

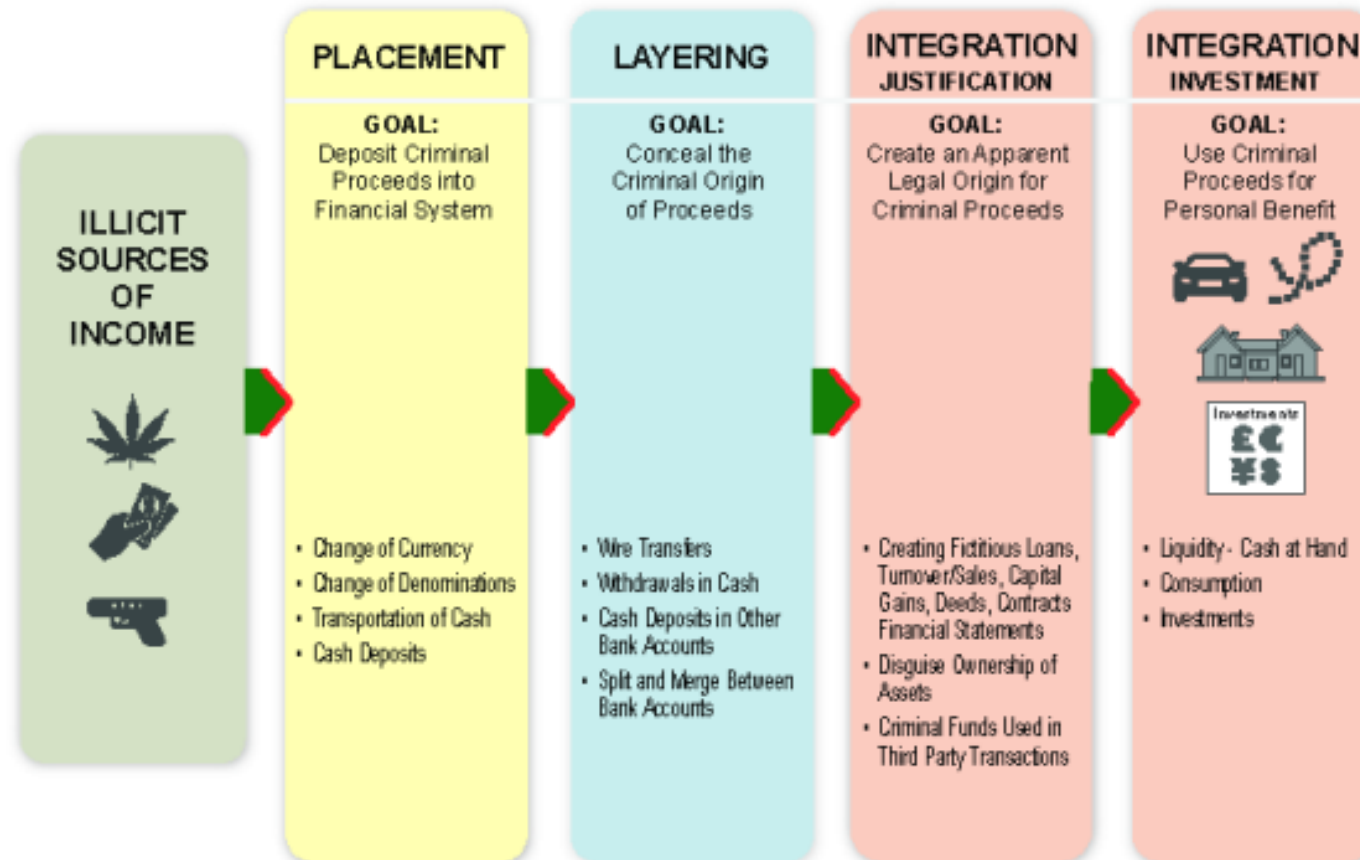
# MONEY LAUNDERING WHAT IT LOOKS LIKE

# Money Laundering Stages

---



# Money Laundering Stages



# Laundering Criminal Property

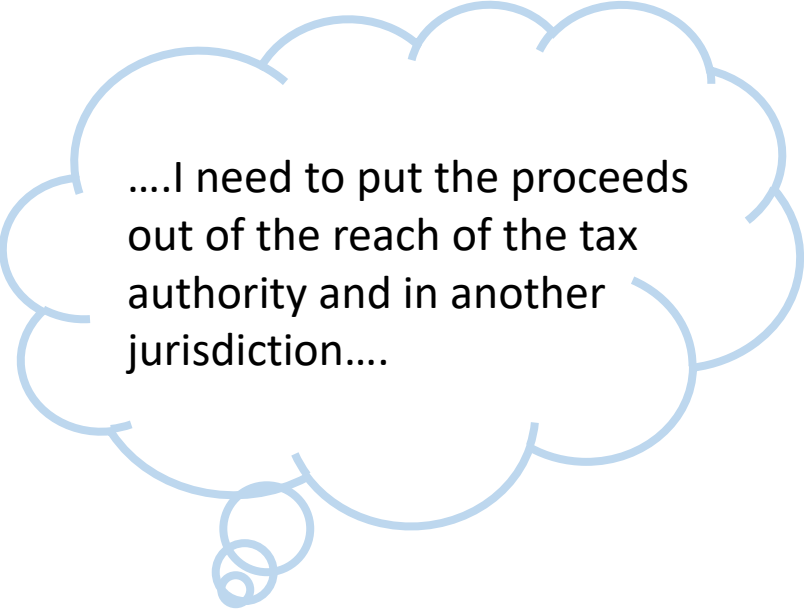
---

Placement-Layering-Integration

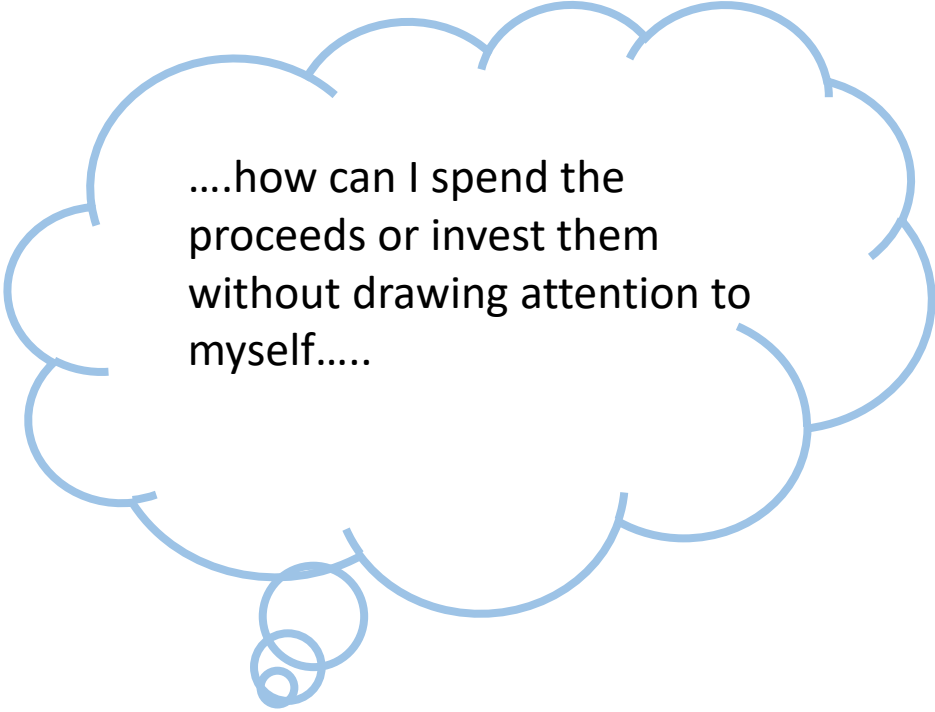
*or*

Enable-Distance-Disguise

\*ref 'Criminal Capital' – Stephen Platt



....I need to put the proceeds out of the reach of the tax authority and in another jurisdiction....



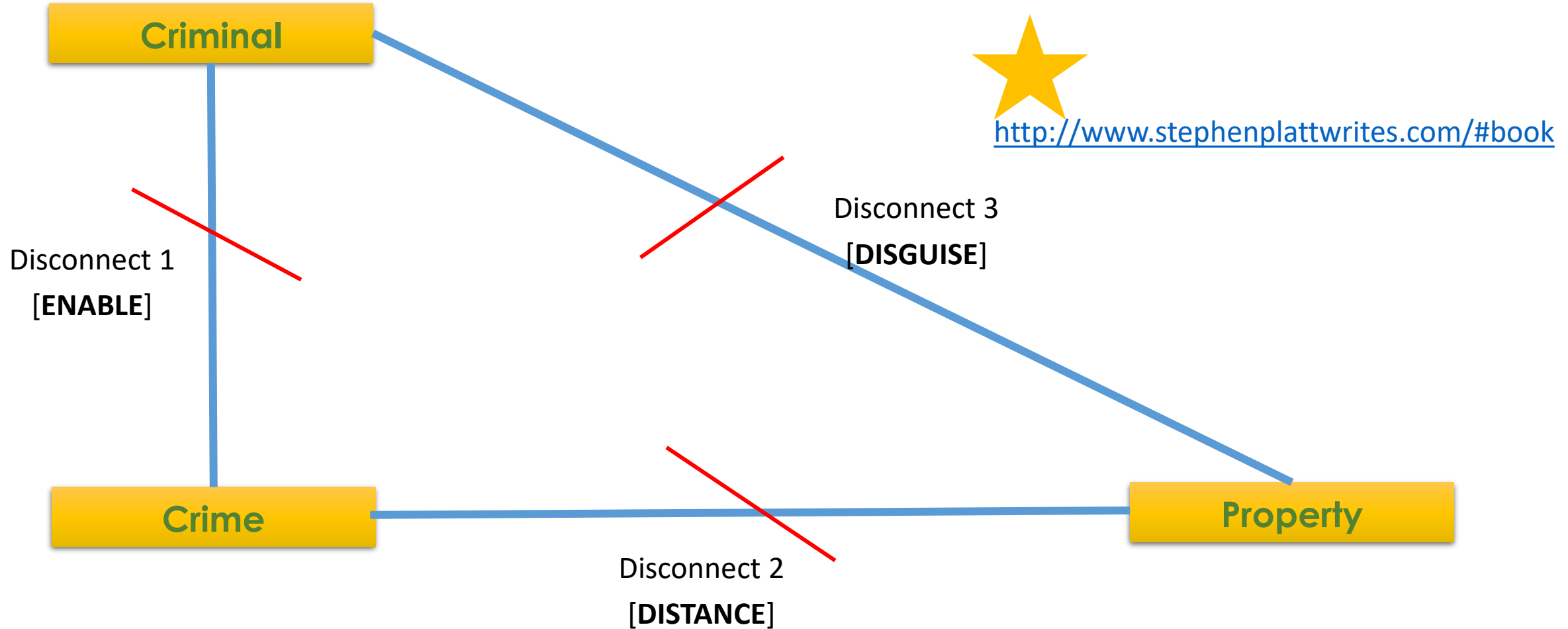
....how can I spend the proceeds or invest them without drawing attention to myself.....

# Stephen Platt's model

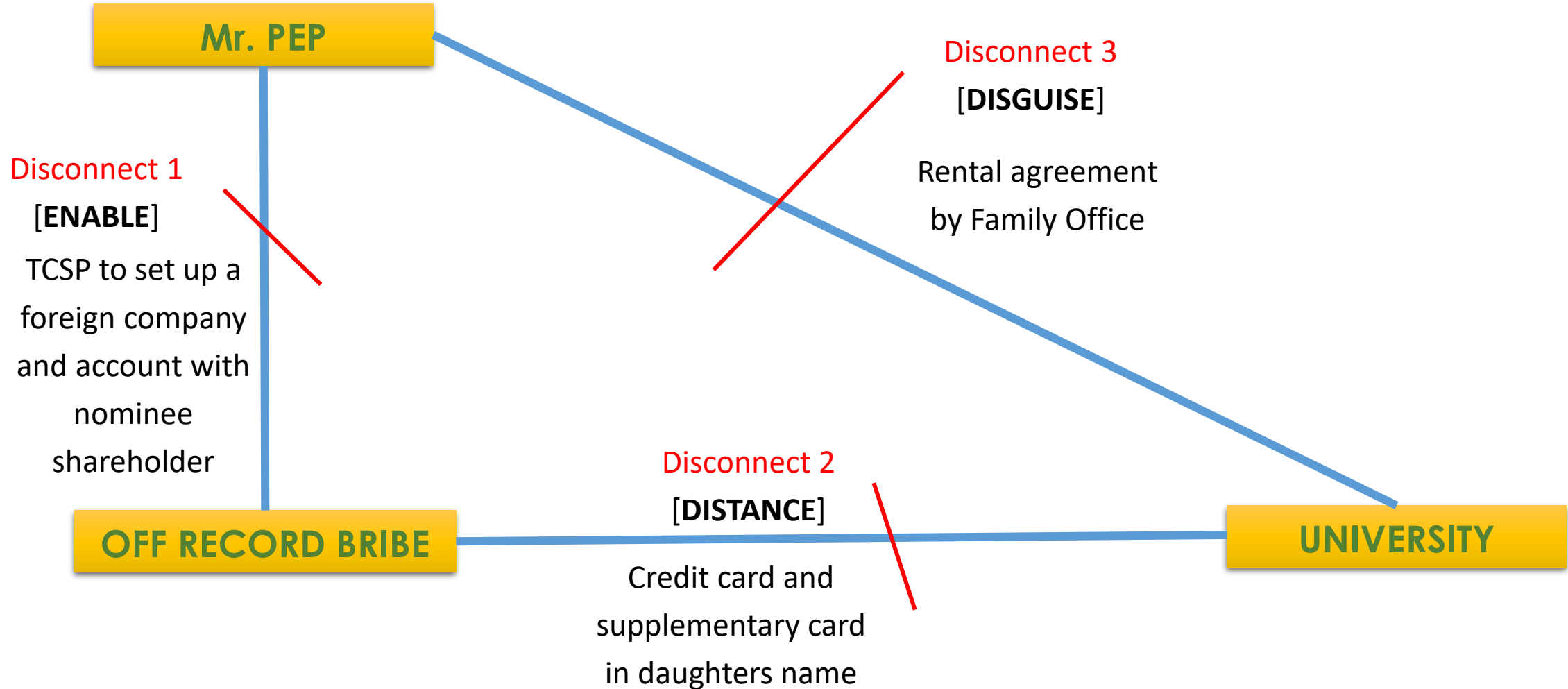
---

- **ENABLE** – set up a shell company, with a nominee director in a country with poor regulations.
- **DISTANCE** – open a company bank account in another similar jurisdiction, use TBML to transact. Company purchases a luxury asset.
- **DISGUISE** – set up a trust for the ownership of the asset for use by tax criminal.

# Where's the 'placement' in IFCs?



# Example of model



# “Criminal Property”

---

Property is criminal property if –

- (a) it constitutes a person’s benefit from **criminal conduct** or it represents such a benefit; and
- (b) the alleged offender **knows or suspects** that it constitutes or represents such a benefit, and includes terrorist property

If the person is in possession of criminal property  
– they could be charged with money laundering  
in addition to other offences



# Anwoir – points to prove

---

- ▶ Previous convictions and bad character
- ▶ Association evidence
- ▶ Drug contamination
- ▶ Covert meetings
- ▶ Transaction make sense?
- ▶ Anti-surveillance tactics
- ▶ Unexplained cash in accounts
- ▶ Legitimate income versus expenditure
- ▶ Provable lies or false records

# ILLICIT ACTIVITIES

CONVERTING

ARRANGEMENTS



ACQUISITION

CONCEALING

# ILLICIT ACTIVITIES

# Three Main Money Laundering Offences

## **Concealing etc**

---

- ▶ Concealing
- ▶ Disguising
- ▶ Converting
- ▶ Transferring
- ▶ Removing from the country

# Three Main Money Laundering Offences; **Arrangements**

---

- ▶ If a person –  
enters into or becomes concerned in an arrangement  
which that person knows or suspects  
facilitates (by whatever means)  
the acquisition, retention, use or control of **criminal property** by or  
on behalf of another person.

# Three Main Money Laundering Offences; **Acquires**

---

- ▶ A person commits an offence if that person –
  - (a) acquires **criminal property**;
  - (b) uses **criminal property**; or
  - (c) has possession of **criminal property**.

# Offences

---

Female A sells ganja up in a car park

A traffic stop results in her getting arrested in a Mercedes with a decent amount of weed. The Mercedes is registered to her boyfriend, Mr. Biggy

Her mobile telephone is analysed. Her messages include:

*“biggy – get the Merc. Use dollar from them stems that I dropped in u account & put only in ur name. Luv u, honey”*

# Offences

---

Male A falsely declares USD \$50,000 in income to the tax authorities for the reporting period

He actually received USD \$75,000 as income

He transfers the additional USD \$25,000 to his unemployed wife to look after it and promises to take her on a cruise

# Offences

---

Bank employee receives a complaint from a victim who informs them that they hold his stolen funds from an investment fraud in Canada that he got scammed by

The bank becomes concerned and transfers the funds to another account in a different country and then exits their relationship – the MLRO said this is the best way of dealing with it



# Offences

---

Accountant agrees with a suspect to falsify VAT returns for a company and hides a number of invoices

The accountant doesn't make a suspicious activity report to the Financial Intelligence Unit

The suspect withdraws the cash from his account and goes on a 3 month trip to Greenland, spending over USD 15,000 on jewellery and entertainment

# Who are the ML suspects?

---

- ▶ Main target?
- ▶ Associates?
- ▶ Family members?
- ▶ Company?
- ▶ Financial Institution?
- ▶ Money Laundering Reporting Officer?
- ▶ Compliance Officer?

*Question. Did they:*

1. Corroborate
2. Critically Assess
3. Scrutinise



# Money Laundering investigations

---

- ▶ Know the main offences and what to prove
- ▶ Failing to report to the FIU, prejudicing and 'tipping off'
- ▶ Calculate the benefit of offending (keep under review)
- ▶ Primary law, secondary law, guidance and policies – RESEARCH
- ▶ Get technical – understand the terms – they are specific
- ▶ Always identify assets and bank accounts

# So where can we use financial information.....?



1 Tracing the locations of  
Persons of Interest

2 Identifying different types of  
criminal offences

3 Identifying motives,  
associations and links

4 Identify use of other services,  
phones, transport, amenities

5 Locating or identifying  
suspects, witnesses, victims

6 Providing information on  
suspects movements

7 To deal with prolific or  
priority offenders

8 Identify criminality – fraud  
and counterfeiting

9 Preventing and detecting  
crime

10 Identifying realisable assets  
and criminal property

Mike Tyson:

“Everybody has a plan until they get punched in the mouth”

# Using financial information as part of the investigative strategy

---



Identify the most appropriate line of enquiry to pursue

Determine the objective of pursuing a particular line of enquiry

Identify the investigative action necessary

Conduct investigative action, gather maximum material which may generate other enquiries



# The National Decision Model

---

## “CIAPOR”

Code of Ethics

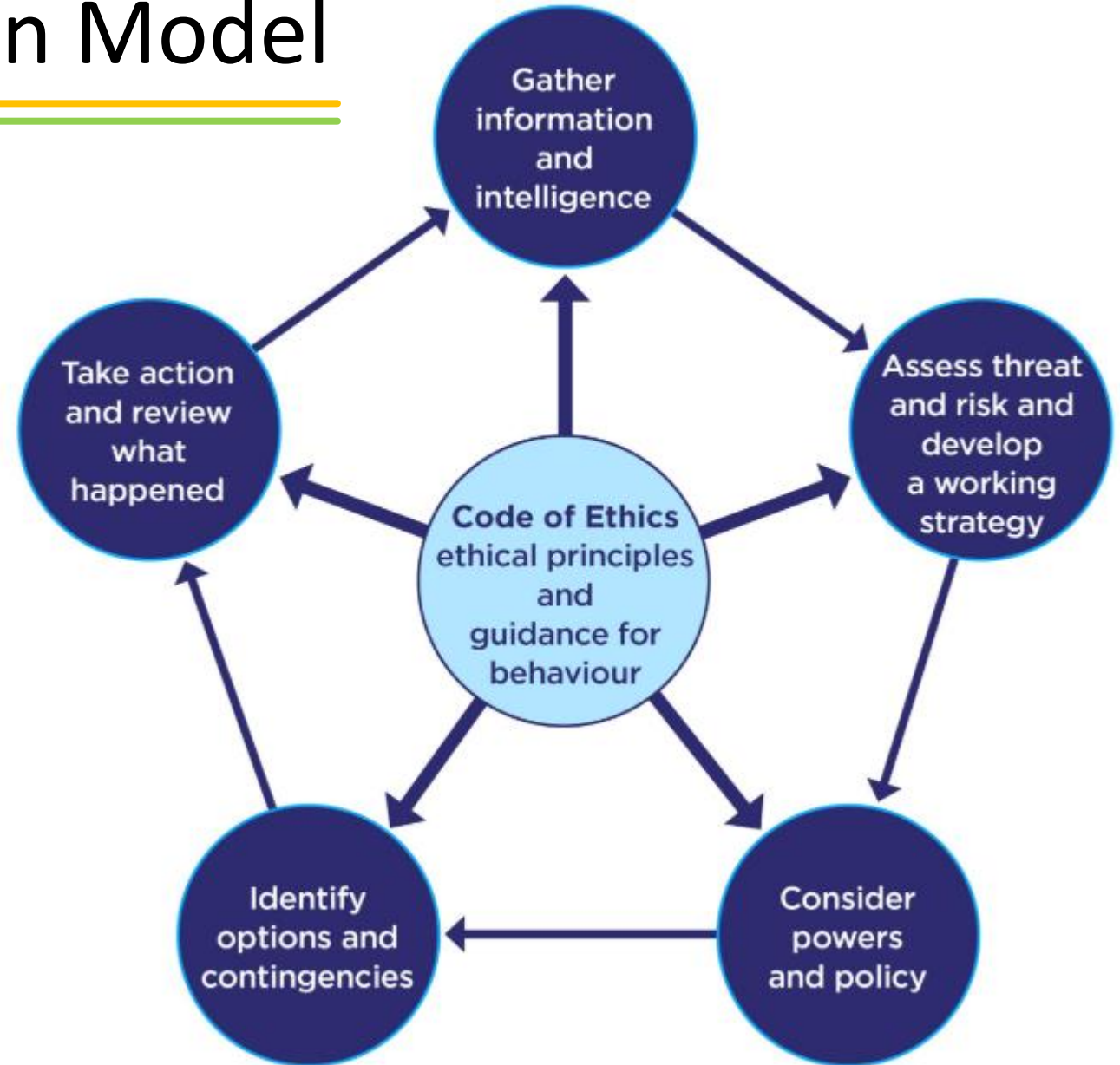
Information

Assessment

Powers and policies

Options

Action and review





# SAFCOM

---

- ▶ SITUATION
- ▶ AIM
- ▶ FACTORS
- ▶ CHOICES
- ▶ OPTION
- ▶ MONITORING

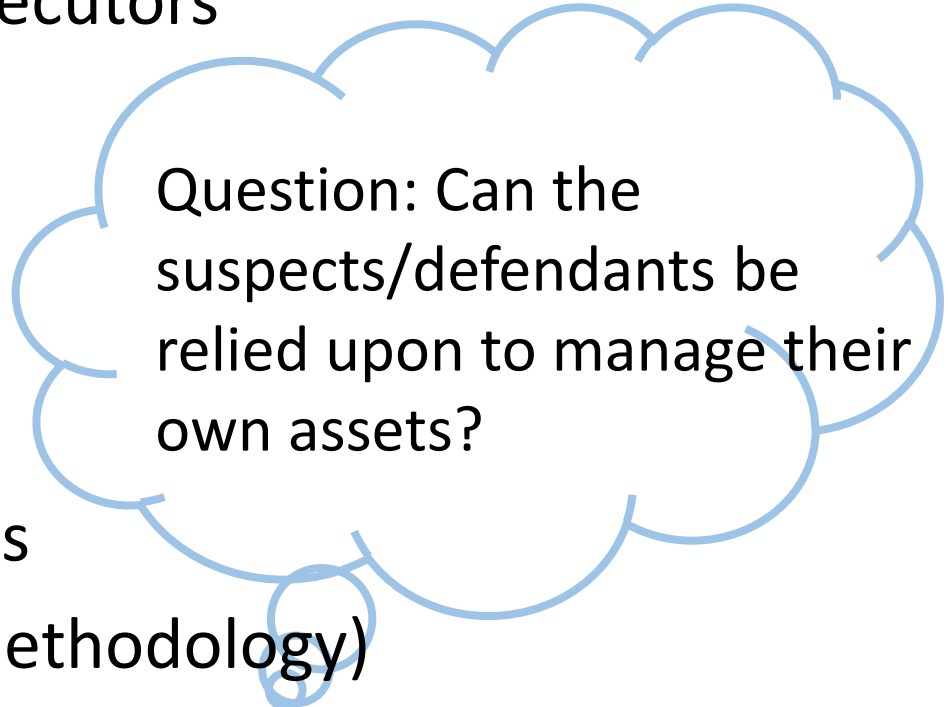


Help, decision  
time!!!

# Money Laundering Strategies

---

- ▶ Develop early written strategies with Prosecutors
- ▶ Think laterally – SWOT analysis
- ▶ Use powers.....effectively
- ▶ Evidence wealth at searches
- ▶ Plan and conduct financial interviews
- ▶ Obtain evidence – use charts and diagrams
- ▶ Asset recovery strategy (FATF change to methodology)
- ▶ Consider and obtain restraint



Question: Can the suspects/defendants be relied upon to manage their own assets?

# Financial interviewing exercise

---



10 minutes exercise – fill up your knowledge bins!

# Financial interviews

---



- How many properties
- Mortgage providers
- Deposit amount
- When bought
- Intending to sell
- Rentals – how?



- Employer
- Roles
- Dates from
- How much
- Payment method
- Pension providers



- Which banks
- Balances
- Joint accounts
- Signatories
- Opening dates
- Types of account

# What do orders mean.....PRIZES!

---

Production Orders

Account Monitoring Orders

Customer Information Orders

Search and Seizure Warrants

Disclosure Orders

Property Freezing/Forfeiture Orders

\*Restraint Orders

Cash Detention/Forfeiture Orders



# Banking Material Schedule

## Training Example (not real)

Institution	Account Name	Account Number	Location	Description	Value	Date Opened	Date Closed	Material obtained	Dates from /to	Exhibit reference	Comments
Fremanistan National Bank	AN Other 1	11112222	Fremanistan	Personal	\$ 6,000,000	5-Feb-19	Open	No			Details received from FIU (INTELLIGENCE ONLY) Requires AMO
Royal Fremanistan Bank	AN Other 2	33334444	Fremanistan	Personal	\$ 253,000	13-Mar-19	Open	No			Details received from FIU (INTELLIGENCE ONLY)
Fremanistan National Bank	COMPANY LIMITED 2	55556666	Fremanistan	Business	\$ 500,000	10-Apr-15	Open	No			Results from Egmont enquiry (INTELLIGENCE ONLY)
Fremanistan National Bank	COMPANY LIMITED 2	77778888	Fremanistan	Business	\$ 0	23-Jul-18	23- Aug 18	No			Details received from FIU (INTELLIGENCE ONLY)
Royal Fremanistan Bank	AN Other 1	99990000	Fremanistan	Personal	\$ 100	5-Feb-19	Open	Yes	11/02/19 to 30/04/21	DB1	Analyzed and scheduled

Record every bank account number  
that you identify from the investigation  
and intelligence material

# Asset Schedule

## Training Example (not real)

Description	Owner	Value	Purchase price	Currency	Date Acquired	Evidence obtained	Recovery Strategy
Property #12, Lets Be Avenue,	AN Other 1	\$ 1,500,000	\$ 1,250,000	USD	19/10/2020	Registrar Details obtained	Restraint to be considered
Safety Deposit Box with Fremanistan National Bank	AN Other 2	Not known			01/06/2021	From Bank Production Order	Search warrant to be considered
100% shareholder in AN Other Inc company in Fremanistan	AN Other 1	Needs valuation	\$ 50,000	USD	30/05/2021	Company records	Restraint to be considered
Vehicle with VRN 123-456	AN Other Inc	\$52,000	\$100,000	USD	11/01/2021	Dealership paperwork obtained	Seizure and restraint to be considered
Bank Account Balance of 1111-2222	AN Other Inc	\$6,000,000	-	USD	05/02/2019	No	Requires a AMO application and restraint
Cash seized under civil recovery regime	Daughter of AN Other 1	\$9,999 and \$50,000	-	USD	-	Customs seizure, tax statements obtained	Cash Forfeiture Order
Rolex watch	Wife of AN Other 1	\$35,000	\$50,000	USD	03/05/2021	Purchase invoices, tax statements	Civil Recovery Order

What's your plan B?

# Value Added Tax Frauds

---

- ▶ EU assessed that EUR 61 billion lost in VAT
- ▶ International engagement through tax agreements vital
- ▶ Benefits and analysis of e-invoicing
- ▶ Missing trader or carousel fraud
- ▶ Small high-value items
- ▶ Legislative changes often required to combat threat
- ▶ Important to follow the money, not the invoices!
- ▶ Often involves Trade Based Money Laundering (TBML) schemes
- ▶ Legal person involvement

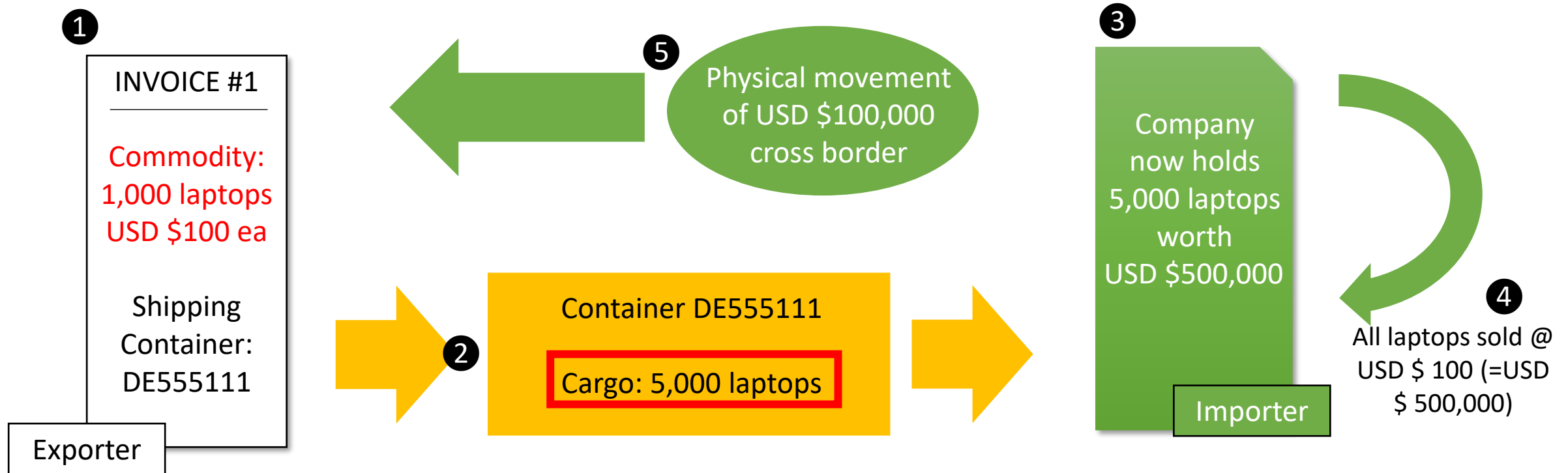


# Trade Based Money Laundering (“TBML”)

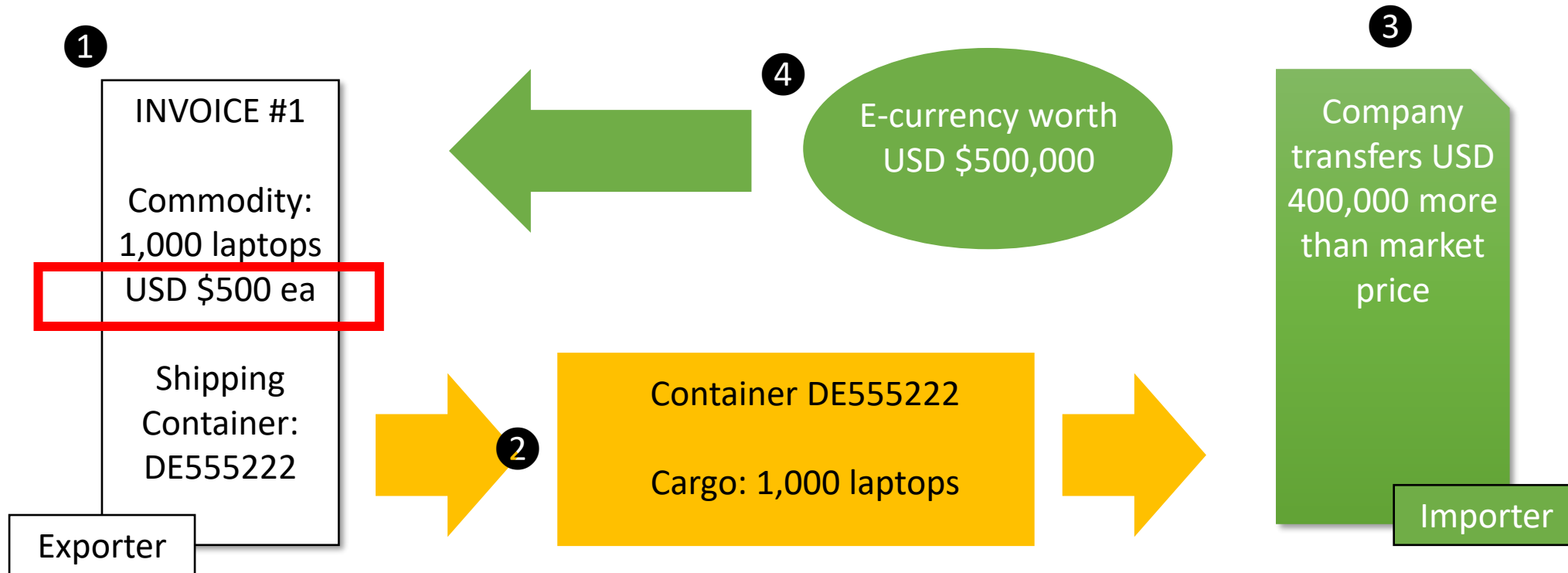
---

- ▶ “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins”
- ▶ Aim is not necessarily the movement of goods but the movement of money, which the trade transactions facilitate
- ▶ Also used to disguise the movement of value in an attempt to finance terrorism, whether from legitimate or illegitimate sources (“TBTF”)

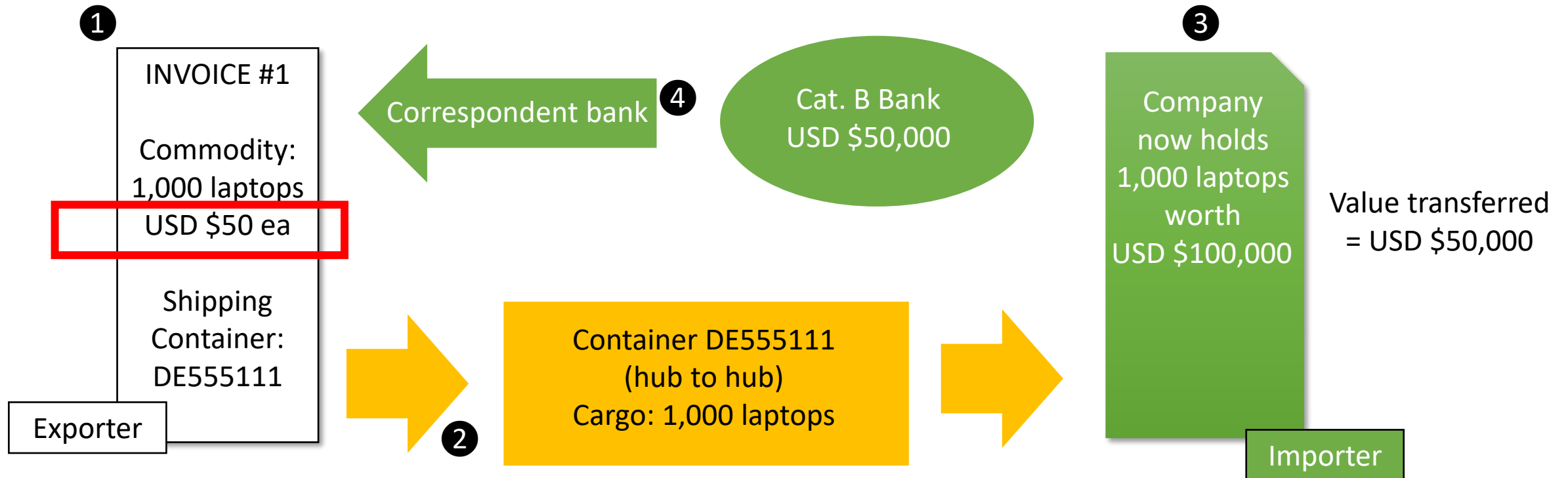
# Under-invoicing / Over-shipment



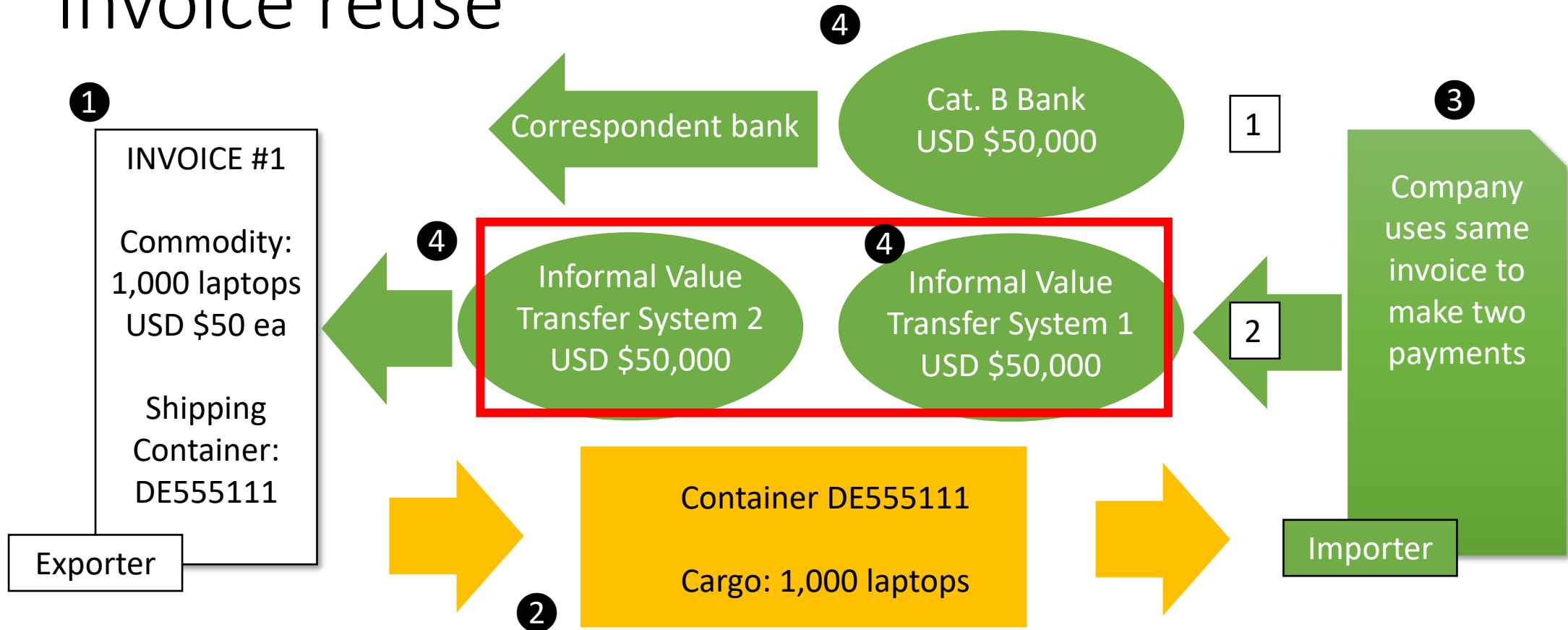
# Over-valuation of goods



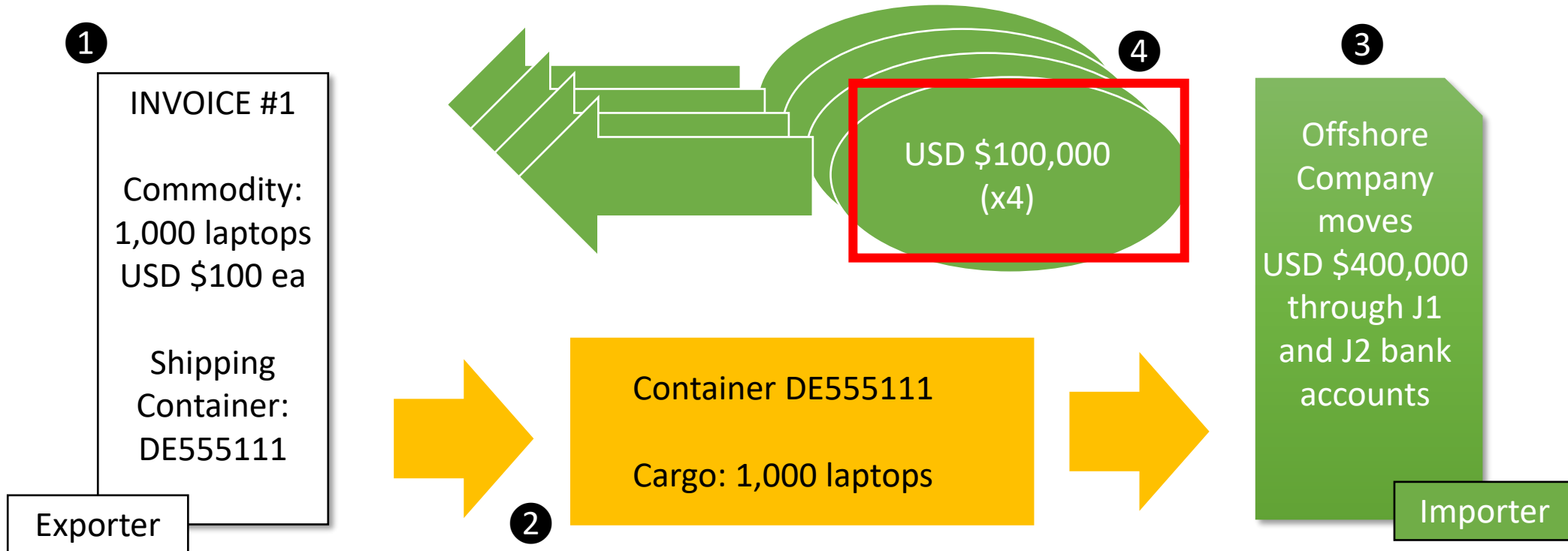
# Under-valuation of goods



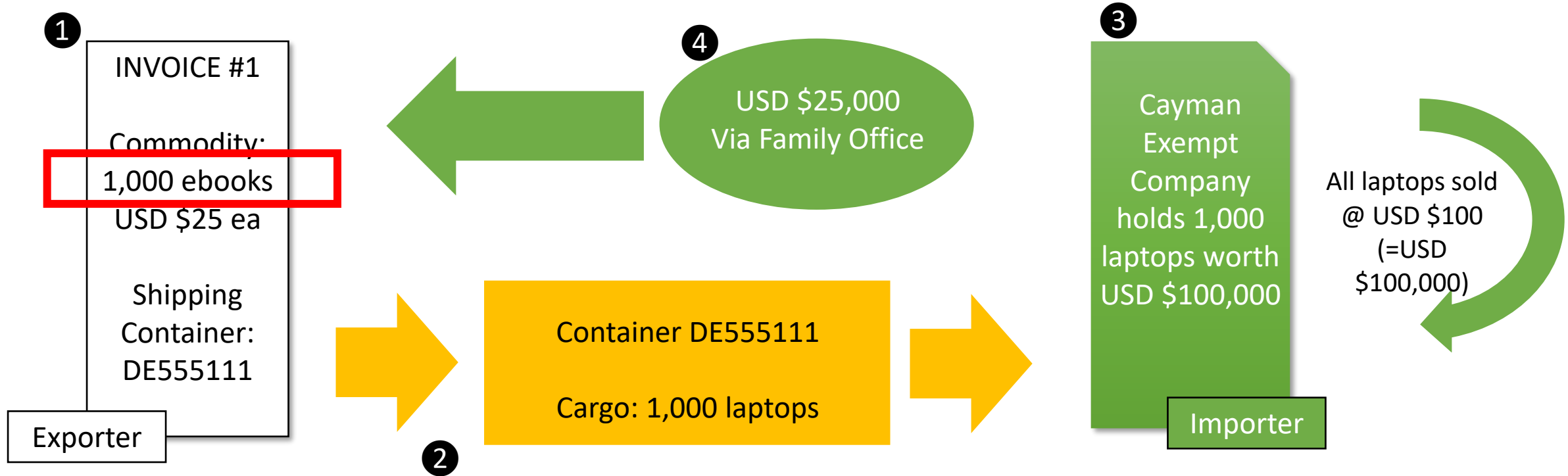
# Invoice reuse



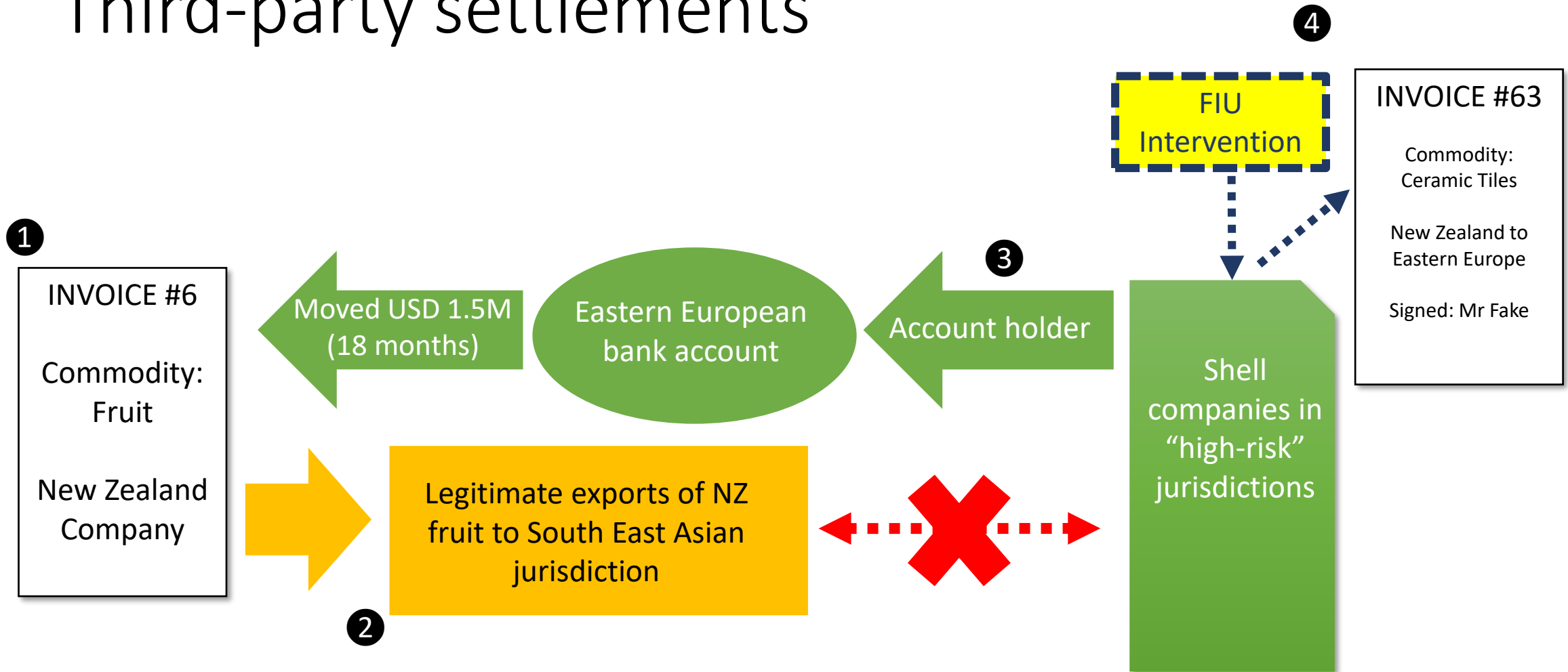
# Multiple invoicing of goods



# False declarations / False invoicing



# Third-party settlements



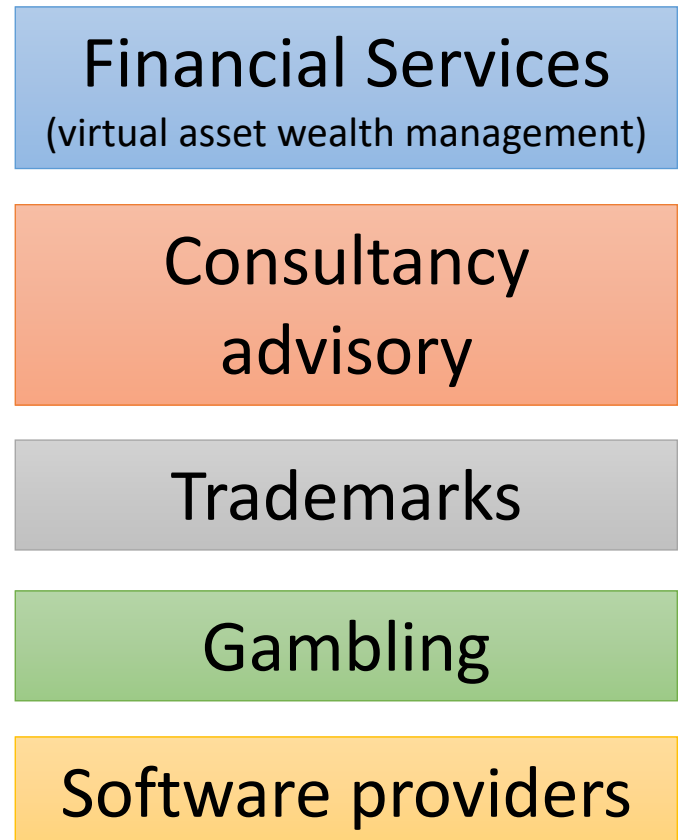


# Services-Based Money Laundering

---

- Recognised as an increasing risk
- SBML schemes rely on exploiting trade in services or other intangibles
- Difficult to assess the legitimacy of the relationship between purchaser and provider
- No physical commodity, no export data

↓ Vulnerable Sectors/Services ↓



# Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures

---

December 2024

# Europol's Key findings

---

- ▶ 85% of the most threatening criminals abuse legal structures
- ▶ Used to support, disguise, facilitate and launder
- ▶ Susceptible to exploitation – knowingly or not
- ▶ Criminally owned = high threat
- ▶ Employees, managers and executives exploit their positions
- ▶ Borderless phenomenon
- ▶ Can serve multiple criminal networks

# Legal Persons – why are they abused

---

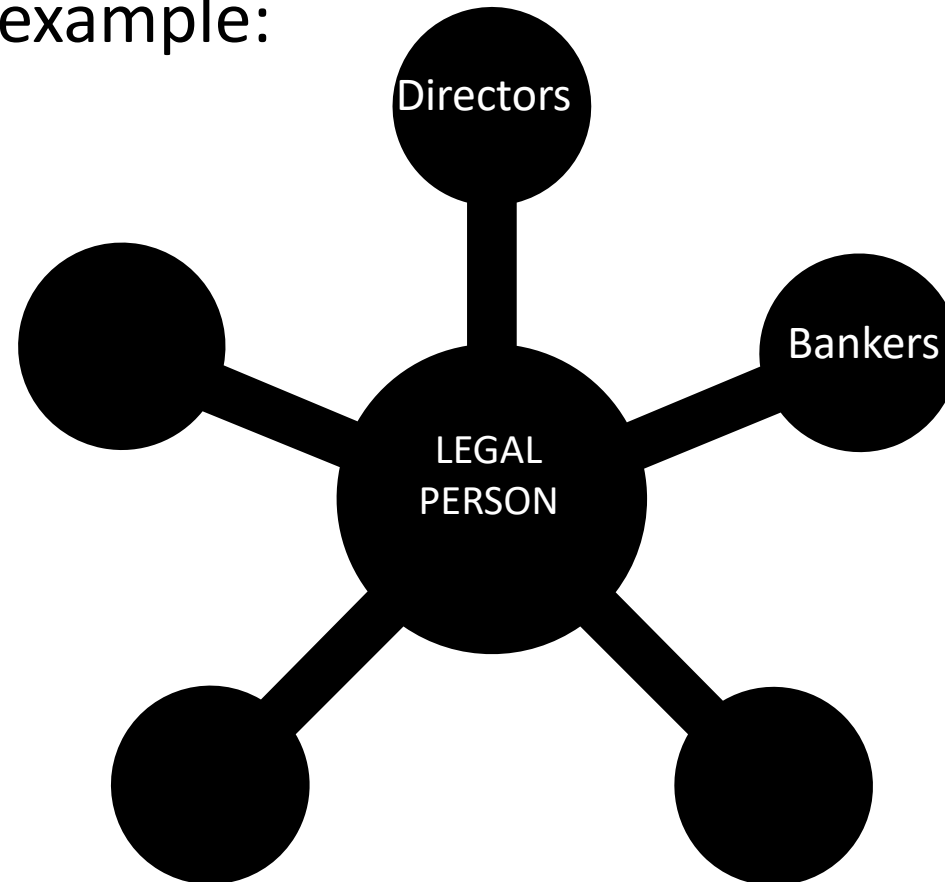
- ▶ Can enable corruption, fraud and tax evasion
- ▶ Assist with spending or investing the proceeds of crime
- ▶ Opaque – useful for Politically Exposed Persons
- ▶ Useful to hide bribery and embezzlement
- ▶ Provide an apparent legitimate commercial justification
- ▶ Comingle illicit finance
- ▶ Asset protection

Understand your  
'nexus risks' and  
other countries  
risks within any  
money laundering  
investigations

# Knowing a legal person

---

Each team draw a chart showing a company and as many different components, for example:



# Legal Persons – why are they abused

---

- ▶ Can enable corruption, fraud and tax evasion
- ▶ Assist with spending or investing the proceeds of crime
- ▶ Opaque – useful for Politically Exposed Persons
- ▶ Useful to hide bribery and embezzlement
- ▶ Provide an apparent legitimate commercial justification
- ▶ Comingle illicit finance
- ▶ Asset protection

Understand your  
'nexus risks' and  
other countries  
risks within any  
money laundering  
investigations

# Assessing Domestic Legal Persons

---

Scale

Quality & Accessibility of Basic Info.

Cross-Border Risk Exposure

Ease, Speed & Costs of Formation/Registration

Attractiveness for Non-Resident Use

Quality & Accessibility of BO Info.

Incidence in analysed ML/TF cases

Existence of ML/TF Typologies



Entity Risk Assessment = National vulnerability to ML/TF cases

# Legal Persons – typology assessments

---

Multi-jurisdiction splitting or ‘stacking’	Foreign ownership/control by shell company
Anomalous complex ownership/structure	Controlled by power of attorney
Use of trusts/foundations in ownership	“Front men” - nominees
Directors are legal persons	Use of private investment/hedge funds
International business companies (IBCs)	Use of fictitious entities
Use of large professional firms (LPP)	Use of fake IDs
Using deceptive names or legal structures	Limited oversight

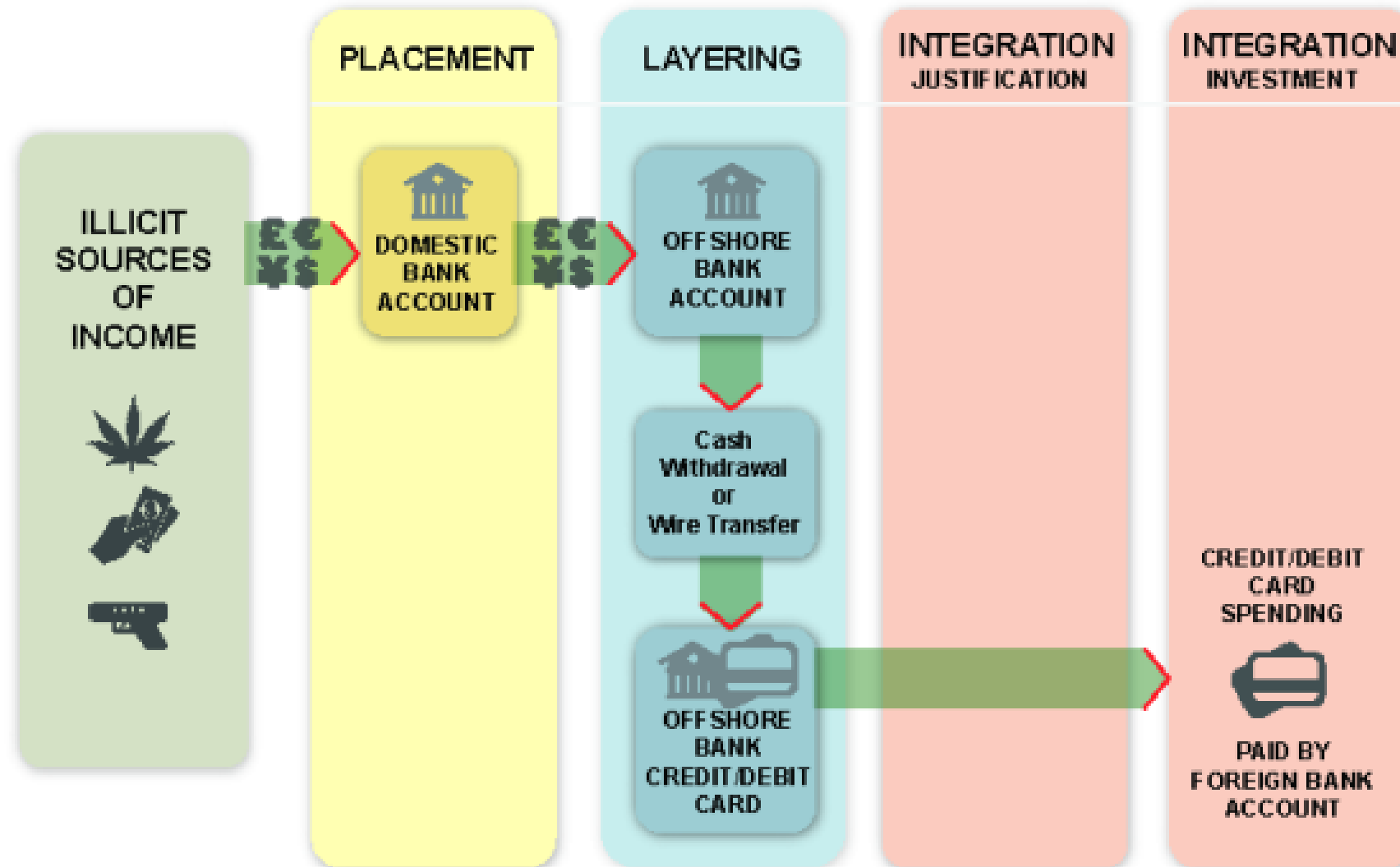
\*Legal persons arrangements ML risk assessment tool – EU/World Bank







# Abuse of a foreign legal person



# Legal Persons: What should we all be looking for?

---

- ❖ Team One: Legal Persons
- ❖ Team Two: Trade Activity
- ❖ Team Three: Account and Transaction
- ❖ Team Four: Trade Document and Commodity



What are the red flag indicators in each of the above? 20 minute breakout and nominate a spokesperson to tell us your findings.....

[http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/report/wco\\_fiu\\_handbook\\_sanitised-public-version\\_wco\\_en.pdf?la=en](http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/report/wco_fiu_handbook_sanitised-public-version_wco_en.pdf?la=en)

# 'Structural' Risk Indicators.....



1	Unexplained periods of dormancy	6	Negative and adverse news, fraud or tax allegations
2	Irregular online presence with boilerplate material	7	Copy-cat names of well-known corporations
3	Unusually complex and illogical structure	8	Non-compliant with filing requirements
4	Trade not associated to address type	9	Lack of typical business activities
5	Nominee appointments and lack of knowledge	10	Mass registration addresses / TCSP

# 'Trade Activity' Risk Indicators.....



11

**Inconsistent with stated line of business**

16

**High-volume and high-value by new trader**

12

**Engages in complex trade deals, third parties**

17

**Doing business with themselves**

13

**Unconventional & overly complex financial products**

18

**'Trend' commodities being traded**

14

**Consistent unreasonable low profit margins**

19

**Goods still in situ/port and yet to move.**

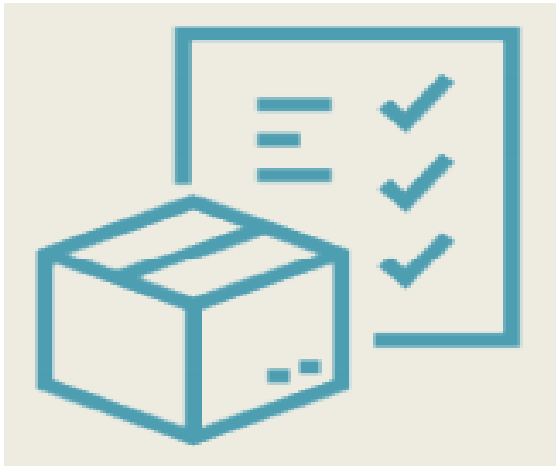
15

**Purchases exceed economic capabilities**

20

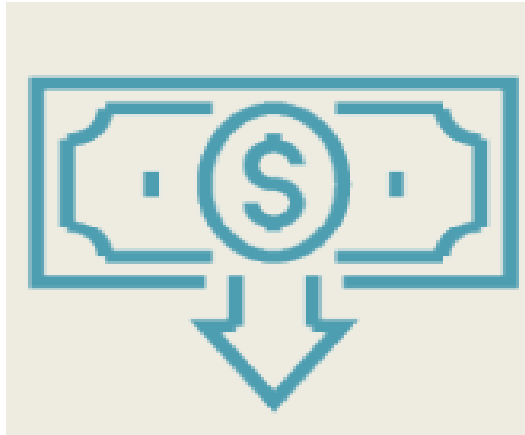
**Offshore company as supplier/buyer**

# 'Account and Transaction' Risk Indicators.....



21	Very late changes to payment arrangements	26	High-volume then quickly dormant
22	Transactions inconsistent with business	27	Unusual, large round amounts
23	"pay-through" or "transit" account	28	Circular jurisdictional payments that return
24	Third-party payments (not the consignee)	29	Back to back Electronic Funds Transfers
25	Reporting threshold circumventions	30	Big difference between declared and market value

# ‘Trade Document and Commodity’ Risk Indicators.....



31 Inconsistencies across contracts or invoices

32 Fees inconsistent with market value

33 Trade and Customs documents missing

34 Unusually simple contracts

35 Imports and exports mismatches transactions

36 Imported commodities exported with false papers

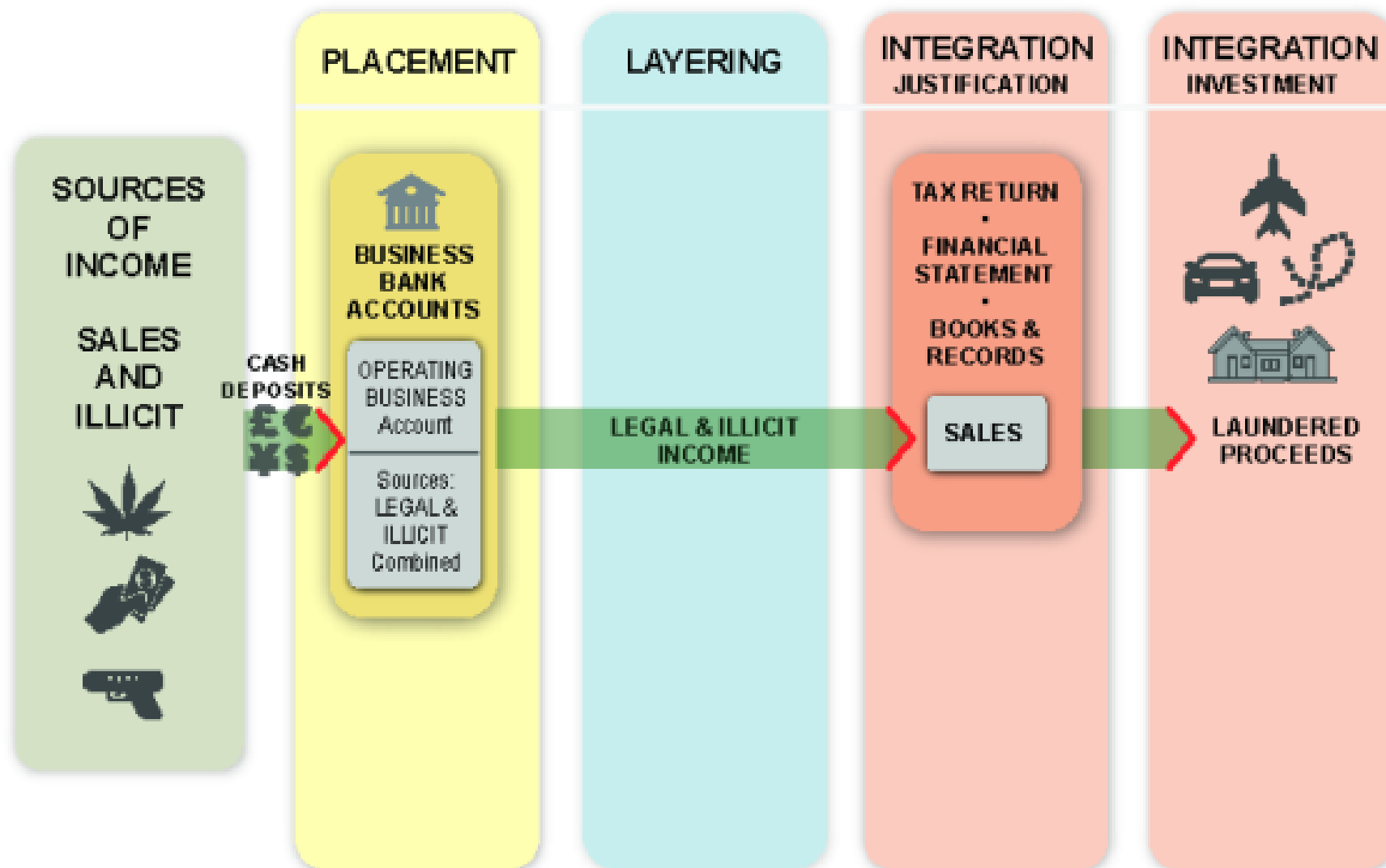
37 No economic justification for routes

38 Dual invoicing or second set of accounts

39 Risky goods: high value goods

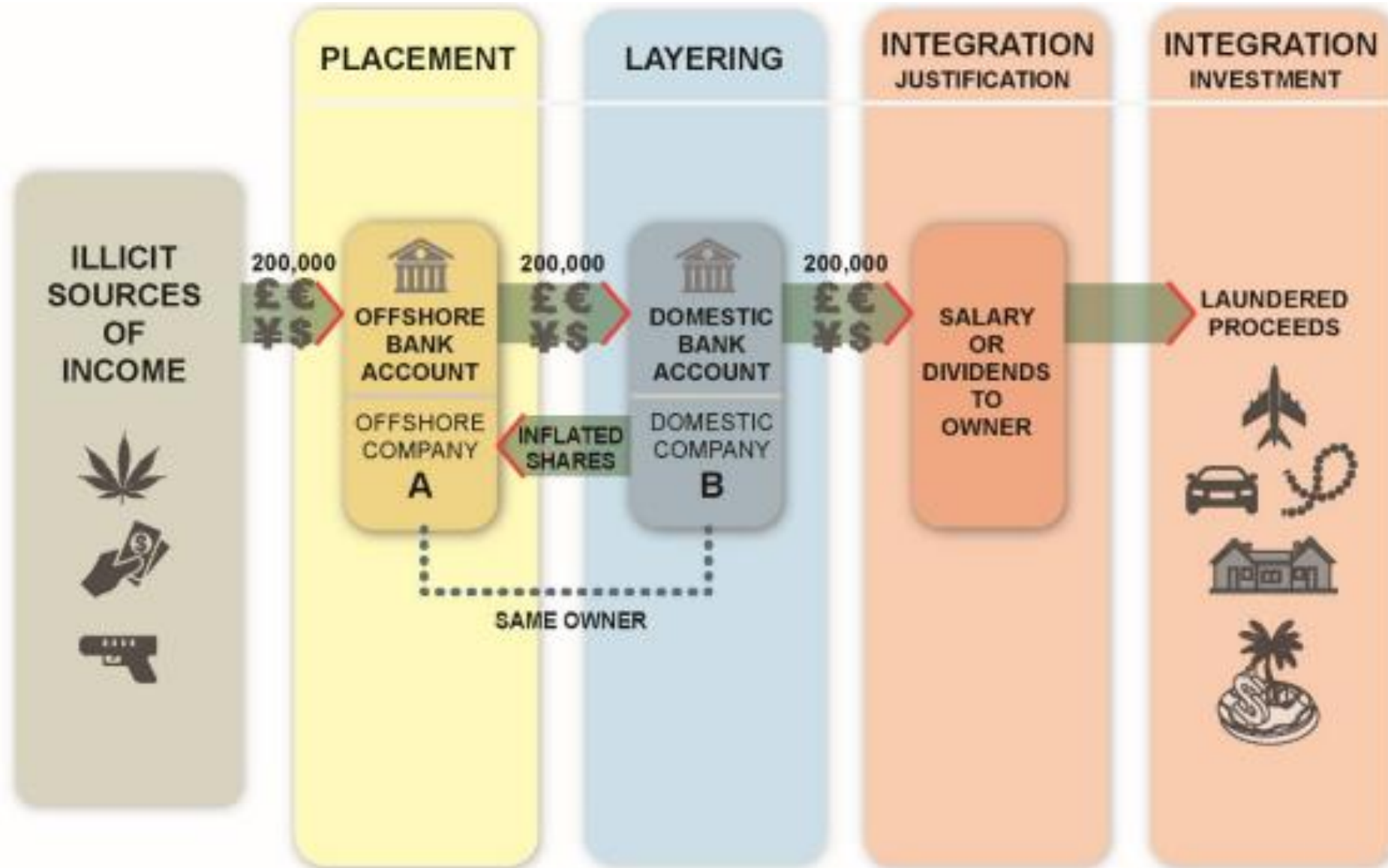
40 Big differences between customs filings and invoices

# Fabricated sales

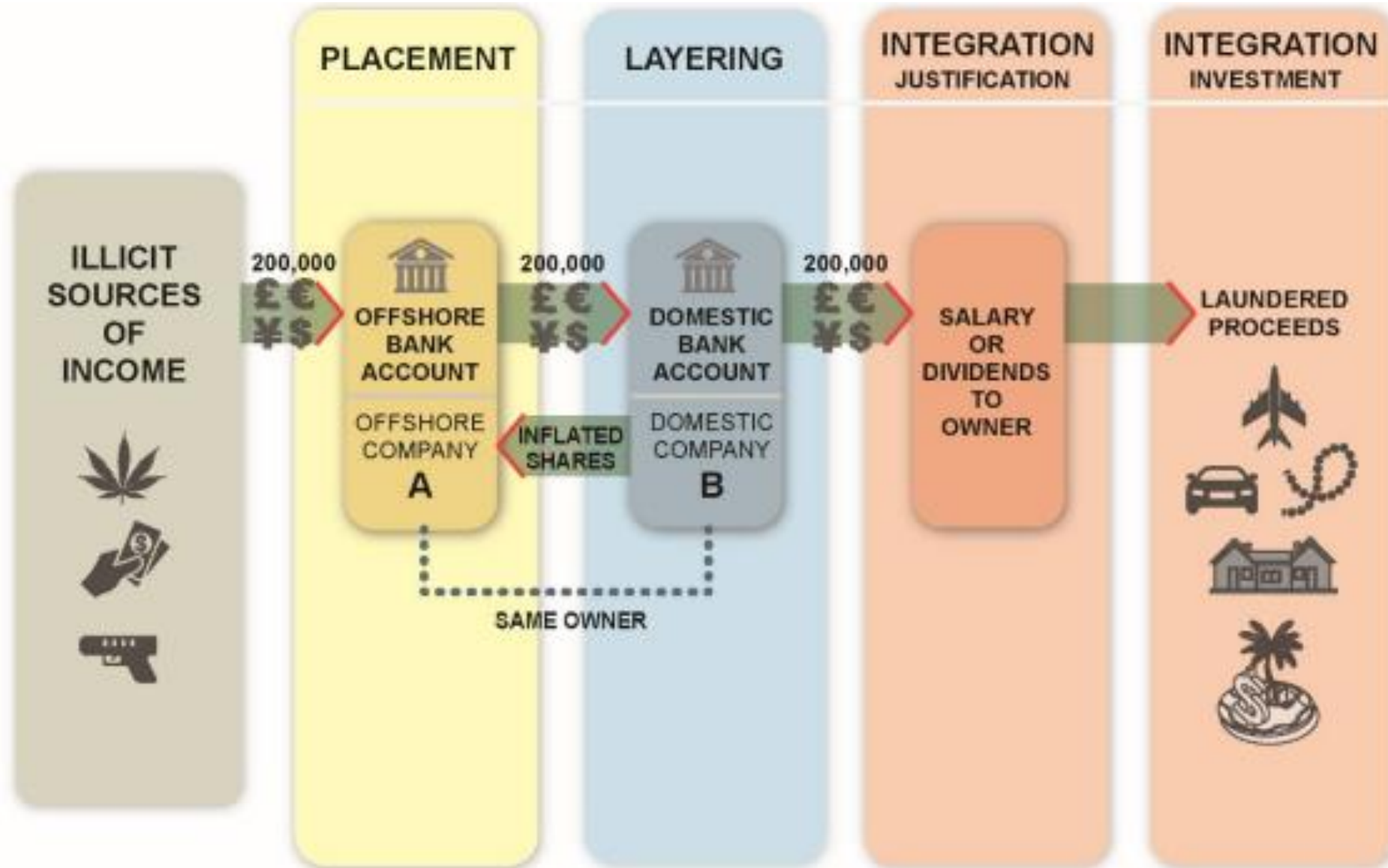




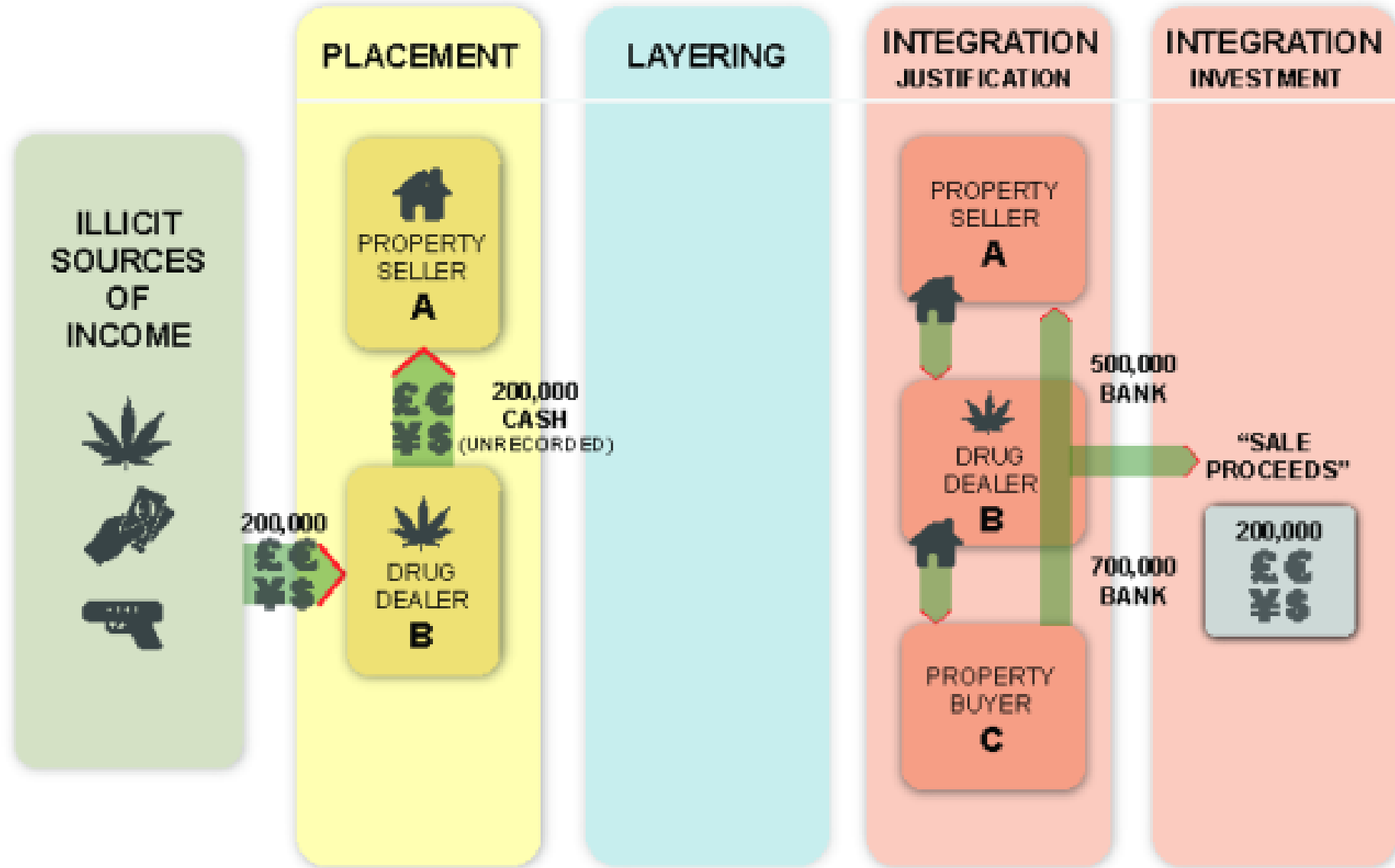
# Non-transparent ownership



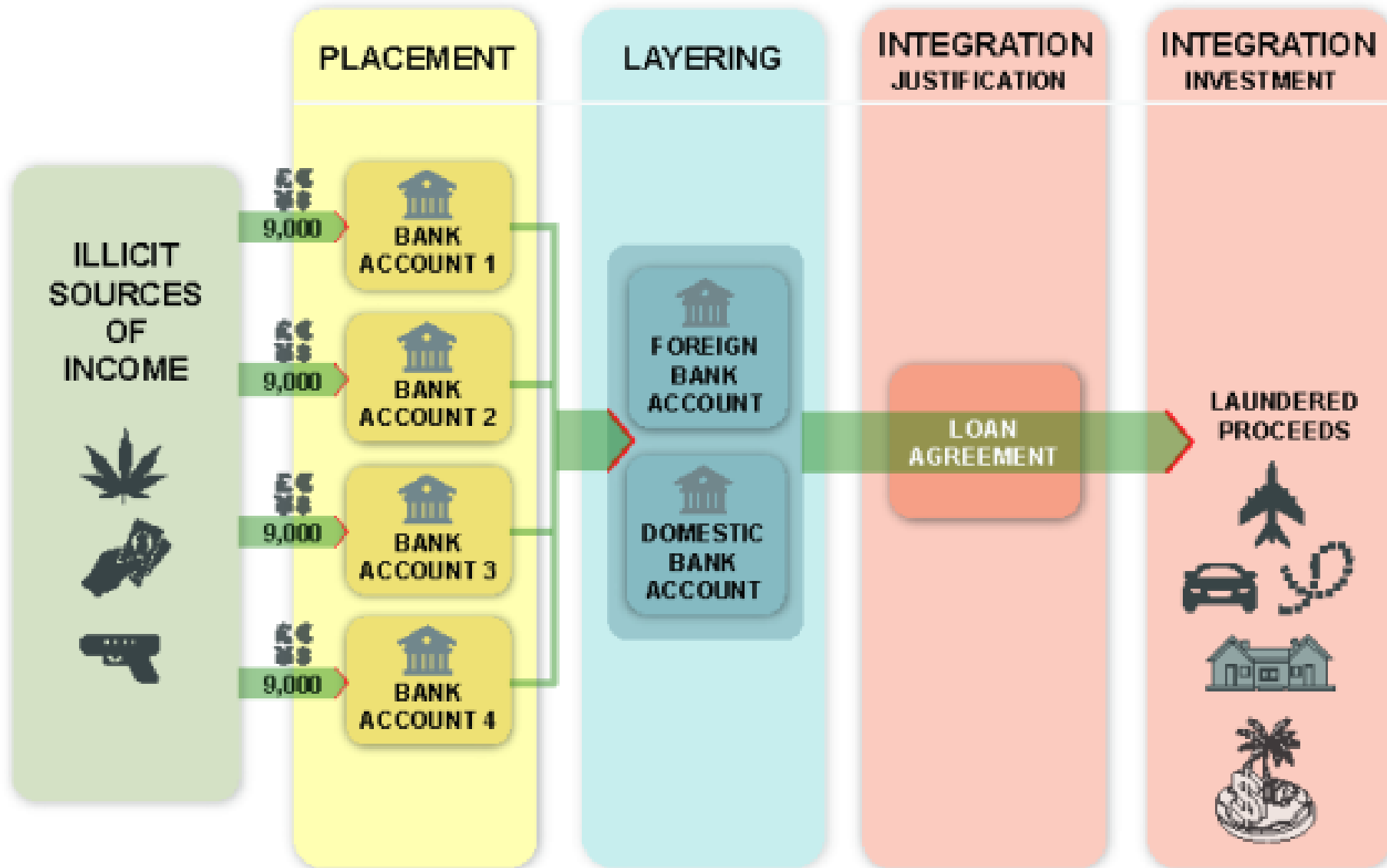
# Non-transparent ownership



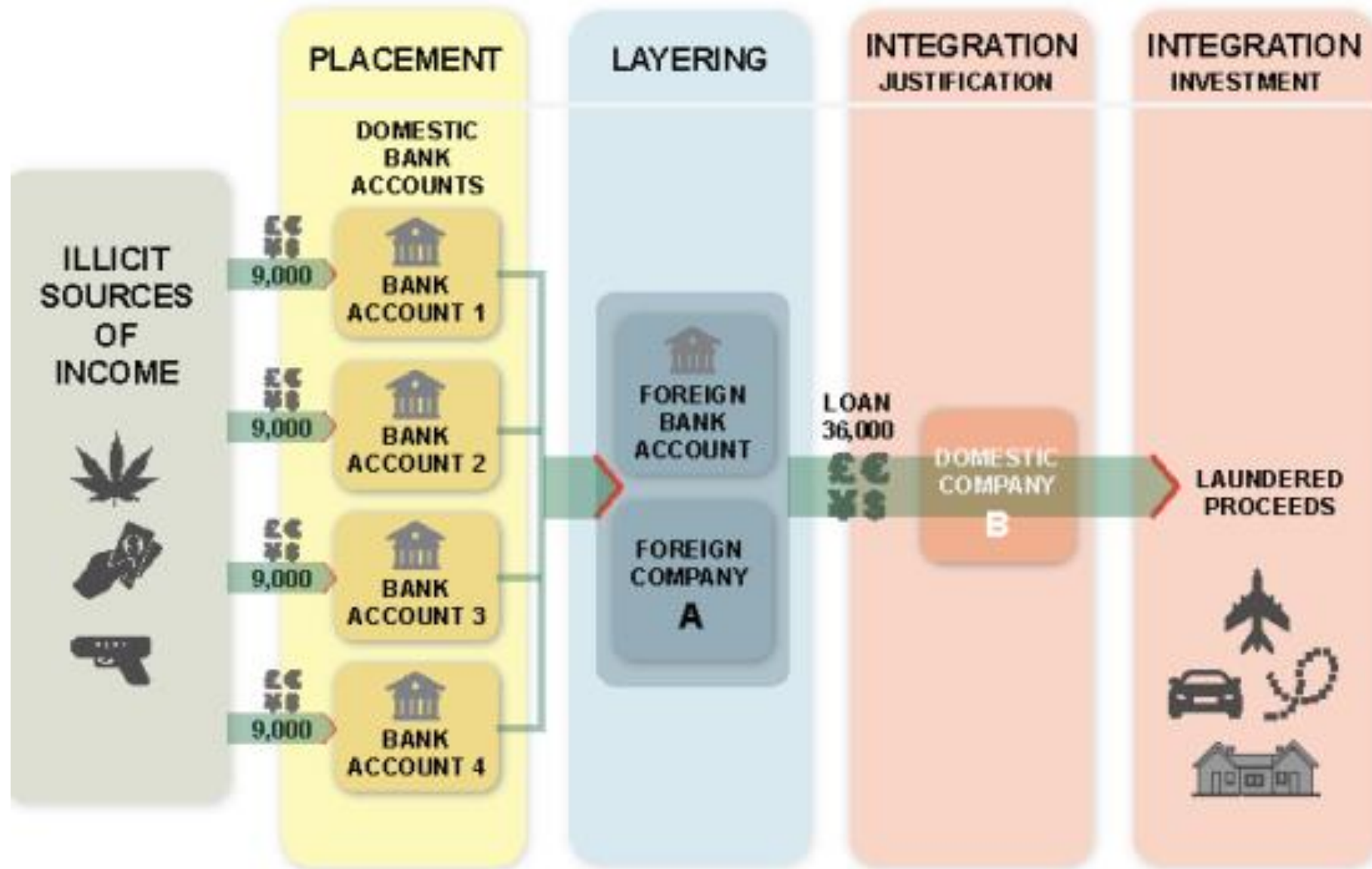
# Property Flipping



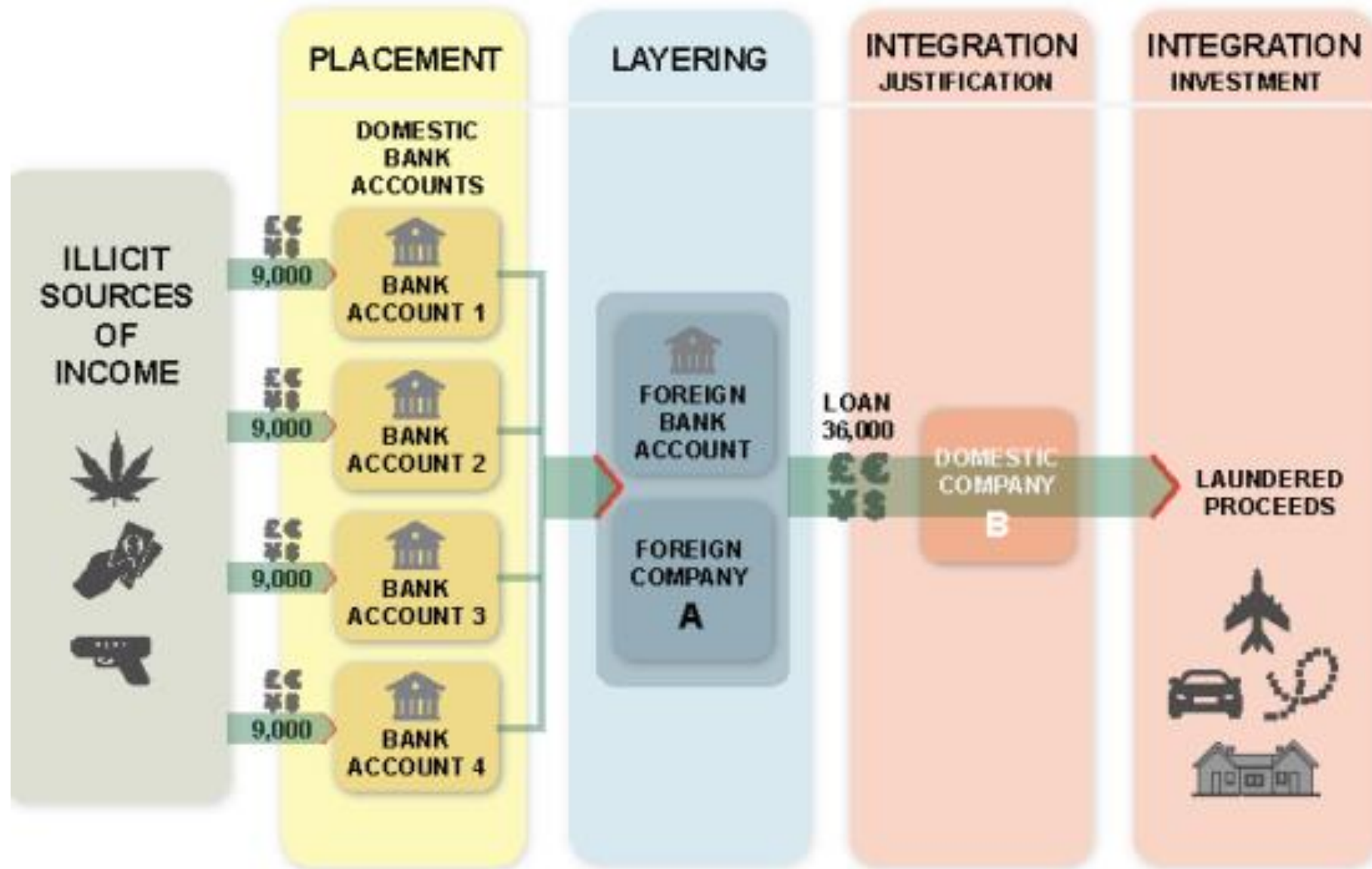
# Structuring or smurfing



# Loan-back money laundering



# Loan-back money laundering



# Schemes – Team Exercises

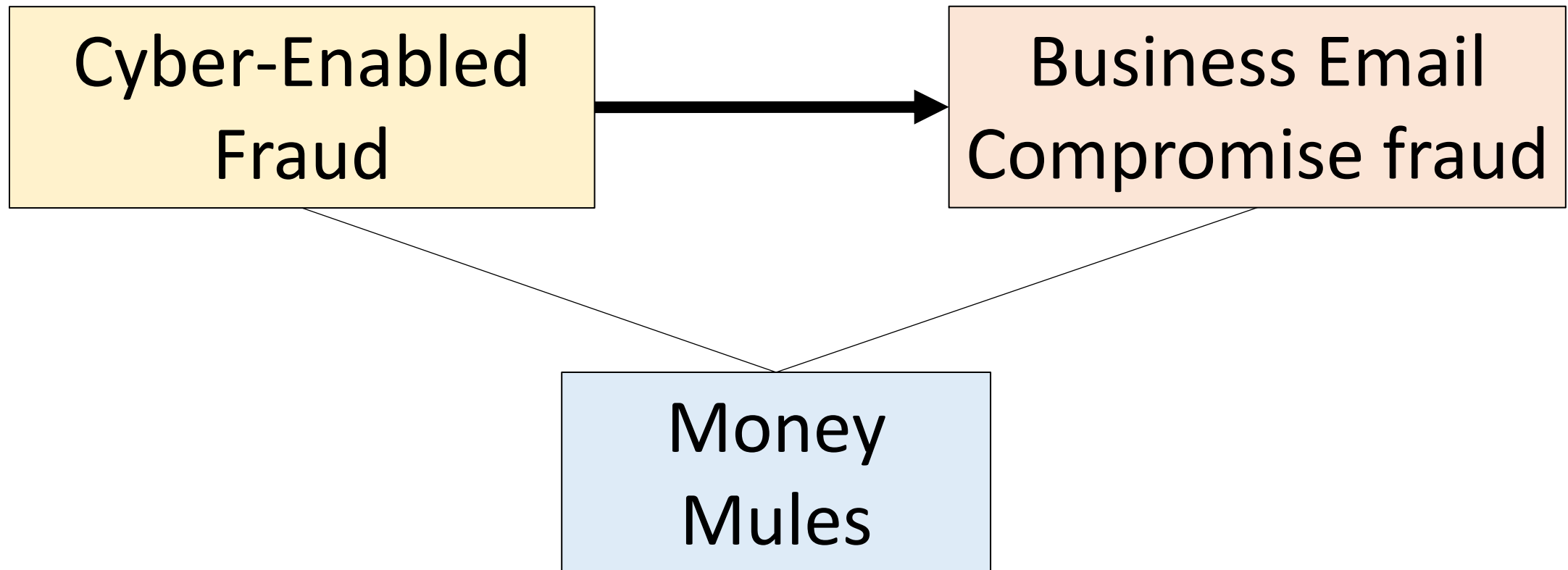
---

- ▶ The prosecutor has asked you to demonstrate the money laundering scheme in your current investigation.
- ▶ Chose a different crime type and using **placement**, **layering** and **integration** method, design the laundering scheme.
- ▶ Use the same type of diagram as the OECD
- ▶ You have 20 minutes
- ▶ Return to present the scheme



# Business Email Compromise (“BEC”) Frauds

---





# Cyber-Enabled Fraud ('CEF')

---

- According to FATF, CEF is a growing transnational organized crime
- CEF 'stack' jurisdictions, making it difficult for law enforcement
- Finances other serious crime, including proliferation financing
- Money laundering groups and professional enablers involved
- 'Money mules' combine others types of money laundering techniques
- Financial transactions executed at near-instantaneous speeds
- Locations of predicate different to where the proceeds are laundered

# BEC or Payment Diversion Frauds

---

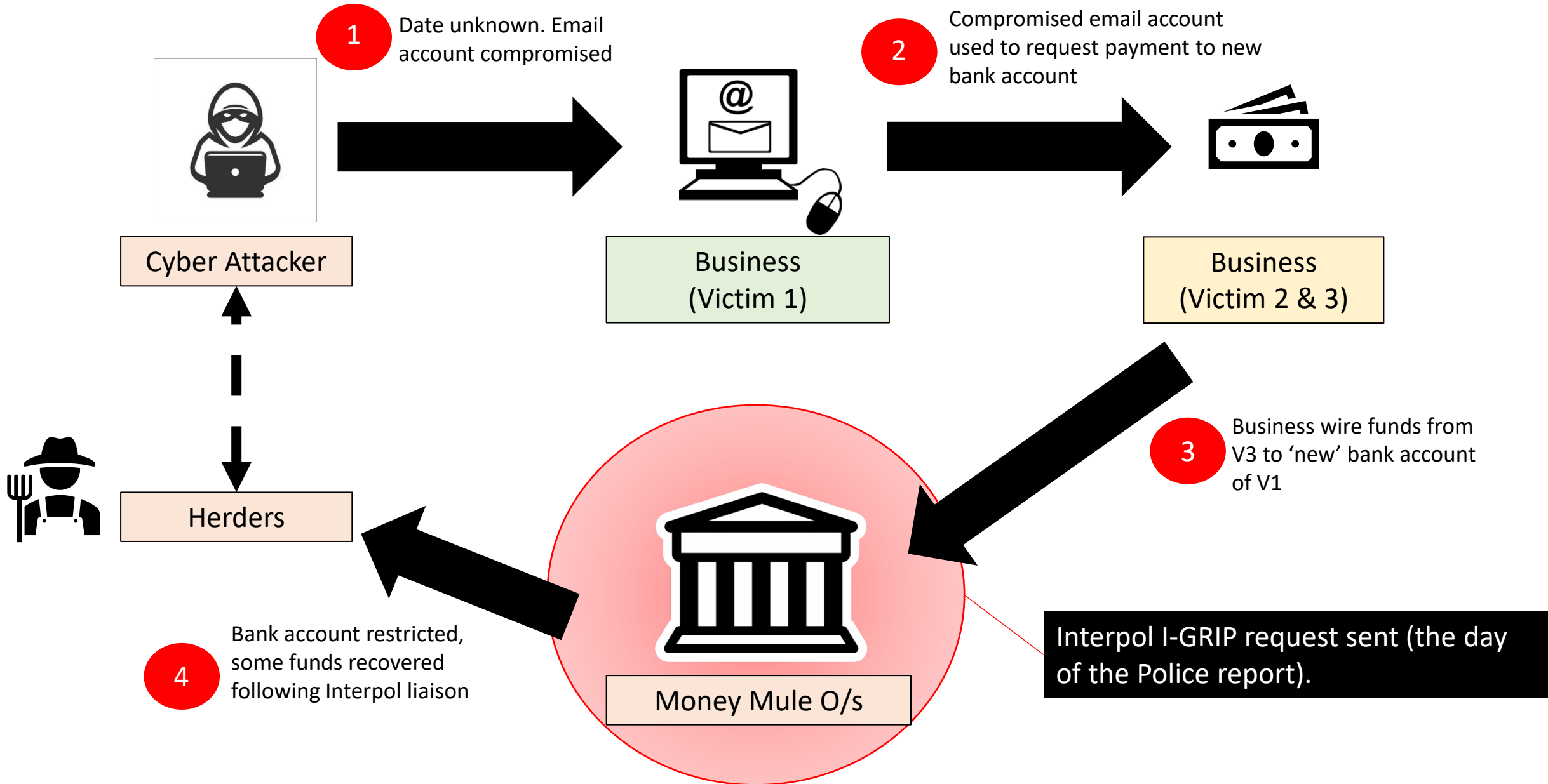
- False invoices or false requests or the diversion of wire transactions
- Victims receive emails to transfer funds to new payment accounts
- Types of BEC include; Invoice fraud, CEO fraud, conveyancing fraud and salary diversion fraud
- Use of fictitious email address or real email address (through an earlier 'hack' or compromise)
- Impersonation of real employees
- Quick detection by victims

# Money mules

---

- Easier to identify due to KYC information
- 'First layer accounts' receive the proceeds
- Bank accounts required for effective execution of BEC frauds
- Once received, funds are rapidly layered by “pass-through” transactions (smurfing and cash withdrawals also used)
- Mules may surrender banking credentials
- Jurisdictional difficulties with prosecutions (suspicion vs knowledge)
- Recovery more successful within 24 to 72 hours of transfers

# Case example of 'suspicion' in BEC



# Recommendations

---

- Joint taskforce or hybrid type investigators
- Establish a centralized and coordinated mechanism between law enforcement
- Develop a rapid international co-operation protocol incorporating:
  - a) INTERPOL's I-GRIP (Global Rapid Intervention of Payments)
  - b) Egmont Group BEC Project
  - c) Convention on Cybercrime (Budapest Convention)
  - d) direct liaison with service providers
- Promote 'Protect and Report' monthly awareness to increase victim reports
- Support the use of SWIFT recall messages with local financial institutions
- Increase identification of cyber-criminals through initial SAR filings