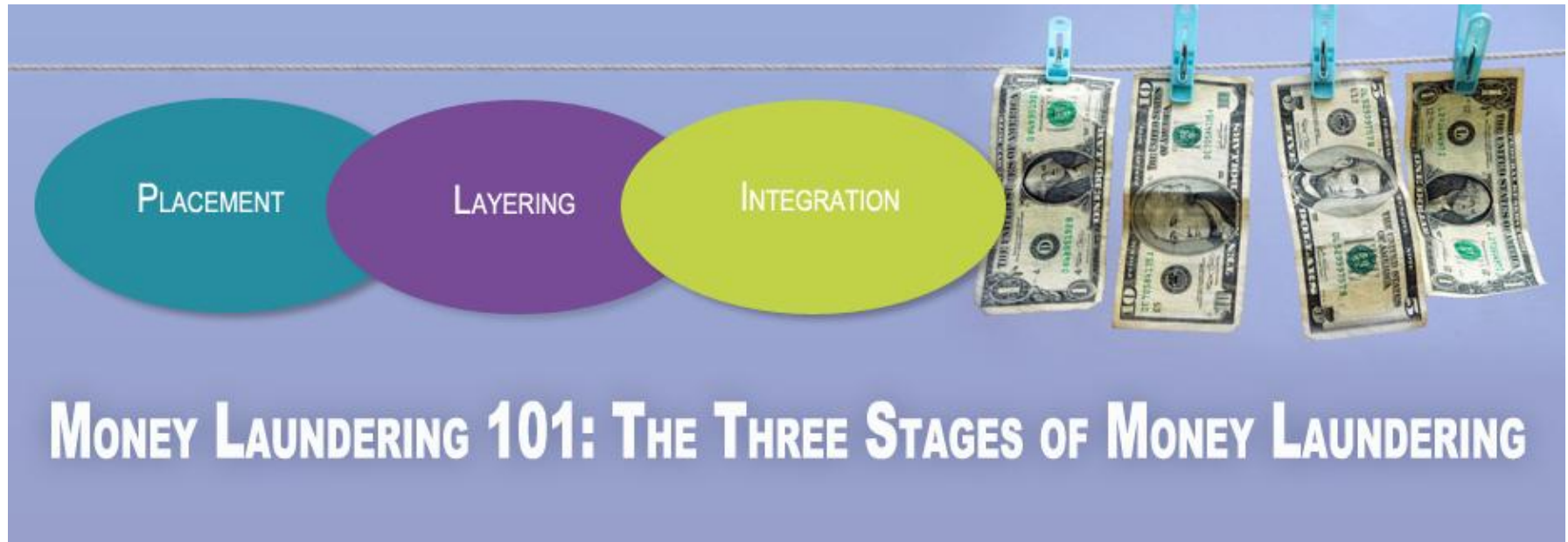
---

When committed intentionally, Money Laundering, is defined as:

- a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

*(4<sup>th</sup> EU AML Directive)*

# The stages of Money Laundering explained



# The stages of Money Laundering explained

---

**Placement** is the introduction of unlawful proceeds into the financial system. **Structuring**, which is considered a type of placement activity, is any attempt to evade legal reporting requirements for cash/currency transactions conducted with a financial institution. Examples of structuring may include, but are not limited to:

- Cashing checks for amounts just below reporting or recordkeeping thresholds.
- Dividing large amounts of cash/currency into smaller sums that fall below reporting or recordkeeping thresholds (**smurfing**) and then depositing the funds directly into a bank account on one or more days, in any manner.

# The stages of Money Laundering explained

**Layering** involves moving funds around in the financial system in order to conceal the origin of the funds. Examples include, but are not limited to:

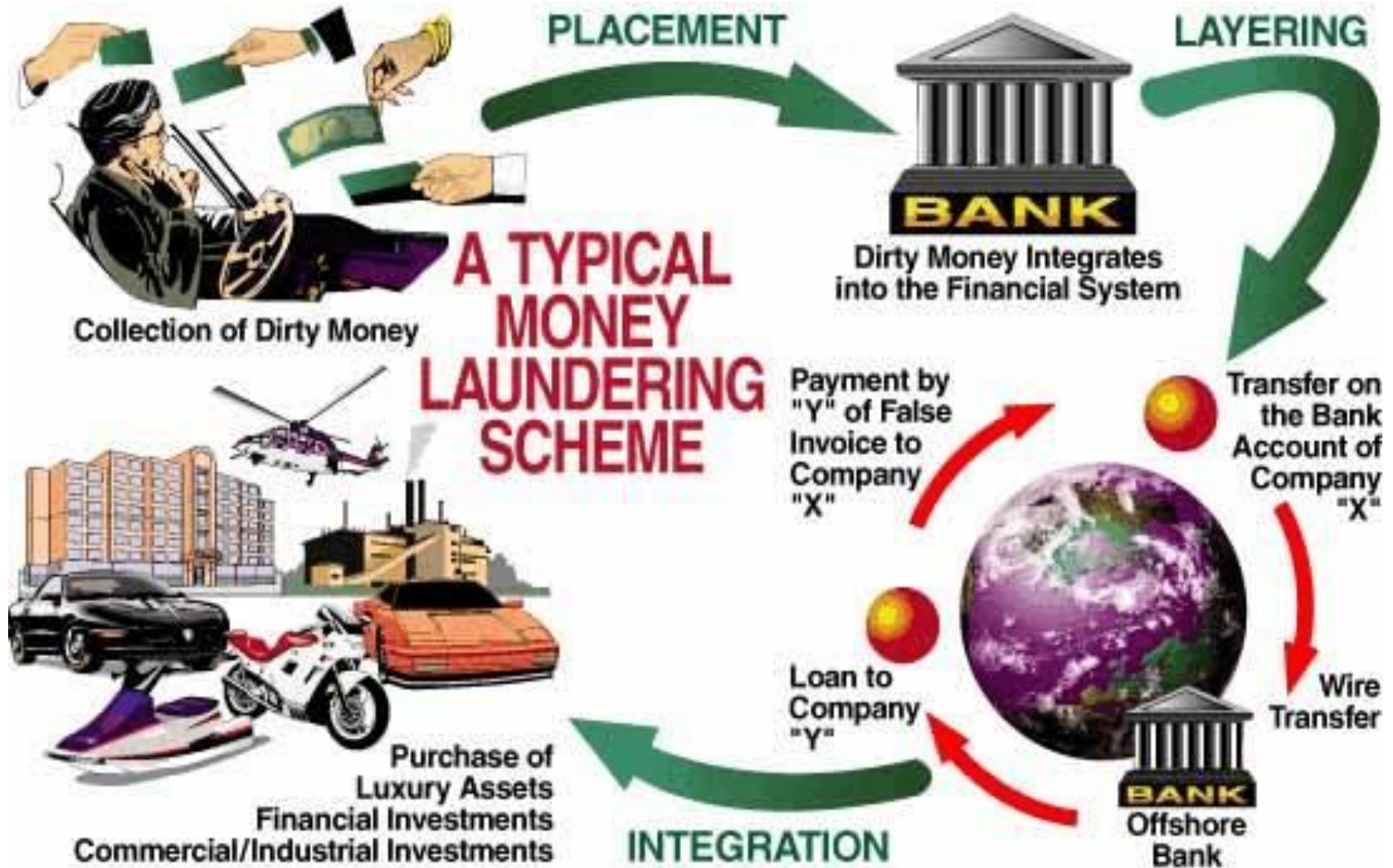
- Exchanging monetary instruments for larger or smaller amounts.
- Wiring or transferring funds.
- Buying or selling securities through numerous accounts.
- Obtaining a loan in one or more financial institutions.

**Integration** is the ultimate goal of the money laundering process. In this stage, the illicit funds may appear legitimate and are often used to purchase other assets, for example:

- Real estate or other assets
- Securities investments
- Cash Intensive Businesses



# Money Laundering Cycle



# BOC Risk Appetite Statement Policy

---

- ❖ The Bank of Cyprus' ("BOC" or "the Bank") Risk Appetite Statement makes reference to "Compliance Risk" and states that:

*"the Bank maintains a zero tolerance for regulatory / compliance risk. It aims to comply with all regulatory requirements and thus avoid all penalties. The Bank must ensure that it adopts all regulatory, legal and compliance requirements in a proportionate way that satisfies the requirements of the regimes in a pragmatic, cost effective fashion. The on-going cost of compliance is a cost of doing business and should not be material in terms of annual income."*

- ❖ Going a step further, the Board's risk appetite with respect to ML/TF risk is as follows:

*"the Bank maintains a zero tolerance for ML/TF risk. The Bank is obliged to transact its business so as to ensure it minimizes the risk of its systems and processes, and those of its affiliates, being used for ML or TF purposes. BOC adopts risk appetite and practices which place it at the "best practice" end of international standards, in relation to preventing Money Laundering and Terrorism Financing abuses."*



# It all comes down to: **KNOW YOUR CLIENT**

**Know your client** (KYC) is the process of an institution verifying the identity of its clients. It is important to help prevent identity theft, financial fraud, money laundering and terrorist financing. The objective of KYC is to enable banks and other institutions to know and understand their customers better and help them manage their risks prudently.

*\*Side effect: It is also great for identifying business development opportunities!\**

**KEEP  
CALM  
AND  
KNOW-YOUR-  
CLIENT**

# KNOW YOUR CLIENT – the client profile

**Customer Due Diligence(CDD)** – one of the measures to prevent money laundering and terrorist financing, by ensuring that we understand **who the customer really is** and **what the expected relationship with them will be**. (part of FATF 40 Recommendations).

A complete client profile contains detailed information about:

- The customer (KYC)
- The customer's business (KYCB)
- The customer's clients / counterparties (KYCC)

*Due diligence must be performed to the organization's satisfaction before engaging in a new client relationship and reviewed/updated periodically in accordance with the risk profile of the client*

# KNOW YOUR CLIENT – the on-boarding process

- Who is the customer – the UBO / physical person exercising management and control (all related entities, affiliates and closely associated persons including owners, directors, authorized signatories etc)
- Establishing/verifying client's identity - Identity documents (physical person / company / legal arrangements)
- Residential / Registered address
- Address of the main economic activities
- Management and control address (physical), headquarters – public information to verify
- Trade name, No of employees
- If customer is part of a group obtain info about the group and understand the role of the customer within the group – level of complexity
- Check against sanctions / PEP lists

# KNOW YOUR CLIENT – the UBO

---

## WHO IS THE ULTIMATE BENEFICIAL OWNER?

The natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

The beneficial owner is always a natural person – a legal person cannot, by definition, be a beneficial owner. The definition therefore also speaks of “ultimate” control: A legal person can never be the ultimate controller – ownership by a legal person is itself always controlled by a natural person

# Client take-on – On-boarding

## Good practice examples

- Files contain a customer overview
- Establishing and documenting PEP and other HRCs' source of wealth.
- Understanding/documenting complex ownership structures and the reasons for them.
- Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.
- Making clear judgments on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.
- Documenting who the counterparties are by establishing that they are in the same line of business
- Ensure declared turnover makes sense (Financial Statements, expected contracts etc.)

## Poor practice examples

- *Failing to consider certain political connections which fall outside the definition of a PEP (e.g. wider family) which might mean that certain customers still need to be treated as HRC and subject to EDD*
- *Failing to record adequately face-to-face meetings that form part of CDD.*
- *Failing to carry out EDD for high-risk/PEP customers.*
- *Failing to conduct adequate CDD before customer relationships are approved.*
- *Over-reliance on undocumented 'staff knowledge' during the CDD process.*

# How far should you extend your CDD?

A client's reluctance to share information about their source of wealth or funds should raise a **red flag**.

## SOURCE OF WEALTH

- **How a customer became wealthy**

- ☐ Was it inherited? From whom? Supporting docs?
- ☐ Was it a lottery win? Proof? e.g. winning ticket
- ☐ Is the client a successful professional person? e.g. bonus
- ☐ Is the client a very savvy investor? e.g. dividends
- ☐ Proceeds from sale of property? Proof?

## SOURCE OF FUNDS

- **Where specifically the funds have come from**

- ☐ Where has the money to be deposited come from? Which jurisdiction?
- ☐ What was the nature of the business deal that generated the funds?



## Source of Wealth:

---

Generic source of wealth descriptions are not acceptable e.g. “savings”, “from family”, “from work”, “lottery”, “profits from investments”, “inheritance”, “business dealing”, “sale of business” or “funds held in Banks” etc. This information is, on its own, considered insufficient as a proof of the legitimacy of wealth.

- Are you convinced that the funds and wealth can be reasonably established to be legitimate?
- Can you independently obtain the evidence of the client’s source of wealth for higher-risk accounts and relationships?
- Are you able to establish or verify the relationship between the client and the third party where accounts are funded by a third party? (restricted to the absolute minimum)
- Do you go all the way in seeking clarity wherever the circumstances are unclear or account structures are complex?

## Source of Wealth:

There is a wide array of sound practices to answer these questions until satisfied that a customer's source of wealth has been corroborated. These could include:

- In-depth interviewing
- Collection of documentary information (e.g. Financial Statements)
- Reference to publicly available information

It is very important however to note that both the data collected and the documentary evidence should be meaningful, sufficient and should not be excessive. Information should be carefully analyzed by exercising relevant commercial and professional judgment, and should be documented in easy to read format, for the regulator or any third person (e.g. another colleague).

Also, it should be noted that resistance or failure of the client to disclose such information or provide relevant documentation could be considered a **RED FLAG**.

# Enhanced Due Diligence (EDD)

---

**EDD:** A greater level of CDD undertaken for high risk entities. It typically involves **independent** verification of information e.g. obtaining audited company accounts

## Indicators for EDD:

- High / Significant risk clients (ie PEPs, Private Banking clients)
- High / Significant risk activities (ie oil trading, online services)
- High risk transactions (ie non intra group lending)

# Enhanced Due Diligence (EDD)

---

## **Before a client is opened in the system check:**

1. Legal & commercial reason for the existence of a complex structure
2. Verification of a client's ID (obtain copies)
3. Economic profile
4. World check etc
5. Counterparties (are they in the same line of business?)
6. Declared Turnover

The above need to be updated at regular intervals.

For all credit transactions check the source and origin of funds.

# Customer Profile - Enhanced CDD measures - examples

- Obtaining **additional information** on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating **more regularly** the identification data of customer and beneficial owner.
- Obtaining additional information on the **intended nature of the business relationship**.
- Obtaining information on the **reasons for intended or performed transactions**.
- Obtaining the **approval of senior management** to commence or continue the business relationship.
- Conducting **enhanced monitoring** of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an **account in the customer's name** with a bank subject to similar CDD standards.
- Obtaining information on the **source of funds** or **source of wealth** of the customer.
- Obtaining information on the customers counterparties.

# Politically Exposed Persons (PEPs)

## FATF Definition

- *PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.*
- *Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.*
- *Close associates are individuals who are closely connected to a PEP, either socially or professionally.*

## 4MLD

- *In one of the situations where enhanced due diligence should always be conducted, namely for politically exposed persons, the Directive has been strengthened to include politically exposed persons who are entrusted with prominent public functions domestically, as well as those who work for international organizations.*



# Identifying PEPs

---

(i) **Natural persons who have, or had a prominent public function in the Republic or in a foreign country:**

1. heads of State, heads of Governments, ministers and deputy or assistant ministers;
2. members of parliaments;
3. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
4. members of courts of auditors or of the boards of central banks;
5. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
6. members of the administrative, management or supervisory bodies of State-owned enterprises.

*None of the categories set out above shall be understood as covering middle ranking or more junior officials*

# Identifying PEPs (cont'd)

(ii) **“Immediate family members” of PEPs** include the following persons:

1. the spouse;
2. any partner considered by national law as equivalent to the spouse;
3. the children and their spouses or partners;
4. the parents.

(iii) **Persons known to be “close associates” of a PEP** include the following:

1. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a person referred to in subparagraph (i) above or who is known to be connected with that person in any other close business relationship.
2. any natural person who has sole beneficial ownership of a legal entity (e.g. a company) or legal arrangement (e.g. a trust) which is known to have been set up de facto for the benefit of the person referred to in subparagraph (i) above.

☐ In case of companies, we should check whether the BNOs, directors, authorised signatories are PEPs.

☐ Where a person has ceased to be entrusted with a prominent public function for a period of at least one year, credit institutions shall not be obliged to consider such a person as politically exposed

# PEPs

- Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs.

*People cease to be PEPs once they are no longer influential. Any decision to declassify a PEP should be made carefully and supported with ample evidence to prove the case. MLCO approval is required to declassify customers as PEPs*

- Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations definition of a PEP (e.g. wider family) which might mean that certain customers still need to be treated as high risk and subject to enhanced due diligence.

*The PEP definition extends to family members who are either blood relatives or connected via civil partnerships. Nonetheless, this should not rule out EDD on a family member who is not a blood relative or civil partner, for example, yet still exerts an influence on the PEP. Any indicators of suspicion should immediately raise alarm bells and trigger further investigations. Although someone may not meet the legal definition of a PEP, they could still pose a high ML/TF risk.*

**Source: FSA 2011 report**

# Definition of Private Banking client for AML purposes

---

- Private Banking clients are considered to be high risk for AML purposes.
- BOC interpretation: a Private Banking client is one that keeps an investment portfolio equal to or greater than EUR200k.

## Factors that may contribute to the vulnerabilities of PB as regards ML

- Powerful clientele
- The high level of confidentiality associated with private banking
- The close relationship of trust developed between relationship managers and their clients,
- A culture of secrecy and discretion developed by the relationship managers for their clients, and
- The relationship managers becoming client advocates to protect their clients.

# Legal Structures and Corporate Vehicles

---

There are numerous types of entities, which

- Legally make businesses
- Own assets
- Sue
- Open accounts at Financial Institutions
- Are used as part of Legal Structures

The main are:

**Corporations**

**Partnerships**

**Trusts**

**Foundations / Private Foundations**

Corporate

} Vehicles

# TRUST

---

A trust is an arrangement where a person (the settlor) gives money or property to another person (the trustee), to be held in trust for the benefit of either the trust's beneficiaries or a purpose recognized by law.

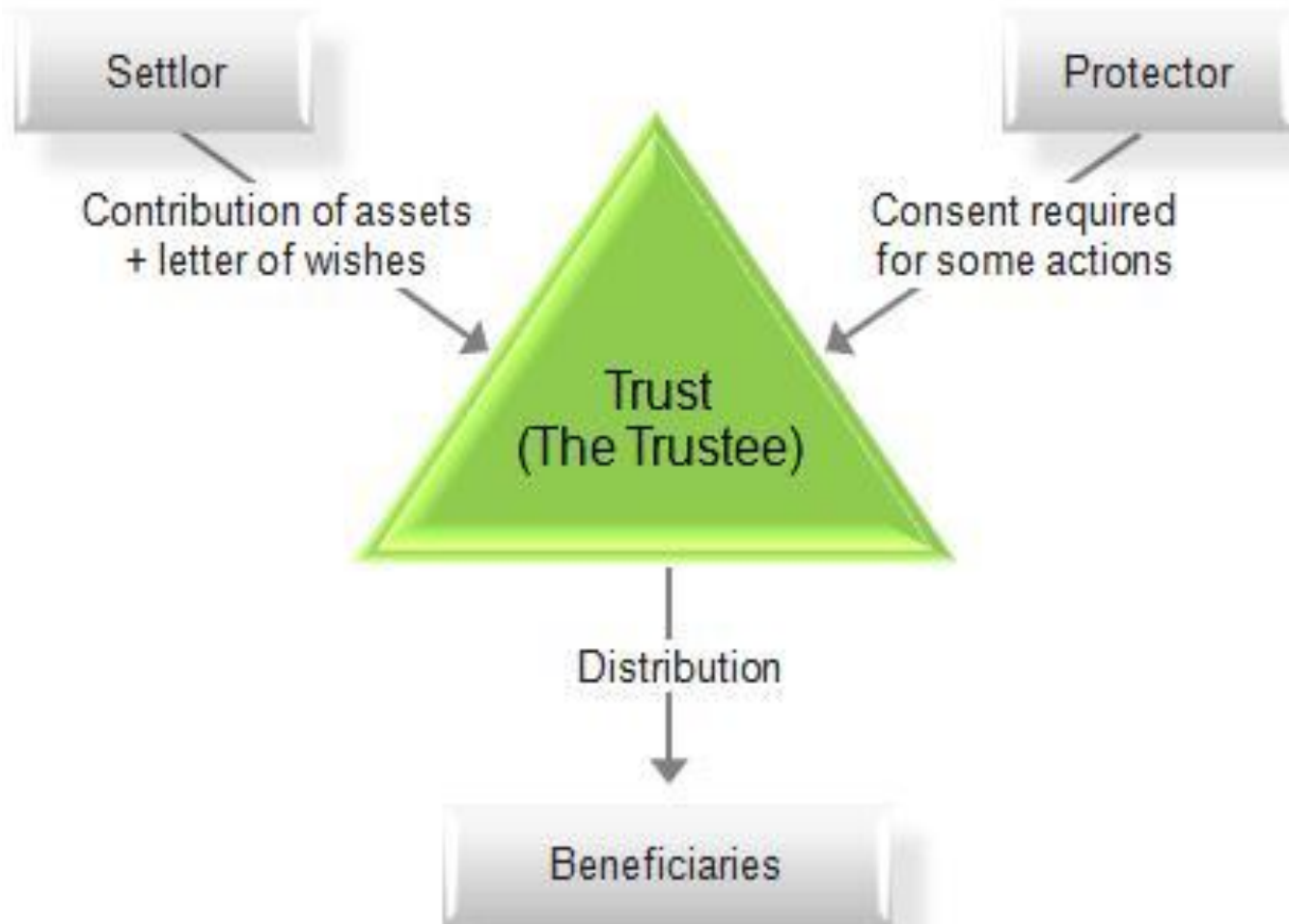
A trust has no “legal personality”, it is not a legal entity.

The Trustee is given legal title to the trust property, but is obligated to act for the good of the beneficiaries.

Trust property can include money, investments, land, buildings, paintings, furniture, jeweler, boats, aircraft, even fine wines.




# TRUST



# Beneficial Owners of a Trust

---

1. Any individual, who has vested interest in at least 10% of the trust property
2. Beneficiaries
3. Any individual who has  **control** over the trust

## Power to:

- Dispose, advance, lend, invest, pay or apply trust property
- Vary the trust
- Add or remove person as beneficiary / trustee
- Withhold veto to any of the above

# FOUNDATION

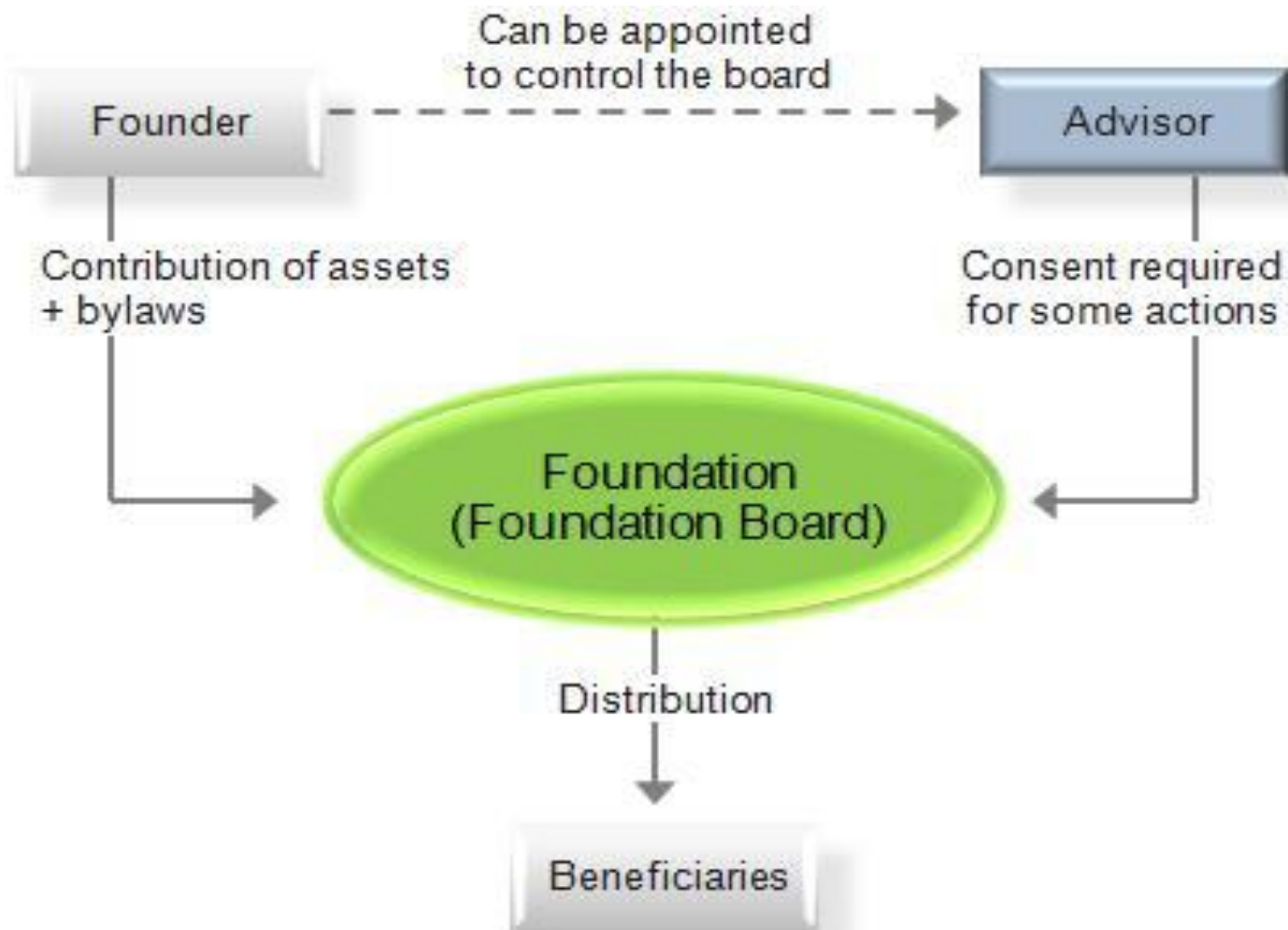
---

The Foundation is a legal entity comparable to that of a company.

The Foundation has constitutional documents in the form of Charter and Bylaws. Assets are held by the foundation for the purposes set out in the foundation's constitutive documents.

There is a Foundation Council/Board, which administrate the assets and is responsible for fulfilling the purpose of the foundation.

# Chart of a PRIVATE FOUNDATION



# Beneficial Owners of Private Foundations

---

Where the individuals that benefit, have been determined:

1. Anyone who benefits from at least 10%

Where the individuals that benefit, have yet to be determined:

2. The class of persons in whose main interest the foundation is set up or operates.
3. An individual who controls at least 10% of the foundation's property.



# RISKS OF TRUSTS, FOUNDATIONS

---

1. Defraud authorities, creditors, commercial disputes
2. Tax evasion vehicle (declaring as charitable)
3. Service providers with no effective AML procedures
4. Dummy Settlor (conceal Identity of the actual Settlor)
5. PEPs (Settlors, beneficiaries)
6. Beneficiaries who are HR charities
7. Assets derived from cash based businesses or connected to gambling, armaments, MSB
8. Settlers / beneficiaries based or conducting business in or through HR countries (AML, sanctions, embargoes...)



## RED FLAGS:

---

- Unexplained relationship between settlor, beneficiaries, controllers, property and 3<sup>rd</sup> parties
- Change of beneficiaries without notifying bank
- Large payments (for unspecified services) to consultants, related parties, employees, etc
- Addition of beneficiary (especially after the death of settlor)
- Level of assets / value of transactions inconsistent with the profile of the client
- Transactions with no link between stated activity and recipient
- Frequent cash deposits/withdrawals by unrelated individuals
- Distribution to PEPs, HR Charities or unregulated organisations

# Sophisticated, Complex Legal Structures

Are used  
by:

- Wealthy individuals
- Successful businesses
- **Criminals**

For:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability
- **Money Laundering**

*\* Refer to OE151 for the definition of a complex structure (BOC interpretation) and procedure to follow during client on-boarding*

## Why are legal structures complicated?

1. **Multiple layers** of ownership with one or **more entities** (in each layer) some of them may be **different in type** incorporated in **different jurisdictions** and may **include trust or PIF**.
1. Existence of services of “nominee shareholders” and “nominee directors”.



Opportunity to launder money, or to move funds to finance terrorism or criminal organizations in **complete anonymity**

# Why are legal structures complicated and Risky?



Shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership which is spread across jurisdictions.



Formal nominee shareholders and directors where the identity of the nominator is undisclosed.



Complex ownership and control structures involving many layers of shares registered in the name of other legal persons.



Informal nominee shareholders and directors, such as close associates and family.



Bearer shares and bearer share warrants.



Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.



Unrestricted use of legal persons as directors.



Use of intermediaries in forming legal persons, including professional intermediaries.

## Money laundering through Real Estate sector

*Classic method* of laundering dirty money, particularly in countries with political, economic and monetary stability.

**Main Reason** → Significant regulatory weaknesses:

1. Brokers/Agents do not perform DD over buyers
2. No reporting requirements (brokers/Lawyers)
3. Foreign company can buy property in any country, without having an in-country presence

## RED FLAGS:

Buying-Selling

REAL ESTATE

Investments

1. Cash deposits
2. Renovation and reselling as high-end property
3. 3<sup>rd</sup> party payment
4. Using a Loan or Mortgage
5. “Reverse flip” or Under valuation
6. Sell the property many times
7. Rent property to generate rental income
8. Overseas ownership

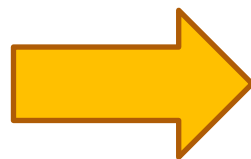


# Trade-Based Money laundering

- One of the most *sophisticated methods* of cleaning dirty money
- Among the hardest to detect

## Methods:

- ☐ Payments to a vendor by unrelated 3<sup>rd</sup> parties
- ☐ Repeated import-export of the same HV commodity
- ☐ Falsifying documents
- ☐ Misrepresenting financial transactions
- ☐ Double invoicing
- ☐ Commodity over or under valuation



Important: almost 80% of TBML is done through normal current accounts, without the use of LCs, bills of exchange etc. Accordingly, IBU staff should be cautious and aware.

## RED FLAGS:

---

1. Significant discrepancies ☐ bill of lading-invoice (authenticity)
2. Significant discrepancies ☐ value on invoice-market
3. Type of commodity shipped VS business activity
4. Size of shipment Vs regular business transactions
5. Goods shipped through jurisdictions and unconnected subsidiaries for no apparent reason
6. Packaging inconsistent with the commodity shipping method
7. Unusual shipping routes or transshipment points





## Reliance on third parties for customer identification and due diligence purposes - Introduction

- Article 67 of the Law permits persons carrying out financial or other business activities to rely on third parties for the implementation of customer identification and due diligence procedures.
- The Law (article 67) explicitly provides that the ultimate responsibility for performing the above mentioned measures and procedures remains with the credit institutions or the person who carries out the financial or other business activities which relies on the third person. Consequently, the responsibility to apply customer identification and due diligence procedures cannot be delegated to the third person.

# Definition of ‘third party’

---

□ A credit or financial institution or auditors or accountants or tax consultants or independent legal professionals or persons providing to third parties trust and company services, governed by the European Union Directive and situated in the European Economic Area or third equivalent country, and who:

(i) are subject to mandatory professional registration by law

and

(ii) are subject to supervision with regard to their compliance with the requirements of the European Union Directive.

□ It should be noted that the term “financial institutions” does not include dealers in foreign exchange.

# Business Associates

---

- Independent Professionals, natural or legal persons, who recommend customers to open accounts with the Bank. Responsibility for the customer identification process and the due diligence procedures remains with the Bank, in accordance with the procedures that are recorded in the relevant circulars.
- The Business Associates are approved by the Manager International Business Network or the Manager International Banking & Wealth Management Services or the Director International Banking & Wealth Management Services.
- Witnessing Agreement needs to be signed by each individual person in the Associates' office who will have the authority to witness customers signatures on all Banking documents.

# Definition of Terrorist Financing

---

By any means, directly or indirectly,

- Unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used in
- Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict
- When the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

*(United Nations 1999 International Convention for the Suppression of the Financing of Terrorism)*

# The Terrorist Financing Process



- Donations
- Self funding
- Criminal activity

- To a terrorist network
- To a terrorist organization
- To a terrorist cell

- Purchase weapons or bomb-making equipment
- Payments for recruitment & training
- Finance living expenses of terrorists

Funds used to finance terrorism are considered an 'instrument of crime' (which are either illicit or legitimate funds directed towards a criminal purpose).

*(AUSTRAC TF report 2014)*

# Differences between ML and TF

	<i>Money Laundering</i>	<i>Terrorist Financing</i>
<b>Motivation</b>	■ Profit	■ Ideological
<b>Source of Funds</b>	■ Internally from within criminal organizations	■ Internally from self-funding cells (increasingly centered on criminal activity)  ■ Externally from benefactors and fundraisers
<b>Conduits</b>	■ Favors formal financial system	■ Favors cash couriers or informal financial systems such as hawala and currency exchange firms
<b>Detection Focus</b>	■ Suspicious transactions, such as deposits uncharacteristic of customer's wealth or the expected activity	■ Suspicious relationships, such as wire transfers between seemingly unrelated parties
<b>Transaction Amounts</b>	■ Large amounts often structured to avoid reporting requirements	■ Small amounts usually below reporting thresholds
<b>Financial Activity</b>	■ Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens	■ No workable financial profile of operational terrorists exists, according to U.S. 9/11 Commission
<b>Money Trail</b>	■ Circular — money eventually ends up with person who generated it	■ Linear — money generated is used to propagate terrorist group and activities

Source: James R. Richards

# Terrorist Financing Red Flags

---

- The stated occupation of the customer is not in line with the type or level of activity in the account.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Fund transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Periods of transaction dormancy, which could be the result of terrorist training or engagement in combat.

# Terrorist Financing Red Flags

---

- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Charitable activity in areas of conflict especially in Syria.
- Client accesses accounts, and/or uses debit or credit cards in high risk jurisdictions, specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Client indicates planned cease date to account activity.
- Client or account activity indicates the sale of personal property/possessions.
- Client depletes account(s) by way of cash withdrawal.
- Sudden settlement of debt(s) or payments of debts by unrelated 3rd parties.



# Direct operational cost of Terrorist Attacks (Estimates)



<i><b>Attack</b></i>	<i><b>Date</b></i>	<i><b>Cost</b></i>
London Transport System	July 7, 2005	GBP 8,000
Madrid Train Bombings	March 11, 2004	US\$ 10, 000
Istambul Truck Bomb Attacks	Nov. 15 & 20, 2003	US\$ 40,000
Jakarta Marriot Hotel Bombing	August 5, 2003	US\$ 30,000
Bali Bombings	October 12, 2002	US\$ 50,000
USS Cole Attack	October 12, 2000	US\$ 10,000
East Africa Embassy Bombings	August 7, 1998	US\$ 50,000
9/11	September 11, 2001	US\$ 500,000

# Real – Life Case: The 9/11 Terrorist Attacks

---

- Funding for the 9/11 terrorist attacks has been estimated at a total cost of somewhere between \$400,000 and \$500,000. The 24 accounts of the 19 hijackers carried average balances of only \$3,000 to \$5,000. The wires in and out of the accounts and the other activity was relatively modest and not suspicious.
- However, the accounts were opened with visas from foreign countries; the account holders were not permanent residents; many accounts had the same address and phone number; most addresses used were not permanent addresses, but mail boxes, and were changed frequently; there were frequent international wires in and out of the accounts; there were numerous balance inquiries; there were immediate withdrawals after deposits were made; and ATMs were frequently used, and often by individuals who did not own the accounts.

# What are Sanctions?

---

Sanctions are

- unilateral or multilateral
- economic actions
- taken against a target
- to influence their actions.



Four primary things sanctions prohibit or restrict:

- Diplomatic
- Financial
- Trade
- Travel

# Who issues Sanctions?



**In the United States sanctions are issued by the Office of Foreign Asset Control (OFAC) or the Bureau of Industry & Security (BIS).**



**United Nations (UN) Resolutions can result in sanctions. If you live in a UN member state you are likely to be subject to UN Sanctions.**



**The European Union (EU) also issues sanctions which are enforced by each EU member state**

**Any country can impose unilateral sanctions on any other territory.**

# EU Sanctions

---

## General

- The European Commission proposes restrictive measures and adopts a Common Position.
- Sanctions are given effect in Council Regulations, Council Decisions and Commission Regulations.
- Sanctions are then enforced by Member States.

## EU Sanctions apply to:

- Everyone in the EU, including foreign entities or individuals acting in the EU.
- Imports to or exports from the EU.
- EU registered companies and citizens anywhere in the world

# OFAC Sanctions

---

## General

- The US Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces US economic and trade sanctions.
- OFAC sanctions generally prohibit:
  - Transactions with, payments to or investments in entities located in a country/ies that is/are subject to an OFAC embargo.
  - Transactions with, payments to or dealings with persons or entities identified on OFAC Specially Designated Nationals (SDN) List.

OFAC SDN List: ([www.treasury.gov/resource-center/sanctions/SDN-List](http://www.treasury.gov/resource-center/sanctions/SDN-List))

- List of roughly 4,000 entities– terrorists, drug traffickers and others
- Includes individuals, entities, vessels and aircrafts
- Frequently updated

## OFAC Sanctions (cont.)

---

### OFAC Sanctions apply to:

- Everyone in the US, including foreign entities or individuals acting in the US.
- Imports to or exports from the US.
- US companies, including foreign offices or branches, anywhere in the world.
- US citizens or permanent residents anywhere in the world, even if working for a foreign company.

# Sanctions Type & Scope

Sanctions can be:

- 1) **Specific** ☐ Relate to specific lists of named individuals, legal entities, organizations etc
- 2) **General** ☐ Cover all transactions with certain countries / jurisdictions, all transactions within a certain area of activity etc
- 3) **Sectoral** ☐ Cover certain parties in specific sectors, but only restrict certain type of transactions





## Sanctions Vs AML

---

### Sanctions

- Strict or Absolute Liability
- Real Time
- No value thresholds
- Controls mitigate severity of fines for a violation
- Targets prescribed by law

### AML

- Reasonableness
- Look back
- Risk based thresholds
- Controls determine whether violation occurred
- Targets identified by red flags & typologies.

# Sanctions Evasions

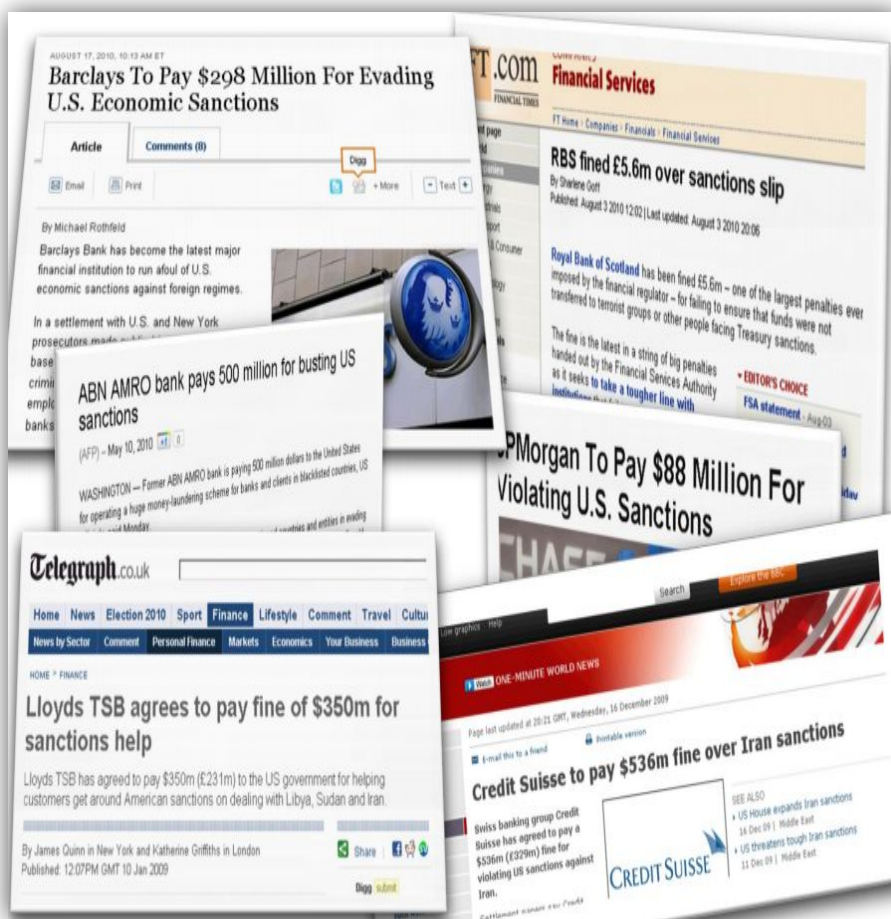
---

- Forgery of documents
- Nested accounts
- Stripping wires
- Restructuring of corporate entities
- Re-routing of transactions
- Withholding or providing false information
- Using client accounts to conceal origin of funds



# Sanctions & Embargoes

Regulators are very serious – fines can be huge:



Year	Entity	Penalty
2009	Lloyds TSB Bank	\$217,000,000
2010	Barclays Bank plc	\$176,000,000
2012	ING Bank N.V.	\$619,000,000
2012	Standard Chartered Bank	\$132,000,000
2012	HSBC Holdings, Inc.	\$375,000,000
2012	Bank of Tokyo-Mitsubishi UFJ, Ltd	\$8,571,634
2013	Royal Bank of Scotland plc	\$33,122,307
2014	Clearstream Banking S.A.	\$152,902,000
2014	Bank of Moscow	\$9,492,525
2014	BNP Paribas S.A.	\$963,619,900
2015	Commerzbank A.G.	\$258,660,796
2015	Credit Agricole	\$329,593,585
2016	Barclays	\$2,485,890

# Effective Transaction Monitoring

---

## Article 58(e) of the Law

**What is required is a** “detailed examination of each transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose”

# Effective Transaction Monitoring

---

- In practice, where a client's instruction or transaction or behavior is not consistent with what is anticipated i.e. if it does not make sense or appears logical then an explanation must be sought by contacting the client.
- If there are unexpected jurisdictions or organizations/ counterparties/ associates involved, again explanations should be sought.
- It should be noted that failure to provide satisfactory answers or cancelling transactions when pertinent questions are asked are reasons for concern.
- One main method for documenting the exercise of judgment/reasonableness during ongoing transaction monitoring is the collection of sufficient (not excessive) supporting documentation, which should be kept in the client file.

# CUSTOMER REVIEW PROCESS

---

Financial regulators require banks and non-banking financial institutions to perform AML KYC due diligence when onboarding a new customer and also on a periodic basis throughout the life of the relationship.

Periodic KYC CTF reviews are conducted on a periodic basis:

- to ensure that existing customer information is kept updated.
- to confirm that each customer's assigned risk rating continues to reflect the appropriate AML risk rating.
- to capture any material change in the customer's profile or any potentially suspicious activity that was not detected by the firm's real-time transaction monitoring platforms.

# CUSTOMER REVIEW PROCESS

---

A review should be performed when an unusual and/or significant transaction takes place, when the customer documentation changes substantially or when there is a material change in the way the account is operated. Events for review may include changes in the legal/ownership structure, new accounts, dormant accounts, changes in risk category, negative information (internet, press, regulator, MOKAS, foreign bank) etc.

When a client is being reviewed, one should ask himself/herself: “if this customer had come to me today, in this form, is this the KYC/CDD information that I would have asked for? Or had I known then what I know now, would I have asked for more information or different information?”

In other words, is the KYC/CDD information that the organization holds on the customer still appropriate and proportionate to the money laundering risk now presented by that customer?.

# CUSTOMER REVIEW PROCESS

---

- Review each customer's information: name, address, ID number, certificate of good standing (if applicable), and the customer's original information to determine if there are any material changes
- Check customer file for insufficient information – request updated documents from client
- Rescreen each customer's information against specially designated and country-based sanctions lists (OFAC lists)
- Periodic VS circumstantial (large transaction, change in legal/ownership structure, change in signatories, new accounts, dormant accounts)
- In instances where there is a substantive change (i.e., a different country of residence), reassess and reapply the risk rating for that customer
- Re-evaluate cooperation - *exercise judgment!*



# CUSTOMER REVIEW PROCESS

---

- The number of enquiries received from Correspondent Banks
- The number of filtering alerts handled during the period examined
- Determine any potentially suspicious activities that were not detected by the Bank's real-time transaction monitoring platforms.
- Change in risk category can also be due to negative information (internet, press, regulator, MOKAS, another bank)
- Important to evaluate the quality of supporting documentation provided
- The level of responsiveness and willingness of the client to provide additional supporting documentation or clarification when requested
- If a client refuses to provide information the Bank should consider terminating the relationship, closing any accounts, filing a suspicion report.

*Frequency: Once a year for high risk clients, every two years for significant risk clients, every three years for medium risk clients, every five years for low risk clients*

# CUSTOMER REVIEW PROCESS

---

## Transaction Monitoring during the review:

Need to check that the transactions processed in the period examined:

- Are in line with the nature of transactions that relate to the declared business activities
- Involve counterparties, both for in/out funds, that match the declared ones and if not, discuss with the clients to seek explanation and, if necessary, update their profile accordingly
- If the actual turnover is in line with declared / historic turnover
- Involve reasonable amounts that can be expected for the kind of business activities that the clients are engaged in – REASONABLENESS & JUDGEMENT

# A SAR is born!

---

- All should be aware of when and how to submit a suspicion report
- They should understand that if they have reason to suspect that a person may be involved in money laundering or have relevant information it is their duty to report it to the designated MLCO (Suspicious Activity Report - SAR) => protect themselves and protect their organization
- Delaying or not performing a transaction is not illegal if the client refuses to provide the necessary information / comfort or where there is a reason to suspect illegal or fraudulent actions
- Serious tax offence (element of fraud) has been included in the law as a predicate offence (punishable with imprisonment exceeding one year) to money laundering charges
- The MLCO should encourage appropriate reporting – quality of SARs is the clearest demonstration of an effective AML program
- SARs should be made in good faith and genuine suspicion – protected by the law – defensive, malicious or frivolous SARs are not welcomed

# The “Suspicion Spectrum”

Comfort...curiosity.....unease.....doubt.....concern.....suspicion.....knowledge

- It is important to understand the above so that there is comfort when making a suspicion report
- For example, a client that “looks untrustworthy” should not be a foundation for suspicion
- BUT, a client that was uncomfortable when asking to respond to routine CDD questions, should be considered a foundation for suspicion
- Not requested to confirm beyond doubt that assets or funds may represent the proceeds of crime....a suspicion of criminality in general is sufficient
- But does the suspicion have a rational foundation?
- If you decide not to report and there is money laundering can you explain your decision NOT to report?

# CONCLUSION – Golden Rules

---

*READ THE BANK'S POLICIES & PROCEDURES and IB&WM GUIDANCE – be informed*

*USE YOUR JUDGEMENT – don't be passive*

*DOCUMENT YOUR JUDGEMENT – if you didn't document it, it's like it never happened!*

*IF YOU DON'T KNOW SOMETHING OR IF YOU ARE NOT SURE THEN ASK!*

*Do the Right Thing!*

**THANK YOU!**