OECD International Academy for Tax Crime Investigation

Investigative Techniques for the Effective Use of Banking Information

OECD

CORRESPONDENCE BANKING RELATIONSHIPS (CBR): TRENDS, DRIVERS & WORKABLE SOLUTIONS

Bobby Quiwu Harris
Manager, National and International Relations
Financial Intelligence Unit of Liberia
November, 2021

OECD
BETTER POLICIES FOR BETTER LIVES

PRESENTATION OUTLINE

- Correspondent Banking Relationships - Cross border payments (e.g. SWIFT, MT103/MT202cov, KYC Requirements,)
- Virtual Asset and VASP
- New Payment Products and Services
- De-risking & Drivers of CBRs
- Unintended Consequences
- Workable solutions
- Conclusion

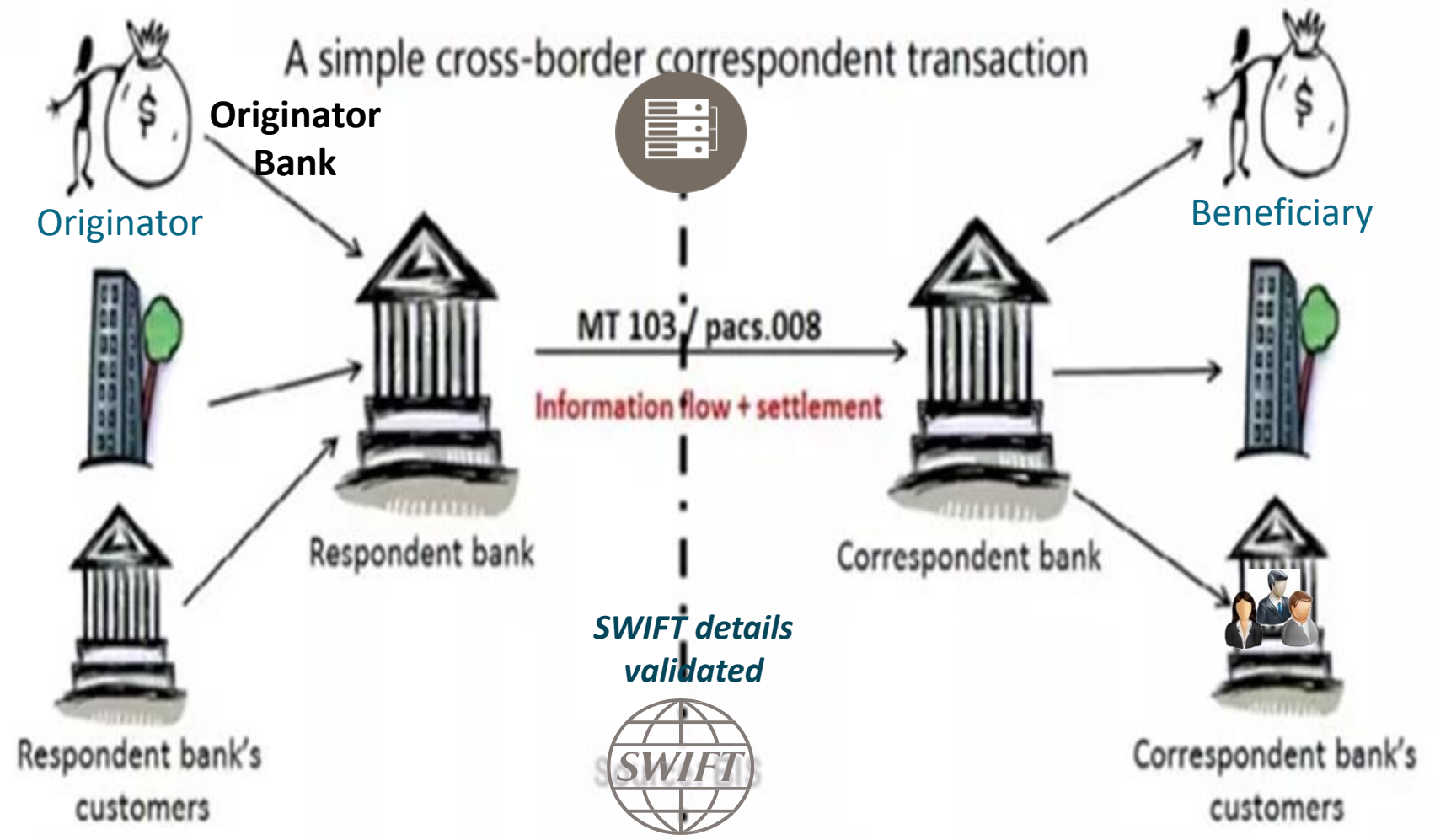
INTRODUCTION

- ✓ The FATF have identified three (3) Broad categories for the purpose of hiding illicit funds and introducing them to the formal economy i) Use of Financial Institutions ii) Physical smuggle of bulk currencies from one jurisdiction to another, iii) Transfer of goods via trade (Trade-Based Money Laundering)

- ✓ The 2007-2008 global financial crisis created a significant shift in the global risk environment and challenges faced by global banks, with significant geopolitical dynamics and concerns on the use of the financial sector for ML/TF.

- ✓ The Global Risk, Trend and Methods of IFFs have become more complex, especially with the introduction of New Payment methods (Financial Inclusion with significant increase in the need for financial institutions to apply RBA

Correspondent Banking Relationships



Correspondent Banking Relationships

- Correspondent banking services encompass a wide range of services which do not all carry the same level of ML/TF risks.
- Some correspondent banking services present a higher ML/FT risk because the correspondent institution processes or executes transactions for its customer's customers.
- Cross-border correspondent banking relationships involving the execution of third party payments are exposed to the higher risk.
- The requirements of both FATF Recommendations 10 and 13 must be met in all cases before cross-border correspondent banking services may be provided to a respondent institution.

Correspondent Banking Relationships

✓ SWIFT Network (MT103/MT202)

- ✓ An MT 103 is a standardized swift message type that is specifically used for a cash transfer from one bank to another anywhere in the world, provided they are a members of the Society for Worldwide Interbank Financial Telecommunications, (Swift). This type of cash transfer instruction is often referred to as a “Single Customer Credit Transfer”.

Correspondent Banking Relationships

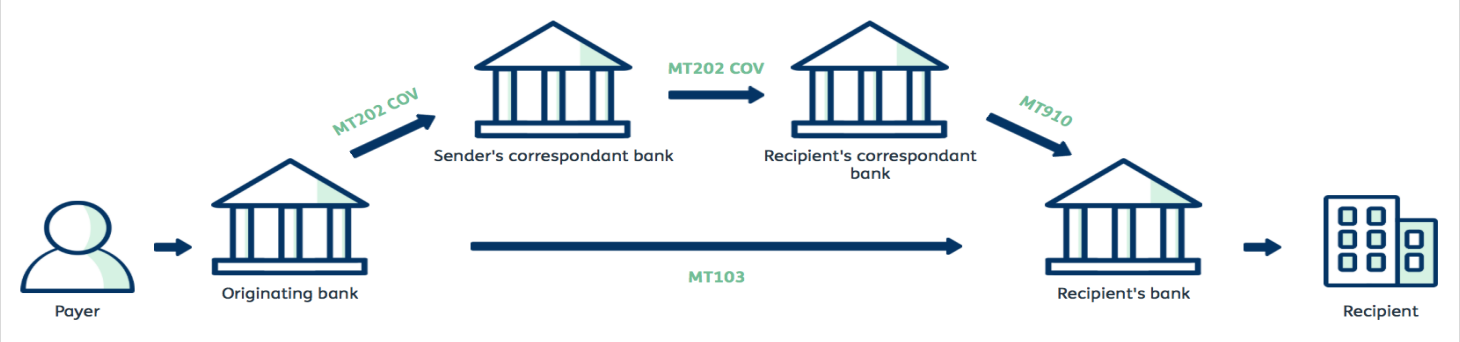
✓ SWIFT Network (MT103/MT202)

- ✓ The swift MT103 is a globally recognized payment message and contains the necessary information such as amount, currency, sent date, value date, remittance information e.g. payment reference, ordering customer, beneficiary, sending bank, receiving bank and a swift reference number.

- ✓ Key Difference between a MT101, MT102 and MT103:
  - ➢ MT101 has been designed for corporates and allows for bulk payments.
  - ➢ MT102 has been designed for multi payment instructions between banks and financial institutions.
  - ➢ MT103 has been designed for a single customer credit transfer.

Correspondent Banking Relationships

✓ SWIFT Network (MT103/MT202)



- Basically for SWIFT payments, funds have to move between several different banks in different jurisdictions, before they reach the recipient.

- The way that the banks in between the sender and recipient communicate the transfer of these funds is with an MT202 cover message.

Key AML/CFT Legislation on Wire Transfer

- ✓ AML/CFT Act, 2012
- ✓ Act to Amend Civil Procedure Law to provide provisional remedies for proceeds of crimes
- ✓ AML/CFT Regulations for Financial Institutions
- ✓ Regulation for the Licensing and Supervision of Money Remittance Entities
- ✓ Regulations on payment of Inbound Money transfers
- ✓ Regulation concerning transfer of Foreign currency
- ✓ Regulations dealing with the cross-border transportation of currency & bearer negotiable instruments

Pending AML/CFT Legislation

- ✓ Financial Intelligence Agency - BILL
- ✓ Money Laundering, Terrorist Financing, Preventive Measures and Proceed of Crimes -BILL

- ✓ **Amendment to the Criminal Code to include**
  - Criminalization of Illicit Trafficking in Stolen and Other Goods
  - Criminalization of Market Manipulations and Insiders Trading

Breakout Discussion

- **What are the legislations in place regarding inward and outward money transfer in your jurisdiction?**
- **How are regulatory expectations aligned amongst regulators in your jurisdictions?**
- **What are the challenges associated with money remittance services in your regime (inward & Outward)?**
- **What do you see as risks of CBRs in your regime?**

Case Study

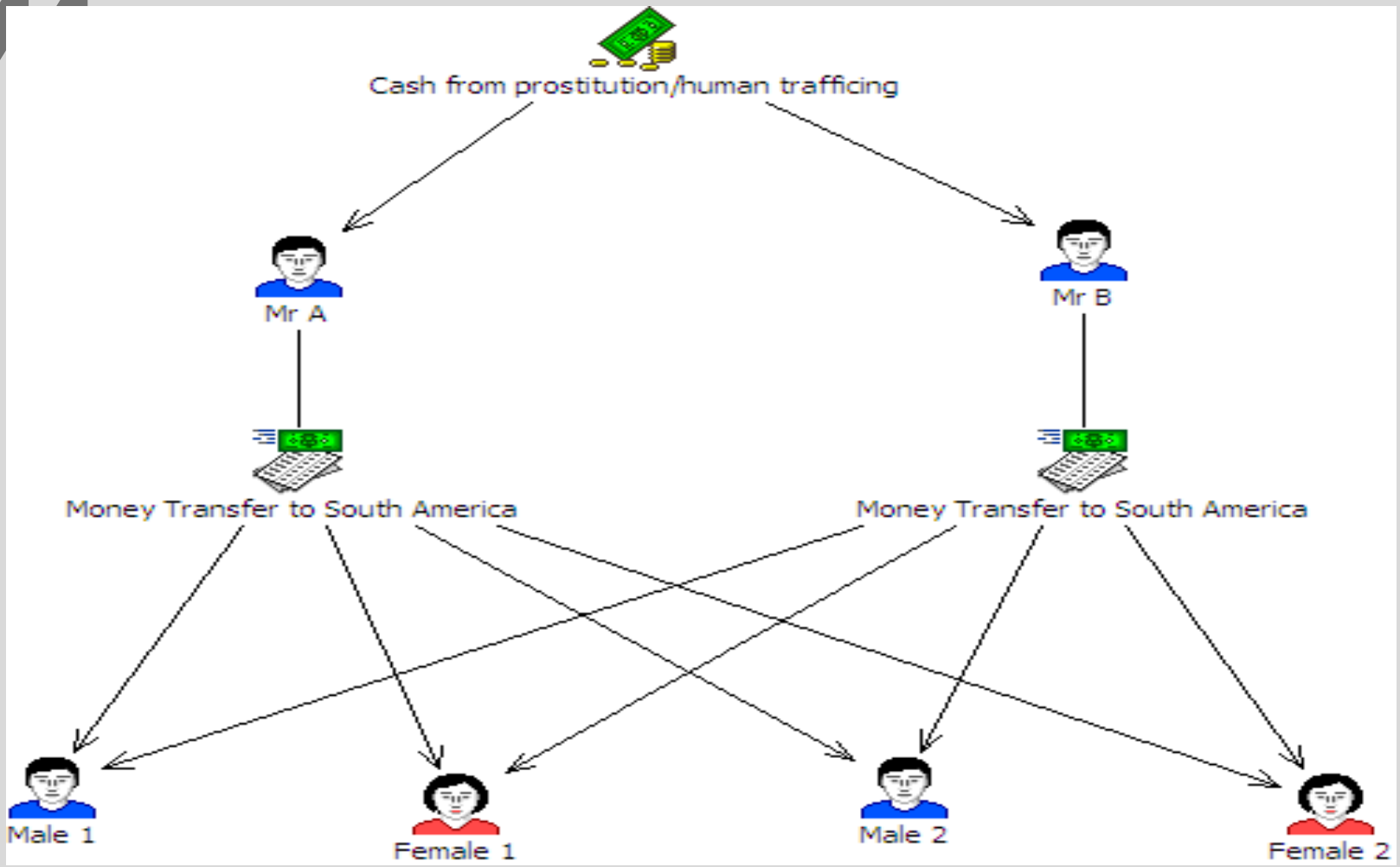
Mechanism: <u>Money Remittance Service</u>

Mr. Romeo A and Mr. Jackson B repeatedly made cash deposits sent via money remittance to Region X to the same recipients. In a few months' time the money remitted amounted to several thousand USD. There was no economic background for the transactions performed. None of the individuals resided at the stated address.

The remittance forms revealed that most of the money was sent by Mr. A, after which Mr. B took over the transactions with the same beneficiaries. When the identification papers of the two individuals were compared, it turned out that Mr. A and Mr. B were in fact one and the same person. Police sources revealed that A‟s identity featured in an investigation regarding human trafficking and exploitation of prostitution.

Identify the Red-flag Indicators

Case Study


Cash from prostitution/human trafficing
Mr A
Mr B
Money Transfer to South America
Money Transfer to South America
Male 1
Female 1
Male 2
Female 2

Case description

Mechanism: Money Remittance Service

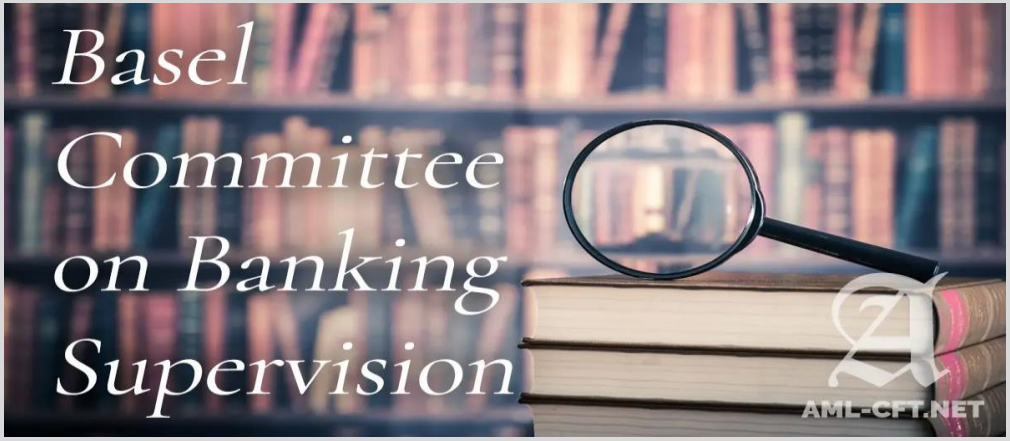
Red-flag Indicators:

I. Structuring

II. Same beneficiaries,

III. A large number of transactions during a short time period

International Standards Governing CBRs



CBRs and International Standards

- FATF Recommendation 13, requires FIs with respect to correspondent banking, to:

a. gather sufficient information about a respondent institution including its line of business;
b. assess the respondent's AML/CFT controls;
c. obtain approval from senior management, before establishing new correspondent relationships;
d. clearly understand the respective responsibilities of each institution; and
e. with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to the correspondent bank accounts, and to provide relevant CDD information upon request to the correspondent bank.

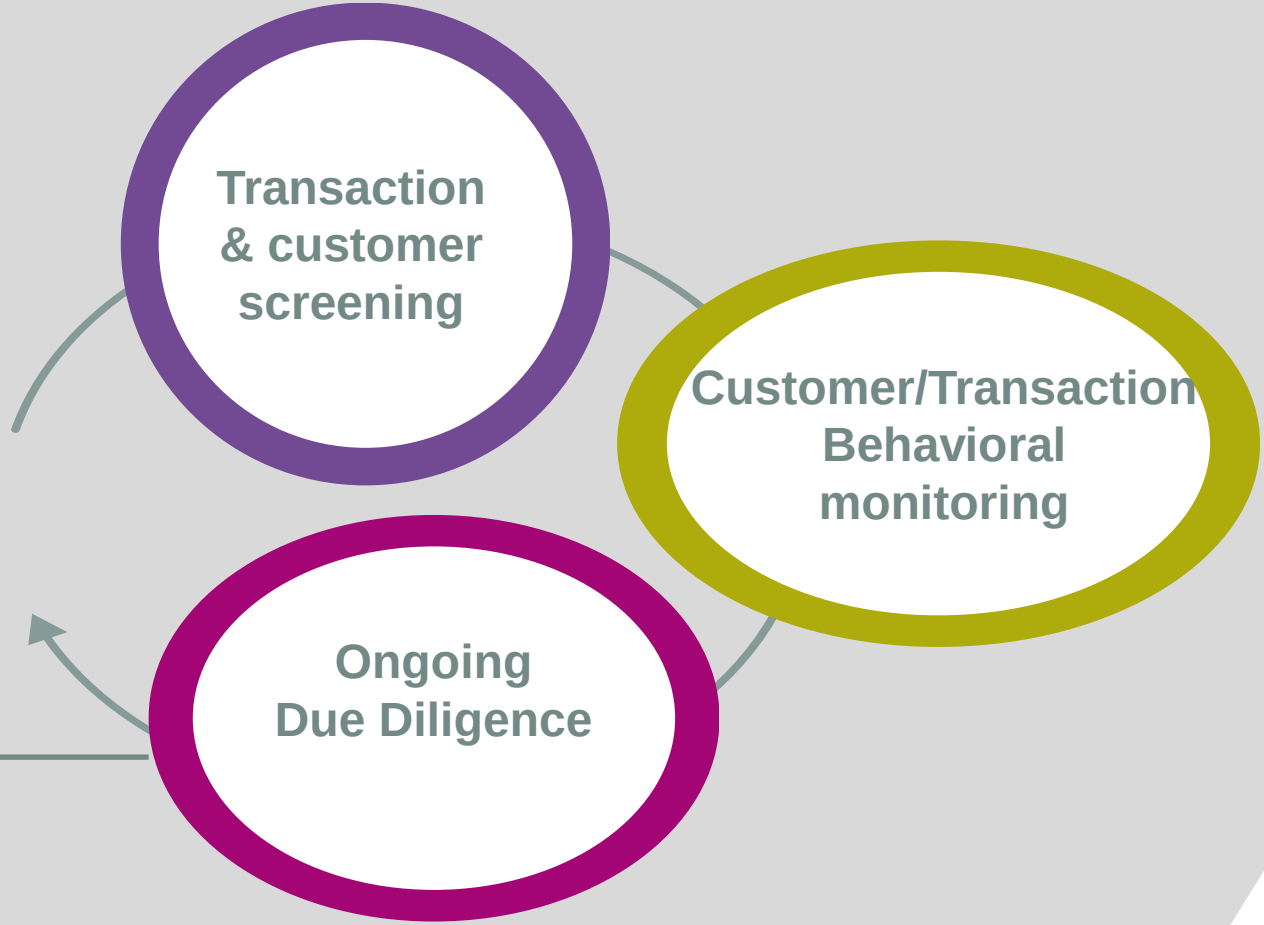
CBRs

✓ **Know you Customers' Customers (KYCC) and CDD –AML/CFT Requirements**

Customer Identification

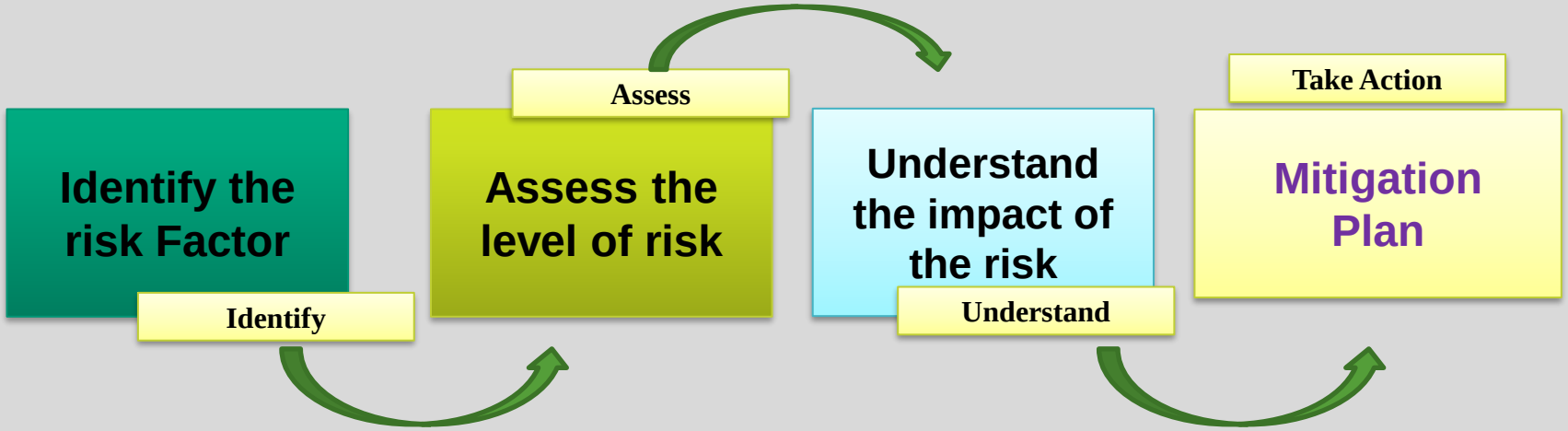
Customer Screening & Risk Profile/ID

Customer Due Diligence



Corresponding Banking Relationship (CBRs)

- Risk-Based Approach (RBAs)



Corresponding Banking Relationship (CBRs)

- Different level of Risk Assessments

MACRO
(National Level)

MICRO
(Sectorial/Thematic)

MESO
(Institutional level)

Case Study

Mechanism: Exchange Bureau

The Romanian FIU received an STR sent by a bank regarding some suspicious cross-border transfers. Thus, three Romanian citizens (X, Y, Z) received small amounts from company LTD (established in country A), justified as “salaries”. After receiving money, X, Y and Z used several schemes o launder money, some of which included exchange houses to change the currency.

For example, on the same day when Mr X received a large bank transfer from Mr M, he withdrew the amount of EUR 20 000 in cash, went to the exchange office and changed Euros to USD dollars. At the same day he visited the bank used for receiving money once more and opened bank account where he deposited EUR 50 000.

Mr Y withdrew the money received and opened bank accounts in smaller amounts in several other banks, exchange houses were used to change the currency. Mr Z changed EUR 60 000 in Bank‟s exchange house (whereas X and Y used private exchange houses) and used it to buy cars.

Case Study

Suspicious elements:

- Cross-border transfers consisting in small amounts under the reporting threshold
- Frequency of cross-border transfers

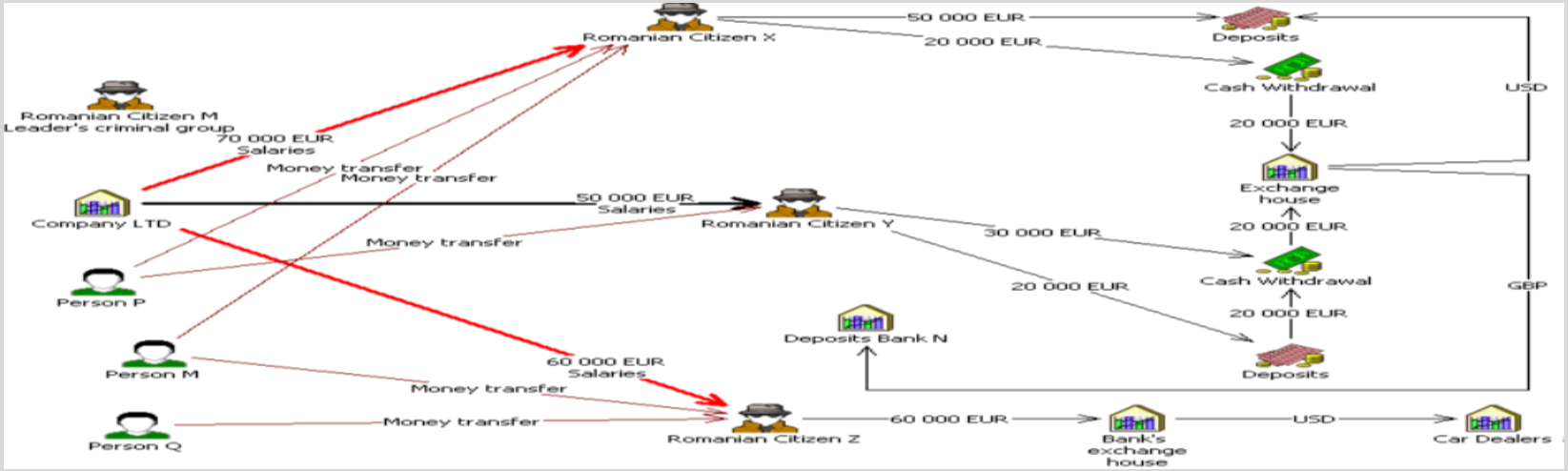
In a short period of time amount received by the Romania citizens was around EUR 180 000.

The request of information was sent to country A and the answer revealed that company LTD was involved in funds transfers in Eastern Europe, the proceeds originated from drugs and weapons trafficking.

The originator of the cross-border transfers originated by X, Y an Z was Romanian citizen Mr. M, the person leading the company LTD, known as the leader of a criminal group involved in drug trafficking and skimming.

Case Study

- It was also detected that Mr M used forged identity document in order to transfer money to Romania. It was also detected that X, Y, Z travelled to country A occasionally, but none of them worked or obtained legal income there. X, Y and Z could not prove that they worked or obtained any legal income from country A, they could not explain the large amount of money that were transferred to their accounts.



Identify the Red-flag Indicators

Case Description

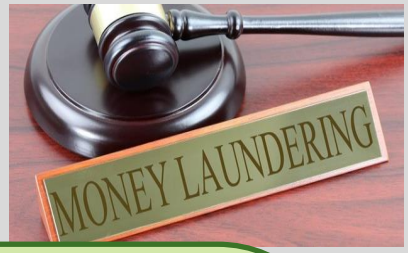
Mechanism: <u>Money Remittance Service</u>

Red-flag Indicators:

i. Money transmitting by criminals,

ii. MR to unusual jurisdictions

Virtual Asset



"A virtual asset is a digital representation of value that can be
-digitally traded , or
-transferred , and
-can be used for payment or investment purposes

Can include:
Virtual currencies, crypto-assets, crypto-currencies, altcoins, privacy coins / Anonymity-Enhanced Crypto-currencies (AECs), so-called stable coins

Virtual assets do not include digital representations of fiat currencies, securities and other financial assets covered elsewhere in the FATF Recommendations

Virtual Asset /Virtual Asset Service Provider VASP

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1) *exchange between virtual assets and fiat currencies;*
2) *exchange between one or more forms of virtual assets;*
3) *transfer of virtual assets;*
4) *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
5) *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

Expectations from National Authorities

Identify, Assess, and Understand the ML/TF risks from VA activities

VASPs should be subject to AML/CFT regime

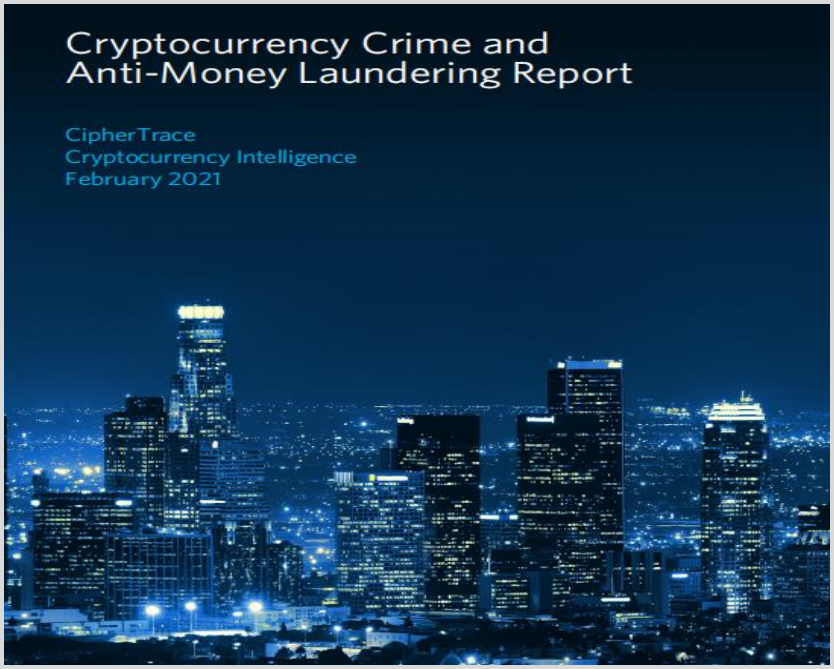
Registration/Licensing requirements for VASPs

VASPs are subject to adequate regulation and supervision/monitoring for AML/CFT

Range of sanctions, require implementation of preventive measures, international cooperation

Virtual Asset – Crypto & ML/TF

- $1.9 billion worth of Crypto crime was committed in 2020, down by 57% from 2019's $4.5 billion.
- Half of all thefts in 2020, totaling $129 million were connected toDecentralized finance (DeFi) hacks and centralized exchange,



Virtual Asset – Crypto & ML/TF

- Once a criminal has a pile of illicitly-gained cryptocurrency sitting in a wallet, the next question they have to answer is, **“How am I going to turn this into cash without getting arrested?”**
- The primary goal of cybercriminals who steal cryptocurrency, or accept it as payment for illicit goods and services is to **launder** the proceeds.

Fun fact:

- Only 270 addresses drove 55% of Money Laundering in Cryptocurrency (2020)

Virtual Asset ML/TF Risk

FATF 12-Month Review of VA and VASPs

- Money Laundering
- Fraud
- Tax evasion
- Sanctions evasion
- Terrorism Financing
- Sale of controlled substances
- Illegal sale of firearms
- Exploitation of children
- Human trafficking
- Computer Crimes (Cyber attacks, crypto jacking, theft, ransomware)

Trends in the use of VAs for ML/TF

FATF 12-Month Review of VA and VASPs

- Relatively small amounts in comparison to ML/TF channeled through the conventional financial systems;
- Mostly one type of virtual asset involved;
- Layering of funds may involve use of more than one type of VA;
- Use of the mixing techniques by laundering assets through services which aim to obscure ownership by taking in assets, co-mingling them, and then providing outputs of equal value to users, less a transaction fee;
- Criminals also sometimes move assets across multiple addresses, VASPs, types of virtual asset, or different blockchains (Layering);
- Professional Money Launderers also exploiting VA to collect, transfer or layer proceeds.

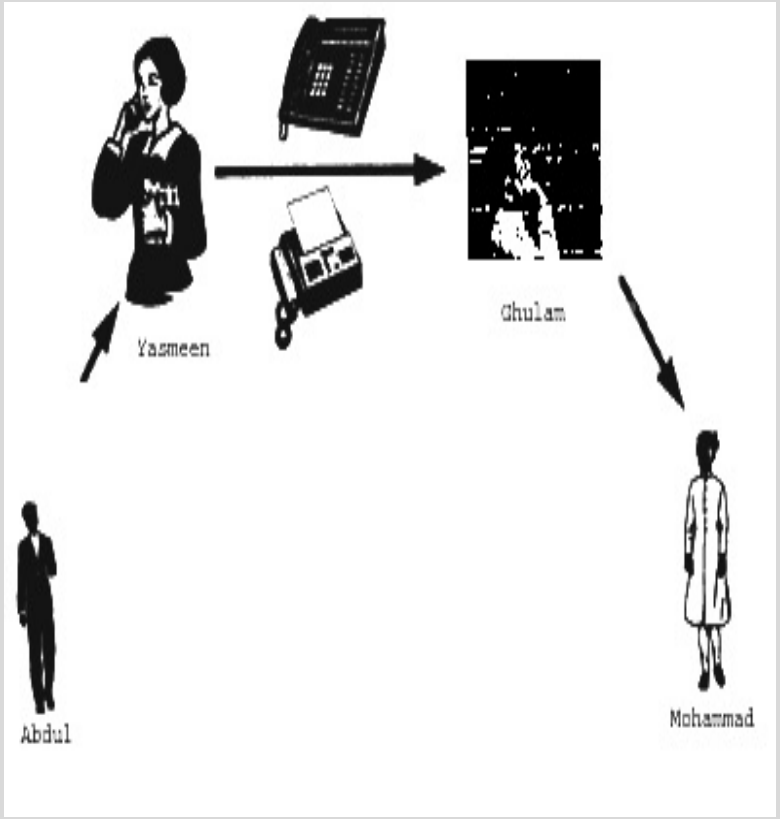
Case extracted from Virtual Assets Red Flag Indicators (FATF, 2020)

- **Use of mixing and tumbling – Helix**
- A darknet-based VASP, Helix, provided a mixing or tumbling service that helped customers conceal the source or owners of VAs for a fee over a three-year period. Helix allegedly transferred over 350,000 Bitcoin, with a value at the time of transmission of over USD 300 million. The operator specifically advertised the service as a way to conceal transactions on the darknet from law enforcement. In February 2020, criminal charges including ML conspiracy and operating an unlicensed money transmitting business were brought against an individual who operated Helix.
- Helix partnered with the darknet marketplace AlphaBay until AlphaBay's seizure by law enforcement in 2017.

Source: United States

Alternative Remittance Services

Hawala and Other Similar Services Provider (HOSSP)



HAWALA Vulnerabilities to ML/TF

There are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include:

- ✓ a lack of supervisory will or resources;
- ✓ settlement across multiple jurisdictions through value or cash outside of the banking system in some instances;
- ✓ the use of businesses whose primary focus may not be regulated as financial institutions;
- ✓ the use of net settlement or cover payments, not serial payments, to settle through the banking system that makes it difficult to track individual transfers;
- ✓ the commingling of criminal and illicit proceeds; and
- ✓ the masking of illicit proceed transfer that appears to be trade.

Hawala Typology

Sanctions Evasion by Criminal HOSSPs

Iran Sanctions Evasion by Criminal HOSSPs: Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) agents arrest Manhattan management consultant on charges of criminally violating the Iran Trade Embargo. ICE agents, acting as part of a New Yorkbased Task Force, arrested Mahmoud Reza Banki on January 7, 2009.

The investigation was conducted jointly by ICE and the U.S. Treasury's Office of Foreign Assets Control. According to the indictment, BANKI provided money transmitting services to residents of Iran by operating a *hawala* in which BANKI received wire transfers in a personal bank account he maintained at Bank of America in Manhattan totalling about USD 4.7 million from companies and individuals located in the following countries: Saudi Arabia, Kuwait, Latvia, Slovenia, Russia, Sweden, the Philippines, the United States, and other countries.

Case Study

Generally, BANKI did not know the wire originators personally. He received the funds with the understanding that an equivalent amount of Iranian currency would, in turn, be disbursed to intended recipients residing in Iran. Banki informed an Iran-based co-conspirator, when funds had been received and the co-conspirator then disbursed the funds in Iran, less any fees.

Banki, according to the indictment, used specific funds transferred into his Bank of America account to make joint investments in the United States with the Iran-based co-conspirator. Among other things, Banki used the funds to purchase a USD 2.4 million Manhattan condominium; to invest in securities for his own benefit and that of the co-conspirator; and to make payments on his credit card accounts, including about USD 55 000 in one month alone in the summer of 2007.

ALTERNATIVE REMITTANCE SERVICES/ FINANCIAL INCLUSION

New Payment Products and Services (NPPS)

Mobile Payments

Prepaid Cards

Internet-Based Payment Services

ALTERNATIVE REMITTANCE SERVICES/ FINANCIAL INCLUSION

Risk Factors that helps to identify ML/TF Risks in NPPS

- ✓Non-face-to-face relationships and anonymity
- ✓Geographical reach
- ✓Methods of funding
- ✓Access to cash
- ✓Segmentation of services

ALTERNATIVE REMITTANCE SERVICES/ FINANCIAL INCLUSION

Risk Mitigation Measures

- ✓ Comprehensive Risk Assessment of all New Products and Services
- ✓ Customer due diligence
- ✓ Loading, value and geographical limits
- ✓ Source of funding
- ✓ Record keeping, transaction monitoring and reporting

De-Risking CBRS

- De-risking refers to financial institutions terminating or restricting business relationships with entire countries or classes of customer in order to avoid, rather than manage, risks in line with the FATF's risk-based approach (RBA).

- This is a serious concern to the extent that de-risking may drive financial transactions into less/non-regulated channels, reducing transparency of financial flows and creating financial exclusion, thereby increasing exposure to money laundering and terrorist financing (ML/TF) risks.

Drivers

Concerns about profitability (De-Marketing)

Increased compliance cost

Reputational and liability risks

Changes in banks' financial risk appetite

De-Risking CBRS

- De-risking refers to financial institutions terminating or restricting business relationships with entire countries or classes of customer in order to avoid, rather than manage, risks in line with the FATF's risk-based approach (RBA).

- This is a serious concern to the extent that de-risking may drive financial transactions into less/non-regulated channels, reducing transparency of financial flows and creating financial exclusion, thereby increasing exposure to money laundering and terrorist financing (ML/TF) risks.

UNINTENDED CONSEQUENCES

- Withdrawal of correspondent banking relationships has direct effect on Money Transfer Operators (MTO) and other remittance institutions

- The closure of correspondent banking relationships has significant humanitarian, economic, political, and security implications

- The exit of financial institutions from correspondence banking relationships have had ripple effects on financial access for the individuals and populations served by those businesses.

WORKABLE SOLUTIONS

- Joint efforts by regulatory/supervisory authorities and financial institutions in reducing the cost of compliance.

- Establish appropriate mechanism for conducting adequate CDD and exchange of information.

- First and foremost, banks must understand why they may be de-risked. Factors such as the political and economic landscape in specific countries will certainly be part of the equation.

- By becoming more transparent with their activities, banks are likely to reduce the likelihood of being or indeed increase their chances of securing alternative arrangements if they are eventually de-risked.

CONCLUSION

- De-risking is the likely consequence of increased regulatory and compliance costs aimed at reducing money laundering and financing of terrorism. It is also driven by business decisions, low returns from business lines, risk management costs and stringent/demanding prudential costs. Efforts made by jurisdictions to achieve development and improve payment system can be undermined by de-risking of correspondent banking relationships.

- The solution for de-risking needs coordinated efforts amongst correspondent and respondent banks, regulators and operators and indeed all stakeholders.

- Governments, regulatory authorities and other stakeholders must therefore intensify efforts geared towards discouraging this phenomenon.

THE END


Merci beaucoup
Thank You
お疲れ様
Danke
Gracias
Grazie
Dank u
谢谢你
Thanks
Obrigado