Virtual Anti-Money Laundering: Current Trends, Prosecutions, and the Challenges presented by Crypto Assets Programme

OECD LATIN AMERICA ACADEMY

17 April 2023

Case key elements

- Money Laundering
- Drug Trafficking
- Shell Companies
- Use of Crypto-assets
- Smuggling
- Foregin Trade

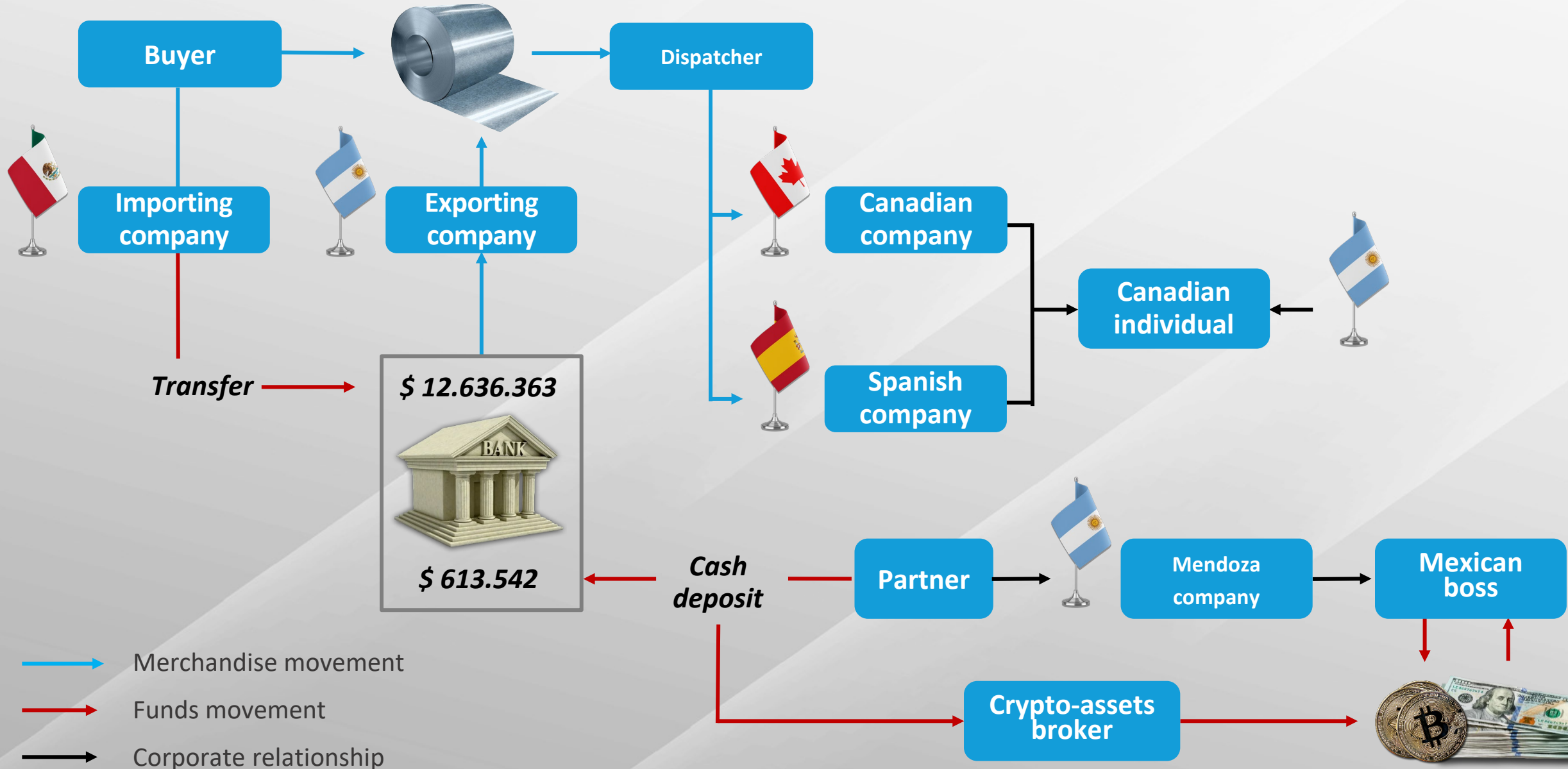
Case description

- DISMANTLING OF AN ORGANIZED CRIMINAL GROUP DEDICATED TO LARGE-SCALE DRUG TRAFFICKING
- ARGENTINE, CANADIAN AND MEXICAN DELINQUENTS
- SIMULATION OF FOREIGN TRADE TRANSACTIONS
- EXPORTS OF STEEL SHEET COILS
- CREATION OF SHELL COMPANIES IN ARGENTINA AND ABROAD
- HIDDEN DRUG IN STEEL COILS
- OPERATOR/BROKER → CURRENCY TRADE → MOVES THROUGH VIRTUAL ASSET TRANSFERS


PFA
8 Rollos de Acero
"Indectados" con COCAINA
PFA
PFA
PFA


PFA
Peso Aprox. 1.800 Kg.
en 1.708 panes de Cocaina
PFA
8 Rollos de Acero
"infectados" con COCAINA
PFA
OPERACIÓN
"B.B. de ACERO"
PFA

Scheme


Buyer
Dispatcher
Importing company
Exporting company
Canadian company
Canadian individual
Spanish company
Transfer
$ 12.636.363
BANK
$ 613.542
Cash deposit
Partner
Mendoza company
Mexican boss
Crypto-assets broker
Merchandise movement
Funds movement
Corporate relationship

Case closure

SENTENCE

- 7 MEMBERS OF THE TRANSNATIONAL CRIMINAL GROUP → SENTENCES OF 5-15 YEARS IN PRISON
- BROKER → 5 YEARS IN PRISON + FINE 8 TIMES THE SUM OF THE TRANSACTIONS (AT LEAST USD 468,400)

SEIZURE

- TWO TONS OF COCAINE (USD 60.000.000)

FORFEITURE

- CASH
- CARS
- TOOLS
- MACHINERY

Objectives of the presentation

Enable the participants:

1. To learn about the roles of the FIU in money laundering investigations.
2. To identify warning signs of money laundering that may arise in crypto-asset transactions.

The global international network

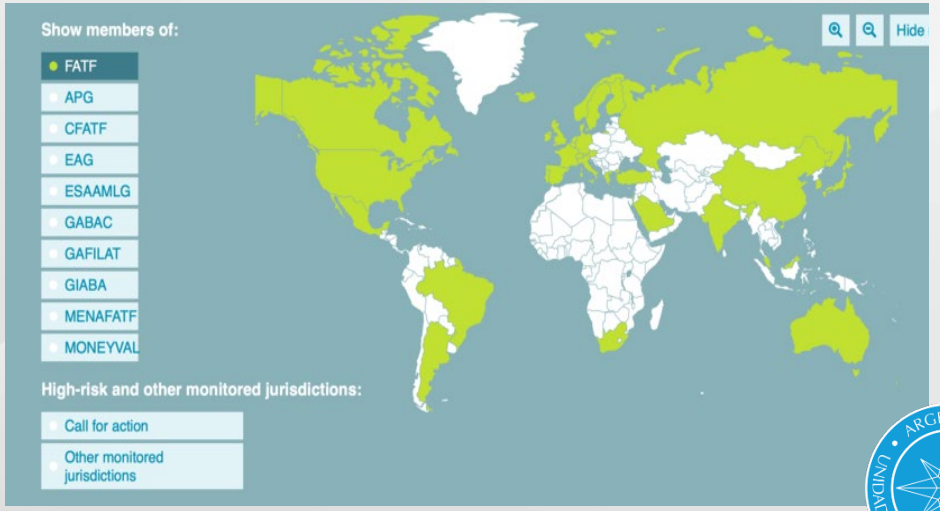
Over 200 participants

Members
Total: 39
(37 jurisdictions and 2 regional organisations)

FATF

Associate Members
(Regional FSRBs)

Observers FATF/GAFI
(UN, WB, IMF)



Financial Action Task Force

The Financial Action Task Force (FATF/GAFI) is an inter-governmental body which aims to:

- Set standards to combat Money Laundering, Terrorist Financing and other threats to the integrity of the international financial system, and
- Generate the necessary political will to bring about legislative and regulatory reforms, and monitor compliance, through the development of mutual evaluation reports, with the aim of protecting the international financial system from misuse by criminals.

Financial Action Task Force

The 40 Recommendations, and their Interpretive Notes, include measures on the prevention and repression of Money Laundering, and combating the Financing of Terrorism and Proliferation of Weapons of Mass Destruction. They are addressed to:

- ✓ Competent authorities (regulators), who are recognised as having powers and responsibilities, and
- ✓ FIU reporting entities engaged in financial activities as well as Designated Non-Financial Businesses and Professions (DNFBPs).

Financial Action Task Force

Members are subject to mutual evaluations to assess compliance.
Depending on the country's rating in the mutual evaluation, if the result is not positive:

- It may be decided to place the assessed country under increased monitoring (better known as the "grey list"), or
- It may be decided to consider the assessed country as seriously non-compliant or lacking the political will and commitment to comply and therefore considered as a high-risk jurisdiction subject to enforcement action (better known as "blacklisting").

FATF RECOMMENDATION No.15

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

FATF Report “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (ML/FT)” :

Provides useful red flag indicators for operational agencies charged with ML/FT prevention such as financial intelligence units (FIUs), government agencies, law enforcement and prosecutors to improve the detection, investigation and seizure of misused Virtual Assets.

Red Flag Indicators related to

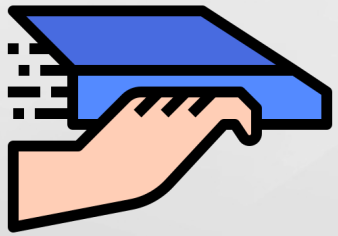
TRANSACTION PATTERNS

Red Flag Indicators related to

ANONYMITY

Red Flag Indicators about

SENDERS OR RECIPIENTS



Red Flag Indicators **Transaction Patterns**

Transaction volumes

Small volumes

Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions - smurfing.

Large volumes

Several transactions with large amounts can also be considered as red flag indicators when they have the following features:

- ✓ made in short succession,
- ✓ made in a staggered and regular pattern, with no further transactions recorded during a long period afterwards,
- ✓ made to a newly created or to a previously inactive account.

Red Flag Indicators **Transaction Patterns**

Acquisition and Immediate Transfer of VA to Virtual Asset Service Providers (VASPs)

- ✓ The transfer of crypto assets requires a minimal amount of infrastructure.
- ✓ Also, it does not require the involvement of intermediaries.
- ✓ The operation takes less time to complete.

This red flag becomes particularly relevant when transfers are made to other jurisdictions where there is no relation to where the customer lives or conducts business, or there is non-existent or weak AML/CFT regulation (disguising the funds' origin).

Another red flag is when VAs are converted to multiple types of VAs, incurring additional transaction fees, but without logical business explanation.

Red Flag Indicators **Transaction Patterns**

Transactions concerning users

TRANSACTIONS CONCERNING NEW USERS

- ✓ A large initial deposit for an amount that is inconsistent with the customer profile. Sometimes followed by withdrawal of the amount soon after.
- ✓ The user withdraws the VAs and attempts to send the entire balance off the platform.

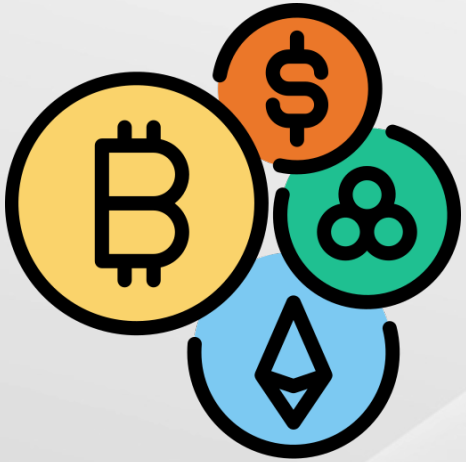
TRANSACTIONS CONCERNING ALL USERS

- ✓ Transactions involving the use of multiple VAs, or multiple accounts, with no
- ✓ logical business explanation.
- ✓ Making frequent transfers in a certain period of time (e.g. a day, a week, a
- ✓ month, etc.) to the same VA account by more than one person, or from the same IP address, or concerning large amounts.
- ✓ Conducting VA-fiat currency exchange at a potential loss.
- ✓ Converting a large amount of fiat currency into VAs, or a large amount of one
- ✓ type of VA into other types of VAs, with no logical business explanation and with no interest in the costs of the operation (e.g. without negotiating preferential prices).

Red Flag Indicators related to **Anonymity**

Transactions on the blockchain are not registered using the identification of the natural person user holding the VAs. However, within the context of an investigation, VSAPs can provide a connection between a public key and its owner, or investigators can use forensic services to trace transactions.

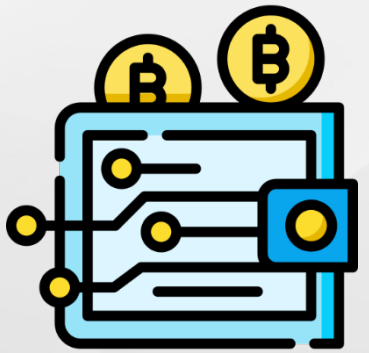
However, in order to disguise the illicit origin of the funds with which VAs are acquired, criminals often make use of some technological methods to try to maintain their anonymity and avoid detection of money laundering activities.



Transactions by a customer involving more than one type of VA, especially those VAs that provide higher
anonymity, such as anonymity-enhanced cryptocurrency (AEC).

Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites.

Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware).

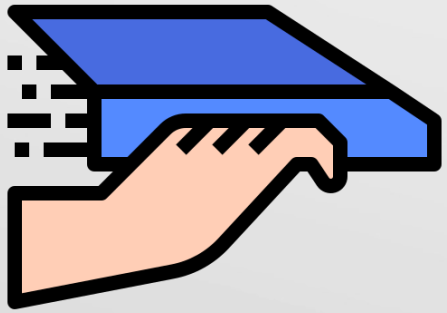


The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.

Users entering the VASP platform having registered their Internet domain names through proxies or using software that allows anonymous communication, including encrypted emails and VPNs.

Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.).

Red Flag Indicators related to **Senders or Recipients**



Irregularities observed during account creation:

- ✓ Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- ✓ Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.

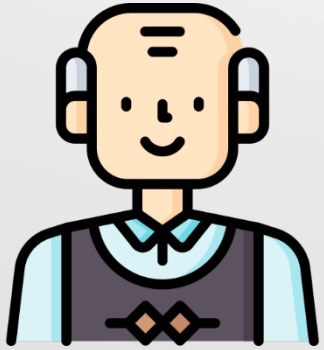
Red Flag Indicators related to **Senders or Recipients**

Client Due Dilligence

- ✓ Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
- ✓ Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- ✓ Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

Red Flag Indicators related to **Senders or Recipients**

Economic and financial profile



A person who is significantly older than the average age of the platform's users opens an account and performs a large number of transactions.

The customer buys large amounts of VAs that do not match their available capital or are not in line with their financial profile.

Red Flag Indicators related to

TRANSACTIONS

Red Flag Indicators related to

GEOGRAPHICAL RISKS

Red Flag Indicators related to

THE SOURCE OF FUNDS OR WEALTH

Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.

Receiving funds from or sending funds to VASPs whose CDD or know-your customer (KYC) processes are demonstrably weak or non-existent.

Red Flag Indicators in **the Source or Funds or Wealth**

VA transactions originating from or destined to online gambling services.

Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.

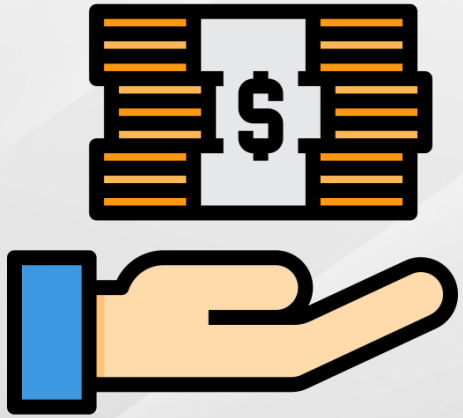
Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency.

A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.

Red Flag Indicators related to **Geographical Risks**

Criminals exploit the gaps in AML/CFT regimes on VAs and VASPs by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs.

A person's funds are disproportionately derived from VAs originating from VASPs based in jurisdictions with non-existent or minimal AML/CFT regulations.



Thinking like criminals

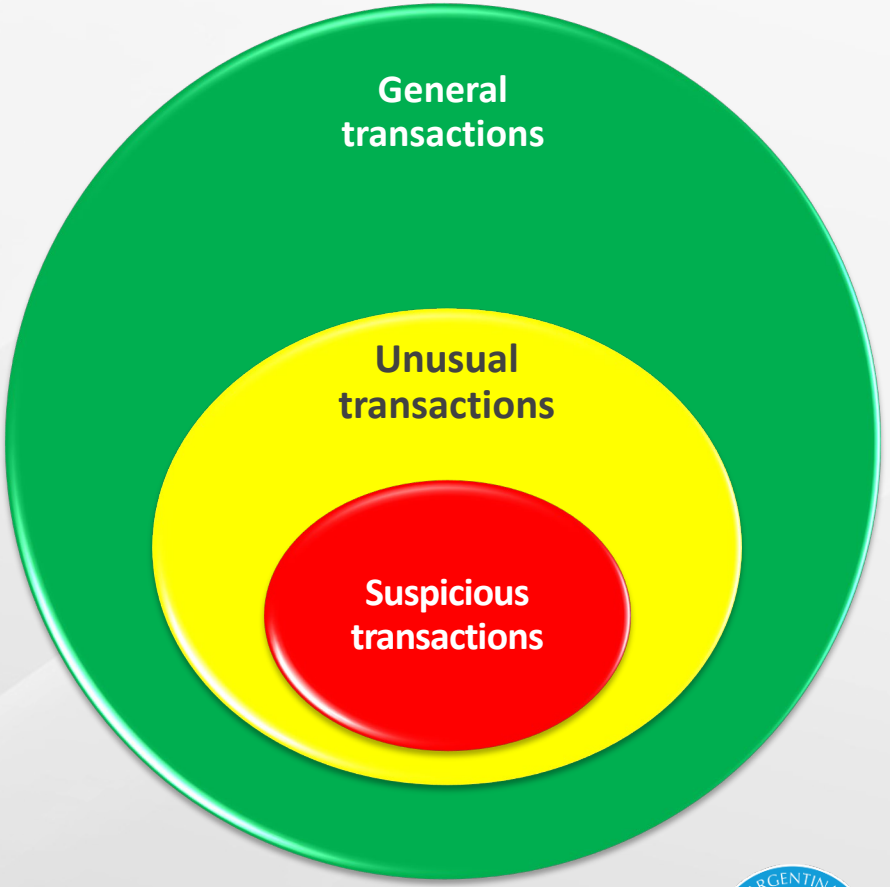
Each team must submit a case which is as strong as possible involving criminal assets that are being laundered and that meets at least one (1) red flag indicator that relates to at least three (3) of the aforementioned Red Flag Indicators (Transaction Patterns, Anonymity, Senders or Recipients, Transactions, Geographical Risks, Source of Funds or Wealth).

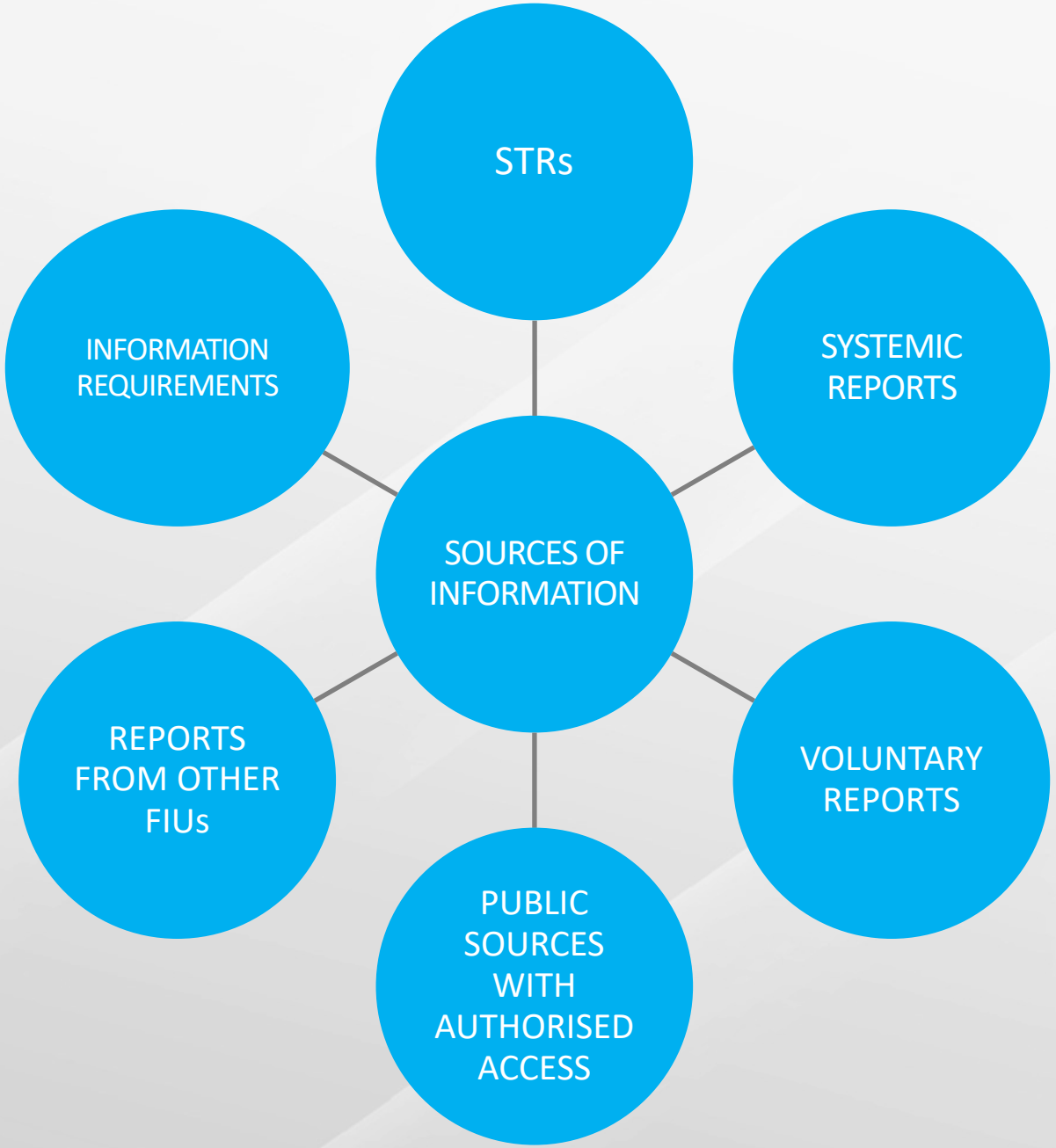
GENERAL TRANSACTIONS

UNUSUAL TRANSACTIONS

ANALYSIS OF THE UNUSUAL NATURE

REPORT OF SUSPICIOUS TRANSACTION




STRs
INFORMATION REQUIREMENTS
SYSTEMIC REPORTS
SOURCES OF INFORMATION
REPORTS FROM OTHER FIUs
VOLUNTARY REPORTS
PUBLIC SOURCES WITH AUTHORISED ACCESS

EGMONT GROUP

- REQUESTS FOR INFORMATION SENT
- REQUESTS FOR INFORMATION REQUESTED
- SPONTANEOUS DISCLOSURES

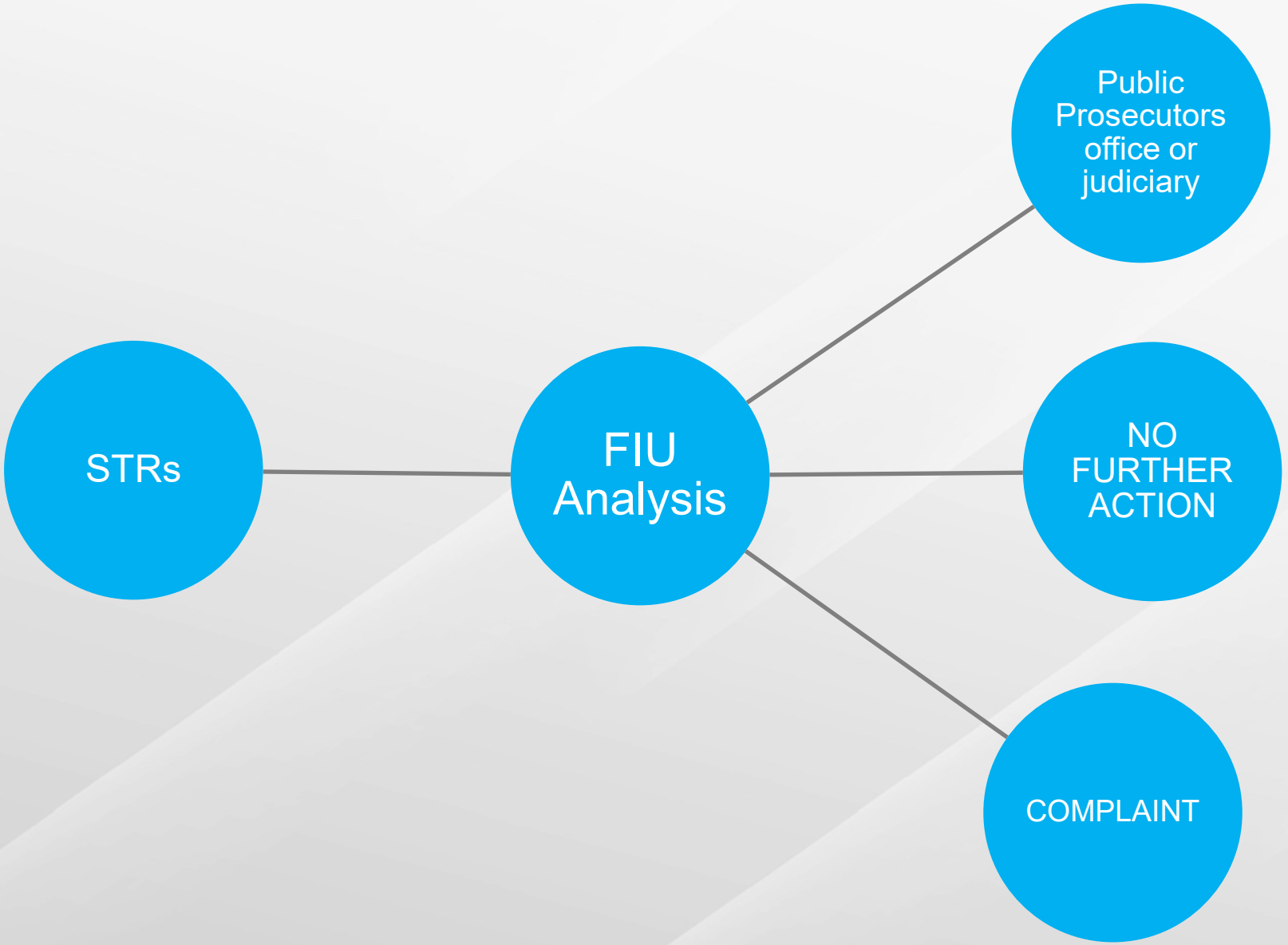
GAFILAT* ASSET RECOVERY NETWORK

- https://www.youtube.com/watch?v=2fdQd6N6yrM

*FAFT of Latin America

Characteristics of Information from foreign sources

- The requested FIU has complete discretion concerning the provision of information. The requesting FIU cannot impose deadlines and has no say in the response.
- The requested FIU has complete discretion concerning the scope of the information provided, and can stipulate that it may only be shared with the FIU, or also with the Public Prosecution Office, or with the judicial authorities, according to its criteria.
- The information provided by the FIU is generally only provided for intelligence purposes (to guide the acquisition of evidence). The FIU has only allowed for the information to be used as evidence in a few rare cases.
- Violation of the above by the administrative or judicial authorities incurs the international responsibility of the State.


STRs
FIU Analysis
Public Prosecutors office or judiciary
NO FURTHER ACTION
COMPLAINT

Thinking like investigators

You have received a Suspicious Transaction Report issued by a bank for transactions that are incompatible with the account holder's profile. The description of the transaction by the reporting person indicates that the account holder is a young person who in the first two days after the creation of the personal account received electronic transfers (home banking) for large amounts made by different persons. The funds were immediately transferred on the same day to the same person's accounts at several VSAPs for the purchase of Bitcoin, from which they were sent to an account of an unknown account holder at a VSAP located in a jurisdiction with weak AML/CFT regulation. The bank also reported that the customer had credits to the account from local VSAPs operating in other jurisdictions. In addition to filing the STR, the bank also reported that the account had a large balance at the time the report was issued.

Group 1

What information do you think you can find in FIU's internal databases?

Group 2

What information would you request from the financial institution?

Group 3

What information would you request from the local VSAP?

Group 4

What information would you request from foreign sources, and in your jurisdiction could you request action be taken on the balance? If so, what?

Thank you!

Dr. Alberto Mendoza