المكتب التنفيذي لمواجهة غسل الأموال وتمويل الإرهاب
EXECUTIVE OFFICE OF ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING

National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee

Rising Use of Virtual Currencies by Criminals to Launder Their Illegal Profit

Public Private Partnership Subcommittee

May 2023

Overview

With the spread and evolution of new technologies, a phenomenon has developed over the past decade that has brought about a radical change in the global economy: virtual currencies.

The first among them to be created are the well-known Bitcoins, launched in 2009. Since then, the spread of such instruments has increased exponentially.

Such instruments aim to exploit the characteristics of both "physical" and "electronic" currency at the same time, creating a payment system that allows for both remote payments (as is the case with electronic money) and a certain form of anonymity, and more precisely "pseudonymity"; the wallet that arranged or received the transaction in fact remains known, but without automatically revealing its owner, as is the case with cash or "physical" currency.

The particular characteristics of such instruments have attracted the attention of various international institutions, first and foremost the Financial Action Task Force which in its June 2014 report on virtual currencies introduced an initial definition of virtual currency, identified as a *"digital representation of value that can be digitally exchanged and serve as a medium of exchange, unit of account and/or store of value, but which is not legal tender in any jurisdiction; is not issued or guaranteed by any jurisdiction, and succeeds in performing the aforementioned functions only through the agreement between the community of users of the virtual currency."*

Additionally, as the use of virtual currencies has immediately brought to light some pressing issues, such as the risk of using them for the purposes of money laundering, self-laundering, and terrorist financing, they have gradually drawn more attention from international and national institutions.

This document will cover:

- Characteristics of virtual currencies
- The Use of virtual currencies for Money Laundering and Terrorism Financing
- Money Laundering and virtual currencies – Domestic perspective
- Red Flag Indicators
- Key Recommendations for Financial Institutions and Private Sector
- Case Studies

Characteristics of virtual currencies

As highlighted by EUROPOL in its 2021 report, different features of virtual currencies could make them a tool for money laundering, such as:

- Anonymity
- Absence of an entity to supervise the executed transactions
- Absence of a Central Authority issuing the virtual currency, capable of exerting active control over it
- Transactions carried out with virtual currencies may take place between entities operating in different states, often even in risky countries or territories, making it difficult to identify the applicable forum and jurisdiction in the event of a dispute
- Multiplicity of virtual currencies in circulation

It should also be considered that the risk increases when transactions are carried out without the involvement of third parties such as exchangers or wallet providers, which are obliged to apply the anti-money laundering requirements of the regulations currently in force.

The Use of virtual currencies for Money Laundering and Terrorism Financing

The usage of virtual currencies in money laundering operations has increased as a result of their rising acceptance and popularity. Cybercrime, fraudulent virtual currency investments, and the use of virtual currencies as a payment method for illegal goods and services are some criminal activities that demonstrate an extensive use of virtual currencies. In any case, criminals always want to use virtual currency to conceal the origin of their illicit riches. The purchase of virtual currencies by criminal networks using illicit revenues and their use to move funds are two examples of how virtual currencies are used in money laundering operations. Professional money laundering networks pose a serious risk and give other criminal networks the ability to function. The majority of money used in cybercrime comes from dark web marketplaces, ransomware, and online fraud. The majority of illegal transactions are connected to these criminal activities.

A new reality has emerged in recent years: the use of virtual currencies by several terrorist groups for their crowdfunding. Due to external factors such as losing their territories and restricted financial regulation, as well as the fact that virtual currency transactions

are anonymous and untraceable, terrorist organizations are increasingly using them to sustain their operations and ensure their survival. According to Coinbase, one of the world's leading virtual currency exchangers, a considerable increase in criminal activity has coincided with the rise of virtual currencies over the past two years. Suspicious virtual currency transactions linked to terrorist activities increased from slightly more than 500 in 2019 to over five thousand in December 2022.

The main features that attract criminals to cybercrime are the high speed of action, accessibility, limitlessness, uncertain jurisdiction of states, and difficulties in conducting legal investigations. For international fundraising, terrorist groups are increasingly employing an integrated strategy that combines social media, messengers, and virtual currency.

Additionally, there are some elements that could make virtual currency more attractive to terrorist groups in the future, including:

1. a more-widespread usage of virtual currencies. The current lack of acceptance of these technologies, particularly in regions where terrorist organizations operate, may vanish as use increases globally;
2. Widespread adoption of second-generation virtual currencies with advanced privacy features will enable more illicit use of these systems;
3. Regulatory oversight in countries such as the United States, Europe, and China makes it difficult to obtain anonymously on an exchange. However, it might be considerably more difficult to track the transactions if trading takes place on a decentralized exchange or in a nation without regulatory monitoring.

Money Laundering and virtual currencies – Domestic perspective

The use of virtual currencies for criminal activities and laundering of profits has grown over the past years in terms of volume and sophistication. Tools facilitating their use are now widely available, and services dedicated to the channeling of criminal profits are well-established. As a consequence, the criminal use of virtual currency is no longer confined to cybercrime activities, but now relates to all types of crime that require the transmission of monetary value. According to analysts, about 23% of transactions are associated with criminal activities .

As previously mentioned, the illicit use of virtual currencies is predominantly associated with money laundering purposes.

Currently, the United Arab Emirates face two main threats related to the use of virtual currencies in money laundering activities:

1. Money launderers that are liquidating billions of dollars in virtual curreNcy, as they try to seek a safe haven for their fortunes.
2. Individuals using virtual currencies to invest in real estate in the UAE be cause of the fear that EU, U.S. or others could freeze their assets. Moreover, some customers are using local companies to turn their virtual money into strong currency and then hide it elsewhere abroad.

The two issues are actually related, and they pose a concrete threat not only for the money laundering activities that could occur in the country, but also for UAE's reputation.

Major exchanges like Coinbase Global Inc and Binance say they are taking steps to ensure that they are not used as a vehicle to evade sanctions and that they are working with law enforcement on the issue. However, as they offer users a high degree of anonymity, European countries and the U.S. have repeatedly called for closer oversight to eliminate any loopholes that could allow sanctions to be circumvented. An additional issue for the UAE is its placement on the Financial Action Task Force's grey list, citing the risks for money laundering in certain industries, including real estate.

However, according to some experts, the relative transparency of virtual currency transactions, which are recorded on the blockchain ledger, makes it difficult to evade large-scale sanctions.

Furthermore, over the last few years, the UAE has taken steps to regulate the industry in order to provide the country with a safe virtual asset economy.

To illustrate, the UAE Cabinet has issued in December 2022 a resolution 111 with the goal to better strengthen the current UAE's legislative framework for Virtual Assets (VA).

In fact, this resolution is aiming to further create a safe, secure and strong regulatory and supervisory regime for VAs, protecting investors and contributing to a buoyant economy.

The objectives of the resolution are to further:

1. Develop legislative framework for VAs sector in the UAE, and ensure rights and obligations of all parties
2. Regulate the VAs sector and VASPs
3. Ensure compliance of the sector with AML/CFT Law and related regultions
4. Support country efforts to provide safe regulatory environment and attract FIs and VASPs
5. Protect the investors from illegal practices.

Red Flag Indicators

Virtual currencies have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store assets digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds and make it harder for reporting entities to identify suspicious activity in a timely manner. These factors add hurdles to the detection and investigation of criminal activity by national authorities, FIU's and the private sector.

The Annex 1 contains a collection of red flag indicators of suspicious virtual currencies activities or possible attempts to evade law enforcement detection. The existence of a single indicator does not necessarily indicate criminal activity. Often, it is the presence of multiple indicators in a transaction with no logical business explanation that raises suspicion of potential criminal activity. The presence of indicators should encourage further monitoring, examination, and reporting where appropriate.

Key Recommendations for Financial Institutions and Private Sector

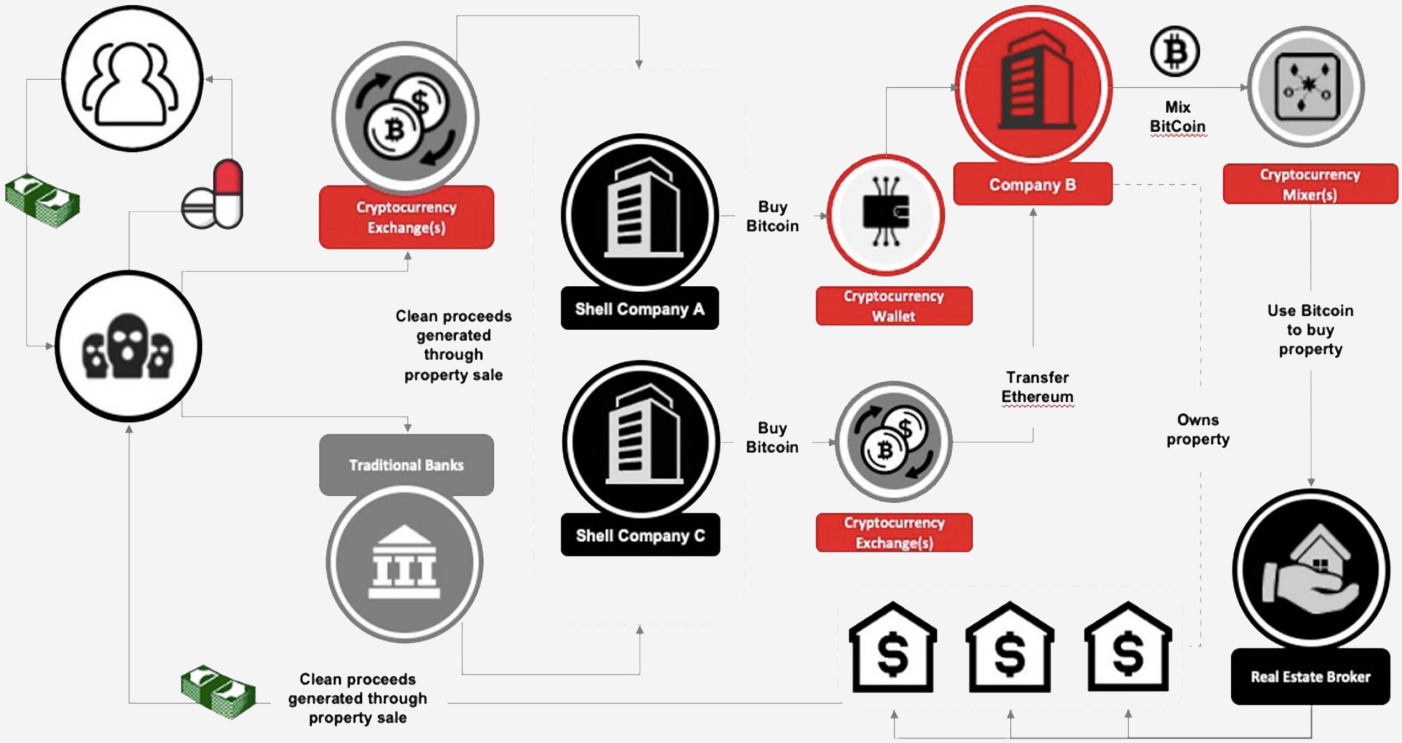
To support FI's and the private sector AML/CFT compliance efforts and enhance the ability to deter and detect ML/TF in the virtual sector, several key points should be followed and implemented:

- Develop or reassess the risk-based programs, policies and procedures to include the FATF recommendations.
- AML/CFT compliance needs to be consistent with local privacy laws.
- Perform an adequate and comprehensive AML Risk Assessment.
- Implement a customer risk-based approach including KYC, customer risk assessments, enhanced due diligence and ongoing due diligence policy and procedures.
- Include the identification and verification of beneficial ownership in the compliance procedures.
- Consider the adequacy of the number of qualified/experienced staff with appropriate authority and resources.

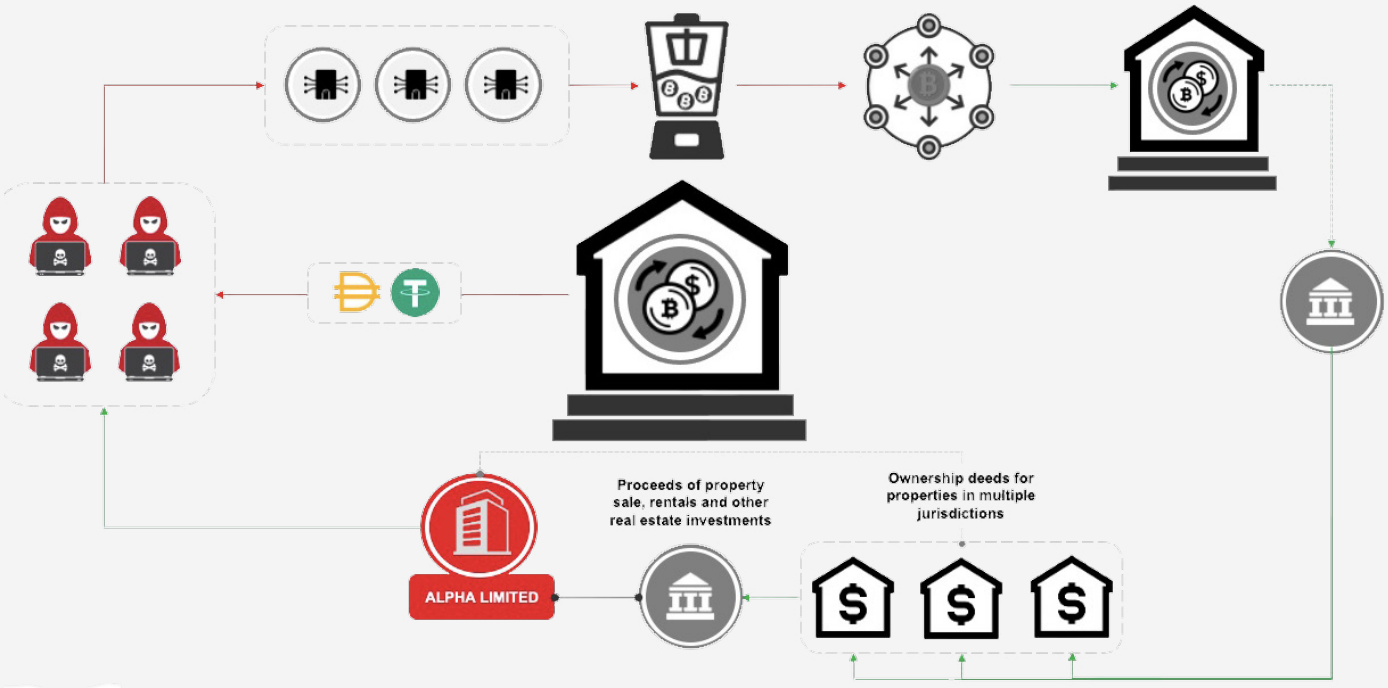
- Have dynamic and regularly checked PEPs and Sanction screening system.
- Implement training programs to assist employees with understanding the way VAs VASPs comply with AML/CTF regulation.
- Maintain informed and strong senior management leadership and oversight who prioritize AML/CTF compliance.
- Assess AML/CFT policies and procedures and conflicts with other policies and procedures.
- Establish internal controls such as CDD, record keeping, transaction monitoring, as well as independent testing (internal and external audit), and training provided to staff on AML/CFT.

Case Studies - The use of virtual currencies to launder money

Virtual currencies have many legitimate uses and benefits, including their potential to provide a cheap, fast, accessible and international payment system to millions of unbanked people worldwide. But like any store of value, they can be misused. Some cases involve criminals using virtual currencies to launder "normal" proceeds of crime or corruption. The case study outlined below describes one of the methods criminals use to wash money and try to hide the origin of the money through the real estate sector.



In recent years, not only virtual currencies but also the rapid rise of stablecoins has led to concerns about their role in financial crime. There are several features associated with stablecoins that can create money laundering and terrorist financing risks, such as:
1) Anonymity: enabling peer-to-peer transactions via the use of unhosted wallets, stablecoins can present elevated risks;
2) Global reach and potential for mass adoption: stablecoins are globally accessible and unconstrained by borders;
3) Layering: price stability of stablecoins can make an attractive way to layer proceeds of crime derived from more volatile cryptoassets. However, stablecoins possess a feature that can mitigate the risks unlike most censorship-resistant cryptoassets like Bitcoin: stablecoin transactions are reversible and allow their issuers to recover funds readily in cases of identified fraud or other criminality. Here below is an example of how hackers can steal stablecoins from exchanges, and launder the funds through various means.



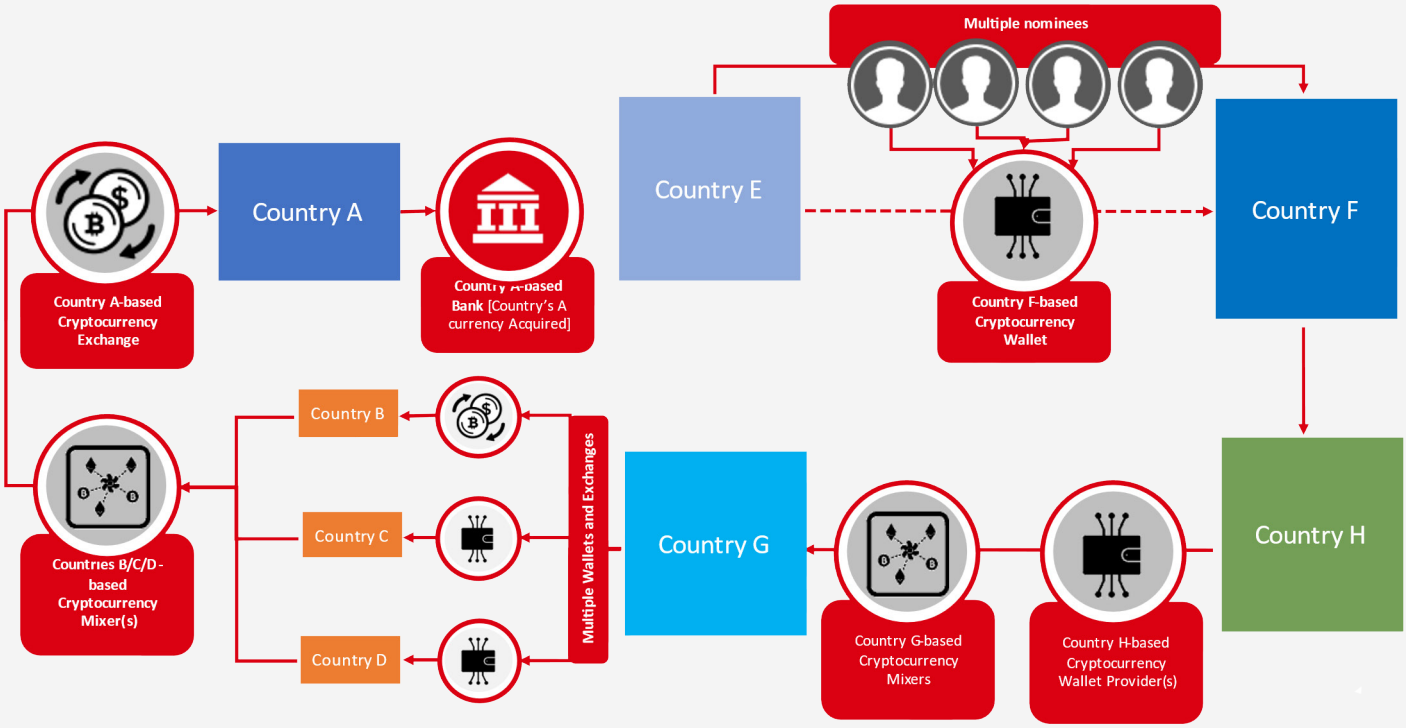
Case Study – The use of virtual currencies to evade sanctions

In year 2022, many analysts have observed that countries under international sanctions could revive their economies using virtual currencies. In fact, they are decentralized, meaning they are outside the control of central authorities, and would therefore allow local companies and individuals to evade sanctions and hold their assets in virtual currency.

Particularly, some experts pointed out that the sanctioned countries may have found a way to undermine sanctions through the use of virtual currency. The first method is through ransomware, that is limiting access to personal accounts with the subsequent ransom request for the release of personal data. A large number of payments are in fact made in virtual currencies and are exchanged on the dark web.

The second method is through mining, which is the validation of blocks of transactions in exchange for a profit. This process, which requires a significant amount of energy and computing power, has led many countries to invest in building larger servers in order to evade sanctions.

The case study outlined below analyzes a case of sanctions evasion through virtual currency wallets and exchanges.



Annex 1: Red Flag Indicators

1) Related to Transactions

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

Transferring virtual currencies immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; or there is non-existent or weak AML/CFT regulation.

Conducting virtual currency-fiat currency exchange at a potential loss.

Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same virtual currency account by more than one person; from the same IP address by one or more persons; or concerning large amounts.

Making multiple high-value transactions in short succession, such as within a 24-hour period; in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or to a newly created or to a previously inactive account.

Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most virtual currencies have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading.

Transactions involving the use of multiple virtual currencies, or multiple accounts, with no logical business explanation.

Converting a large amount of fiat currency into virtual currencies, or a large amount of one type of virtual currency into other types of virtual currencies, with no logical business explanation.

Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency.

2) Related to Anonymity

Transactions by a customer involving more than one type of virtual currency, despite additional transaction fees, and especially those virtual currencies that provide higher anonymity, such as anonymity-enhanced virtual currency (AEC) or privacy coins.

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

The use of decentralized/unhosted, hardware or paper wallets to transport virtual currencies across borders.

Moving a virtual currency that operates on a public, transparent blockchain, such as Bitcoin, to a centralized exchange and then immediately trading it for an AEC or privacy coin.

Abnormal transactional activity (level and volume) of virtual currencies cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.

The use of decentralized/unhosted, hardware or paper wallets to transport virtual currencies across borders.

Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.

Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication.

Receiving funds from or sending funds to VASPs whose CDD or KYC processes are demonstrably weak or non-existent.

Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.

A large number of seemingly unrelated virtual currency wallets controlled from the same IP-address, which may involve the use of shell wallets registered to different users to conceal their relation to each other.

3) About Senders or Recipients

Customer purchases large amounts of virtual currency not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.

Irregularities observed during account creation such as creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs; transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious; trying to open an account frequently within the same VASP from the same IP address.

Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.

A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.

Irregularities observed during CDD process such as 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.

Sender does not appear to be familiar with virtual currency technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers.

A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential ML scheme to obfuscate funds flow with a VASP infrastructure.

4) In the Source of Funds or Wealth

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

The use of one or multiple credit and/or debit cards that are linked to a virtual currency wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing virtual currencies are sourced from cash deposits into credit cards.

Virtual currency transactions originating from or destined to online gambling services.

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

Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.

5) Related to Geographical Risks

Customer utilizes a VA exchange in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.

Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing virtual currencies or sets up new offices in jurisdictions where there is no clear business rationale to do so.

Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.

Customer sends funds to VASPs operating in jurisdictions that have no VA regulation or have not implemented AML/CFT controls.