



EU AML / CFT
GLOBAL FACILITY

LEVERAGING BENEFICIAL OWNERSHIP TRANSPARENCY FOR VIRTUAL ASSETS

SEPTEMBER 2026



**Funded by
the European Union**

E EXPERTISE
FRANCE
GROUPE AFD

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

The European Union Global Facility on Anti-Money Laundering and Countering the Financing of Terrorism (EU AML/CFT Global Facility) is a technical assistance project supporting partner countries worldwide to strengthen their AML/CFT policy and operational frameworks.

Identified as the European Commission's mechanism to support countries engaged in strategic and operational AML/CFT reforms, the EU AML/CFT Global Facility offers various forms of technical assistance programs tailored to the partner countries' needs, on a demand-driven basis and in response to emerging threats.

The EU AML/CFT Global Facility project is funded by the European Commission and implemented by Expertise France.

Disclaimer:

This document has been prepared by Andres Knobel in the framework of the technical assistance programme provided by the EU AML/CFT Global Facility Project, financed by the European Union and implemented by Expertise France.

The views and opinions presented herein are those of the main author and should not be taken as to reflect the official position of the European Union and/or the EU AML/CFT Global Facility.

This document is a strictly confidential communication to and solely for the use of the recipient and may not be reproduced or circulated without the EU AMLCFT Global Facility project written consent.

If you are not the intended recipient, you may not disclose or use the information in this documentation in any way.

For further information, please contact:

European Union AML/CFT Global Facility Project
<https://www.global-amlcft.eu>
info@global-amlcft.eu

Igor Bereza, Key Expert on Beneficial Ownership
E-mail : ibereza@global-amlcft.eu

© **Visual credits:** Images licensed from Envato.

TABLE OF CONTENTS

Abbreviations and Acronyms	4
1. Introduction	5
1.1 Virtual assets	6
1.2 Transparency depends on the eventual involvement of a VASP or other obliged entities	7
2. The relationship between beneficial ownership transparency and FATF Recommendations for virtual assets	9
2.1 Overview	10
2.2 VASP Licensing and registration	11
2.2.1 Detecting foreign VASPs and non-compliant local VASPs	11
2.2.2 Challenges to register VASPs and to identify their beneficial owners based on the entity type	12
2.2.3 Special cases I: DeFi	13
2.2.4 Special Case II: Stablecoins	14
2.3 Customer Due Diligence	14
2.3.1 Exchange brokers	15
2.3.2 Complex structures to hold virtual assets	15
2.4 Travel Rule	16
2.4.1 Counterparty VASP	17
2.4.2 Transactions with unhosted wallets	18
2.4.3 Proposals to reduce risks	18
2.5 Politically Exposed Persons (PEPs)	18
2.6 Targeted Financial Sanctions (TFS)	18
3. Transparency Issues	19
3.1 Secrecy challenges that prevent identifying the beneficial owner	20
3.1.1 Foreign entities and other unregistered entities	20
3.1.2 Bearer shares	21
3.1.3 Nominees	21
3.1.4 Complex ownership structures	21
3.1.5 Types of entities used for virtual assets: pure DAOs and Hybrids	22
3.1.6 FATF Virtual Asset Red-flag indicators on anonymity	24
4. Typologies & Case Studies related to customer due diligence and beneficial ownership	26
4.1 Case study 1: Binance	27
4.1.1 Identifying entities part of the VASP group for sanction purposes	28
4.1.2 Identifying the location of the VASP and connections to different jurisdictions	28
4.1.3 Identifying beneficial owners and controllers of the VASP group for sanction purposes	29
4.1.4 Deliberate lack of CDD, STR filing and other AML obligations despite claims to the contrary	29
4.1.5 Financing of terrorism	31
4.2 Case study 2: Ilya Dutch Liechtenstein	31
4.3 Case study 3: professional investment scam	32
5. Complementary sources of information on virtual assets	33
5.1 The OECD's Crypto-asset reporting framework (CARF)	34
5.2 Local information disclosure regimes	37
6. How the EU Global Facility can Help	39

ABBREVIATIONS AND ACRONYMS

AML	Anti-Money Laundering
BO	Beneficial ownership
CARF	Crypto Asset Reporting Framework
CDD	Customer Due Diligence
CRS	Common Reporting Standard
DNFBP	Designated Non-Financial Business Person
EU	European Union
EUGF	EU AML/CFT Global Facility
FATF	Financial Action Task Force
FT	Financing of Terrorism
KYC	Know Your Customer
ML/TF	Money laundering and Terrorism financing
PEP	Politically Exposed Person
R.	Recommendation
STR	Suspicious Transaction Report
VASP	Virtual Asset Service Provider
TFS	Targeted Financial Sanction



EU AML/CFT
GLOBAL FACILITY

1. INTRODUCTION



Funded by
the European Union

1. INTRODUCTION

This report explains why beneficial ownership transparency is relevant to ensure compliance and risk mitigation regarding money laundering and terrorism financing risks involving virtual assets. Section 1 describes the concepts of virtual assets and virtual asset service provider (VASP) and their money laundering risks. Section 2 explores the relationship between beneficial ownership transparency (based on FATF Recommendations 24 and 25) and virtual assets to comply with FATF Recommendations 6, 7, 10, 12, 13, 15, 16, 22. Section 3 then explores the secrecy challenges that may affect beneficial ownership transparency and thus affect compliance with FATF Recommendations on virtual assets. Section 4 describes typologies and case studies to understand the relevance of beneficial ownership both to ensure compliance and to detect crimes. Section 5 proposes how cooperation with tax authorities may bring additional sources on the beneficial owners of virtual assets, and how money laundering authorities may get access to this information. Finally, Section 6 proposes ways in which the EU Global Facility may assist countries in this topic.

1.1 Virtual assets

Virtual assets (e.g. bitcoin) can be abused to engage in money laundering, and many of its predicate offences including tax evasion, fraud, corruption, as well as the financing of terrorism. Virtual assets are especially exploited in illegal activities including ransomware, hacks and fraud schemes through dating apps and social media. For this reason, since 2019 the Financial Action Task Force (FATF) made it explicit that virtual assets and their intermediaries (mainly virtual assets service providers, or VASPs) must also comply with AML/CFT requirements.

The FATF defines virtual assets as a digital representation of value that can be digitally traded or transferred and that can be used for payment or investment purposes (but excludes digital representations of fiat currencies or securities).

A VASP is defined as any natural or legal person that is not covered elsewhere under the FATF Recommendations (e.g. a traditional financial institution) and as a business that conducts one or more of the following activities or operations for or on behalf of another natural or legal person:



VA-FIAT EXCHANGE

Exchange services allowing users to convert virtual assets into fiat currencies, or fiat currencies into virtual assets.



VA-VA EXCHANGE

Exchange services allowing users to convert one form of virtual asset into another form of virtual asset.



TRANSFER

Transfer services enabling virtual assets to be moved from one person, wallet or account to another.



SAFEKEEPING & ADMINISTRATION

Safekeeping or administration services for virtual assets, including instruments that enable users to access or control those assets.



ISSUER-RELATED FINANCIAL SERVICES

Financial services supporting an issuer's offer or sale of a virtual asset, including participation in an initial coin offering.

As described by the 2021 FATF Guide on Virtual Assets, all FATF Recommendations apply to virtual assets and VASPs just as they apply to traditional financial assets and financial institutions.

However, many of the requirements must also be adapted to the specific circumstances of virtual assets. The features that exacerbate virtual assets ML/FT risks include their:



Global reach.

Virtual assets can be accessed across borders through foreign VASPs, often remotely and with limited identification where AML/CFT standards are weak or poorly enforced.



Rapid settlement.

Virtual asset transactions can settle almost instantly, especially with stablecoins, moving funds far faster than international bank transfers that may take one or two days.



Peer-to-peer (P2P) transactions.

Virtual assets enable direct peer-to-peer transfers without a financial intermediary, allowing high-value transactions to move rapidly across long distances and between different jurisdictions.



Increased anonymity and obfuscation of transaction flows.

Virtual assets can support complex transaction paths, mixers and privacy-enhancing tools, making ownership and the movement of funds significantly more difficult to trace.

1.2 Transparency depends on the eventual involvement of a VASP or other obliged entities

Virtual asset transparency cannot be guaranteed in all cases. Even if a country fully complied with FATF Recommendations, not all virtual asset transactions will be covered by AML regulations to ensure that their customers (users, owners) will be identified. Virtual asset transactions can take place without the use or involvement of a VASP or a financial institution, such as a P2P transaction where users send virtual assets from an unhosted wallet to another unhosted wallet. However, the system relies on the fact that at some point, a VASP will be involved, for instance an Exchange VASP to convert the virtual assets into fiat currency to use it in the real world. In that moment, proper customer due diligence (CDD) / Know-your-customer (KYC) provisions and other mitigation measures will be applied to prevent money laundering and other crimes.



Box 1. The risk of Stablecoins to the AML preventive system

Stablecoins are virtual assets whose value is pegged to the value of some other value, e.g. a fiat currency, such as the US dollar, or pegged to the value of other virtual assets or of commodities such as gold. This stability related to the value of a fiat currency makes the value of stablecoins much less volatile than other virtual assets, and hence in recent times, their use has largely increased, also for illicit financial flows.

As the FATF warned, if regular business (from the real economy) start accepting payments in stablecoins, then stablecoins stored in unhosted wallets could potentially be used to purchase goods and services without needing to first convert them into fiat currency through an Exchange (e.g. a type of VASP). A mass adoption of stablecoins could potentially decrease the use of obliged-entities-VASPs, so there may be no point when users are identified, creating a higher risk for illicit financial flows.





EU AML/CFT
GLOBAL FACILITY

2. relationship between beneficial ownership TRANSPARENCY AND FATF RECOMMENDATIONS FOR VIRTUAL ASSETS



Funded by
the European Union

2. The relationship between beneficial ownership transparency and FATF Recommendations for virtual assets

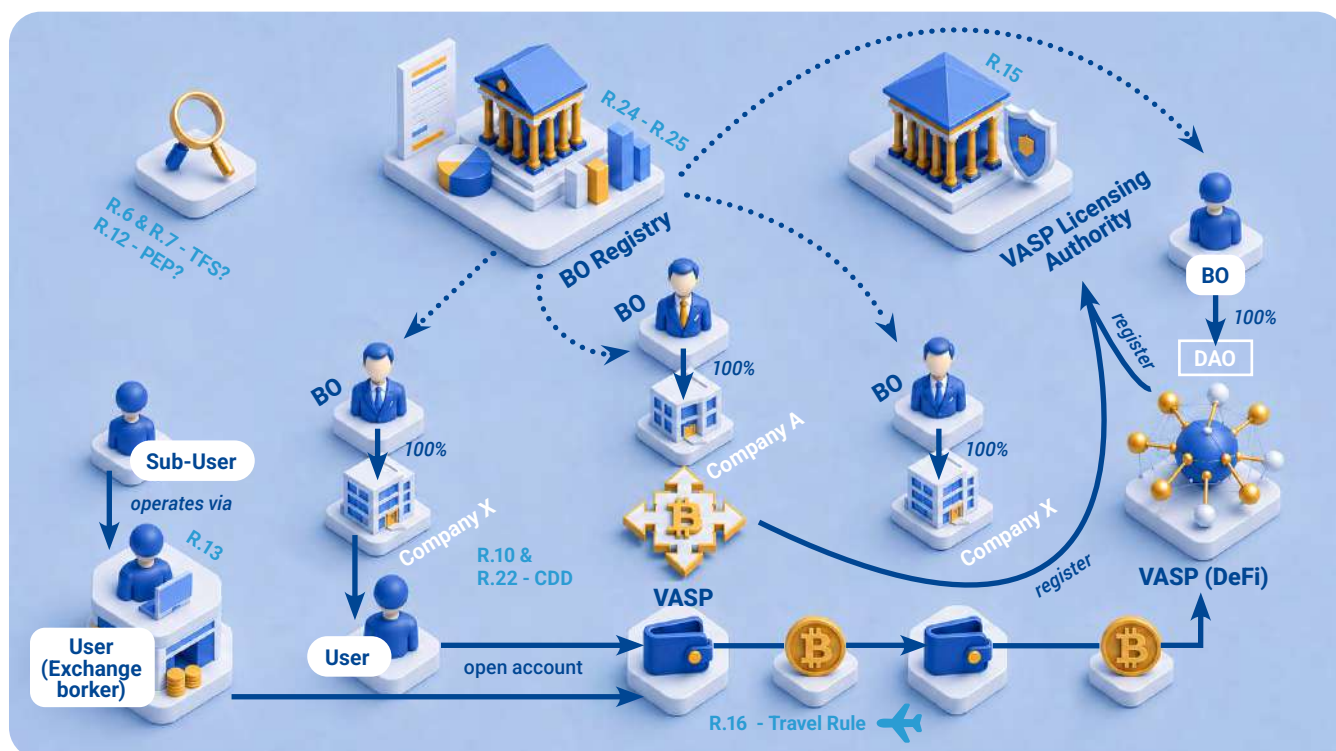
2.1 Overview

As described by the next figure, beneficial ownership transparency is particularly relevant for virtual assets to comply with FATF requirements in the following scenarios:

- **VASP Licensing or Registration.** FATF R.15 requires VASPs to register or license for it to be able to offer their services in the country or to users located in the country.
- **Customer due diligence.** FATF R.10 and R.22 (as VASPs may also be natural persons) establish customer due diligence (CDD) obligations for financial institutions and designated non financial business and professionals (DNFBPs) such as lawyers, to identify their customers when opening accounts or conducting transactions above a certain threshold. These CDD obligations require, among others, to determine the origin of the funds and to identify the customer, including its beneficial owners. In the context of virtual assets, these obligations apply to VASPs regarding their customers (sometimes referred to as “users”).
- **Travel rule.** FATF R.16 requires VASPs to establish the travel rule, mainly to identify the identity of the originator and beneficiary (not necessarily at the beneficial ownership level). In addition, VASPs must notify the beneficiary VASP this information, so that the full chain of transfers can be tracked in case of multiple transactions.
- **Correspondent banking rules.** In nested relationships where a VASP holds an account at another VASP (e.g. a user of a VASP as an Exchange Broker), countries should implement the preventive measures in FATF R. 13 to VASPs.
- **Identification of Politically Exposed Persons (PEPs).** FATF R.12 requires obliged entities (including VASPs) to identify PEPs as part of the risk-based approach. Based on the identity and beneficial ownership information collected as part of CDD and travel rules, VASPs are able to check if any PEP is involved in a virtual asset transaction.
- **Targeted financial sanctions.** FATF R.6 and R.7 require obliged entities (including VASPs) to comply with targeted financial sanctions established by the UN and other relevant bodies to prevent the financing of terrorism and proliferation, respectively. Based on the identity and beneficial ownership information collected as part of CDD and travel rules, VASPs are able to check if any sanctioned individual appearing on a relevant list is involved in a virtual asset transaction.
- **Beneficial ownership transparency.** FATF R.24 and R.25 require beneficial ownership registries and other transparency mechanisms to ensure availability of adequate, accurate and up-to-date beneficial ownership information. These sources of beneficial ownership may support both government authorities (e.g. VASP licensing agency) and obliged entities (e.g. VASPs) to identify and verify beneficial ownership information of virtual assets.



Figure 1. Overview of beneficial ownership transparency related to virtual asset requirements



Source: elaborated by author

2.2 VASP Licensing and registration

Based on FATF R.15, at a minimum, VASPs should be required to be licensed or registered in the countries where they are created. This could be based on their country of incorporation, or where they are registered in the commercial register, where they file the company bylaws or articles of incorporation, or where they obtain a tax identification number.

VASPs should also be licensed or registered when they are physically located in a jurisdiction (particularly for natural persons, who should otherwise be licensed where their place of business is located).

In addition, 35 of 96 jurisdictions with licensing requirements for VASPs reported taking a more extensive approach by requiring offshore VASPs (that are not created or located in their jurisdictions) to be licensed/registered if VASPs meet certain other requirements such as offering their services to local users, having a locally-hosted web address (XXX.com.country-code, e.g. uk), or that passes a value transaction threshold involving local users).

From a beneficial ownership transparency perspective, licensing is relevant because it allows authorities to check and to prevent criminals or their associates from becoming legal owners or beneficial owners of a significant/controlling interest in a VASP, or from holding a management function. Likewise, countries should also identify (and sanction) natural or legal persons that carry out VASP activities without the proper licensing.

2.2.1 DETECTING FOREIGN VASPs AND NON-COMPLIANT LOCAL VASPs

To prevent users from achieving secrecy by conducting virtual asset operations through unlicensed local VASPs and through offshore VASPs, countries are encouraged to also license foreign VASPs and enforce compliance of covered VASPs. The criteria to license foreign-incorporated VASPs offering products and services to local users, could include:

- the location of offices and servers including call centres,
- advertising targeting local users,
- the language on the VASP website and/or mobile apps,
- whether the VASP has a local intermediary to seek or

- visit local clients
- whether the VASP has commercial agreements with local financial institutions.

To detect unlicensed local VASPs and offshore VASPs (as well as local financial institutions offering virtual asset services), authorities could use:

- blockchain analytics to discover wallets with high activity,
- web-scraping and open-source information to

- discover VASPs offering their services to local users
- STRs received by the FIU
- information on license rejections (as they may decide to operate regardless)
- international cooperation

Although not explicitly mentioned by the FATF, jurisdictions could also consider whistleblower programs, anonymous reporting and mystery shopper schemes to detect non-compliant VASPs that fail to license or register.



Beneficial ownership tool: foreign ownership registries

Foreign commercial and beneficial ownership registries, especially if they offer free and online public access, may help identify the country of incorporation of the foreign VASP to send notifications and for enforcement purposes.

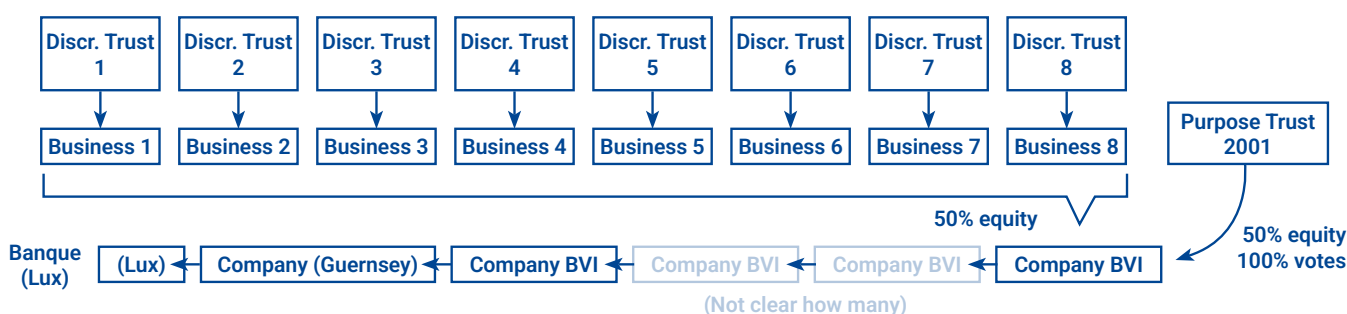
2.2.2 CHALLENGES TO REGISTER VASPs AND TO IDENTIFY THEIR BENEFICIAL OWNERS BASED ON THE ENTITY TYPE

After overcoming the challenge of detecting the VASP and establishing a link to the jurisdiction (see the point above), registration of the VASP may depend on how the VASP is organised. On the one hand, the VASP may be using sophisticated types of entities that are not available nor known by most jurisdictions, including an LLC, a “purpose trust”, a private interest foundation, a Cayman “company foundation” or even structures without any legal form at all, such as a pure decentralised autonomous organisation (DAO). On the other hand, regardless of whether the VASP is organised as a regular structure, such as a company, or as a sophisticated purpose trust, its ownership structure

may be very complex. In all of these cases, it may be hard to determine the beneficial owners (and controllers for liability purposes), especially if there are no local guidelines.

Complex ownership structures are widespread. For instance, in the case of a traditional financial institution from Luxembourg under scrutiny for some of its customers, the ownership structure was very long and complex, involving offshore entities and sophisticated types of trusts such as discretionary trusts and purpose trusts. Authorities will need to understand how to navigate these structures to identify the main controllers and beneficial owners to run the “fit and proper test” as well as to check that they are not designated individuals, etc.

Figure 2. Example of complex ownership structure of bank in Luxembourg



Source: Knobel, A., “Complex ownership structures”, TJN, 2022

Likewise, in the famous Russian Laundromat involving Moldova, a financial institution involved in the scheme was controlled based on a strategy designed to circumvent reporting requirements. Because banking regulations

required identifying individuals who owned more than 5% of a banking institution, shareholdings were deliberately fragmented to own between 4.88 and 4.9% to stay just below the threshold¹.



Beneficial ownership tool: beneficial ownership registries

Beneficial ownership transparency can help address these issues. First, authorities dealing with beneficial ownership registration may have experience analysing complex ownership structures to detect risky schemes. Second, beneficial ownership registries may help determine and verify the beneficial owners and controllers of VASPs, to ensure they aren't criminals. For effective transparency, countries could expand beneficial ownership registration to cover foreign legal persons and arrangements that conduct VASP activities or generally conduct local operations.

2.2.3 SPECIAL CASES I: DEFI

Decentralised Finance (DeFi) refers to decentralised and/or disintermediated applications that offer financial services on a settlement platform (usually using blockchain) to undertake payments, lending, trading, investments, insurance and asset management of virtual assets.

According to the FATF, a DeFi application (i.e. the smart contract) is not a VASP because FATF Recommendations do not apply to underlying software or technology. However, if the DeFi provides or actively facilitates VASP services (even based on automated processes), then it may be required to be licensed. Around half of countries with VASP registration are requiring certain DeFi arrangements to be licensed or registered as a VASP based on the location where the creator, owner or operator maintains control or sufficient influence in the arrangement.

Beneficial ownership transparency may be relevant, as countries could need to identify the creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements. However, in this case, the "control" analysis may be based not just on company statutes, but also based on the smart contract's terms to understand who may change the rules or who are benefitting from the application, such as receiving a fee or profit out of every transaction.



Based on the FATF, owners/operators of a DeFi arrangement may be those who have control or sufficient influence over assets or over aspects of the service's protocol (e.g. based on having special tokens), and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or through voting protocols. Other factors to determine who should be identified may include those who profit from the service or have the ability to set or change parameters of a DeFi arrangement.

¹ Kroll, Project Tenor, Summary Report

2.2.4 SPECIAL CASE II: STABLECOINS

In the case of stablecoins, they should register or get a license as a VASP when there is central developer or governance body of the stablecoin. According to the FATF, a governance body consists of one or more natural or legal persons who, among

others, establish the rules governing the stablecoin arrangement (e.g., determine the functions of the stablecoin, who can access the arrangement and whether/how AML/CFT preventive measures are built into the arrangement).



CONCLUSION – Identifying and enforcing licensing and registration requirements for VASPs may be challenging. Beneficial ownership transparency can help identify the main owners and controllers, or at least serve as a basis on how to determine who is in control or benefitting from a virtual asset arrangement or business. In these cases where it is hard to determine whom to identify, the FATF proposes to consider issues that are typical beneficial ownership criteria, including:

- who profits from the use of the service or asset,
- who established and can change the rules,
- who can make decisions affecting operations,
- who generated and drove the creation and launch of a product or service,
- who maintains an ongoing business relationship with a contracting party or another person who possesses and controls the data on its operations, and,
- who could shut down the product or service.

2.3 Customer Due Diligence

The FATF requires that VASPs establish customer due diligence (CDD) process to help them assess the ML/TF risks associated with covered virtual asset activities or business relationships or occasional transactions above the applicable threshold. These CDD requirements involve identifying the customer and its beneficial owners, and verifying the customer's identity on a risk basis and on the basis of reliable and independent information.

In addition, in the context of enhanced due diligence, VASPs may be required to collect additional information, including the purpose of transaction,

proof of funds ownership, parties to the transaction and the relationship between them, sources of wealth, or the identity and the beneficial ownership of the counterparty. For these purposes, using beneficial ownership registries may help determine and verify the beneficial owners, both of users and their counterparties.

While commercial registries and beneficial ownership registries may help VASPs identify their customers and apply CDD, there are common shortcomings to ensure information in these registries is available, easily accessible and verified.

In addition to these general shortcomings, there are additional circumstances that may increase secrecy risks of VASP customers: exchange brokers and complex ownership structures to hold virtual assets.



2.3.1 EXCHANGE BROKERS

As described below in the Binance case study, customers of a VASP may use their accounts in the VASP as an omnibus account allowing many other sub-customers to operate that account. In this case, these customers are in fact exchange brokers who allow new customers (sub-customers) to operate virtual assets without identifying themselves with the VASP. In other words, while the VASP should have obtained identity information on the customer and its beneficial owners, it may have no data on the customers of its customer. This creates a major money laundering risk.

As proposed by the 2021 FATF Guidance on Virtual assets, a VASP offering services to another VASP (or exchange broker) should apply the correspondent banking rules of FATF R. 13, including:

- obtain information about the other VASP (or Exchange Broker-User) to understand their reputation, business, and types of customers,
- assess the other VASP's AML/CFT controls
- be satisfied that the other VASP has conducted CDD on their own customers and is able to provide relevant CDD information on request.

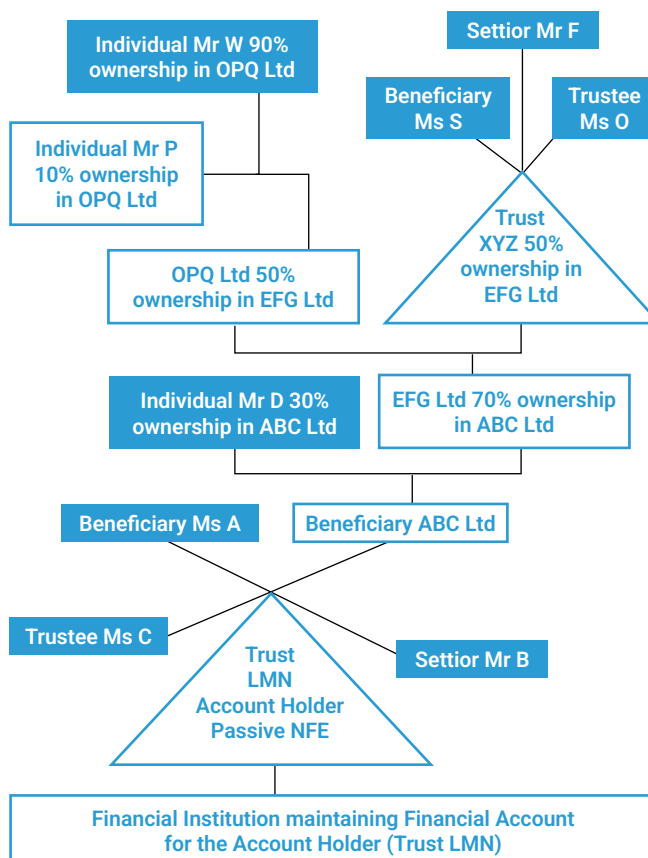
Another solution is for the VASP to directly identify any sub-customer before they may operate in the VASP.

2.3.2 COMPLEX STRUCTURES TO HOLD VA

Customer of virtual assets may set up very complex structures to hide their ownership and control. Although based on some typologies described below, ownership and control of virtual assets seem to be rather simple and straightforward (at most using one entity to hold the account), the experience with more traditional financial assets suggests that holders of bank accounts can be very complex. One possibility is that customers are using simple structures to hold their virtual assets because they are already enjoying a high degree of secrecy and lack of reporting. However, this secrecy may be reduced, as more countries start licensing and registering VASPs, and these VASPs start applying CDD requirements. In the near future, customers of VASPs may also start using more complex structures to hold their virtual assets.

For instance, the OECD Guidelines on automatic exchange of foreign account information, describes the following structure where companies and trusts are combined to hold financial accounts:

Figure 3. Complex ownership structure to hold financial accounts



Source: OECD Common Reporting Standard (CRS) Handbook

2.4 Travel Rule

As described by the next figure, FATF R.16 requires countries to ensure that originating Virtual Asset Service Providers collect accurate originator information and beneficiary information on all virtual asset transfers (regardless if between two local VASPs). They should also submit that information to the recipient VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. The recipient VASP must equally ensure that they receive the Travel Rule information, and check for accuracy. For instance, the sending VASP will inform the identity of the beneficiary (recipient user). Because the recipient VASP should have applied CDD, it can verify if the beneficiary named by the sending VASP regarding that wallet/account, corresponds to the CDD information collected on that wallet/account.

Specifically, the Travel Rule information to be collected by the sending Virtual Asset Service Provider (and

submitted to the receiving VASP) includes:

- originator's name (i.e., the sending person's accurate (i.e. verified) full name)
- originator's "wallet address" of the virtual asset
- originator's physical (geographical) address (verified during CDD), or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth.
- beneficiary's name (identified by the originator user as the receiver of the virtual asset transfer). [While the accuracy of the name need not be verified by the sending VASP, the receiving VASP may check if it coincides with the CDD information they collected. The unverified name should be checked for STR and TFS purposes]
- beneficiary "wallet address".

Figure 4. Travel Rule obligations for ordering and recipient VASPs

Data item and required action	Ordering VASP	Beneficiary VASP
Originator Information	Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory. Accurate, i.e. the <u>ordering VASP needs to verify the accuracy as part of its CDD process.</u>	Required, i.e. the beneficiary VASP needs to <u>obtain the necessary data from ordering VASP.</u> Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP.
Beneficiary Information	Required, i.e. <u>submitting the necessary data to the beneficiary VASP is mandatory.</u> Data accuracy is not required, but the ordering VASP must <u>monitor to confirm no suspicions arise.</u>	Required, i.e. the beneficiary VASP needs to <u>obtain the necessary data from the ordering VASP.</u> Accurate, i.e. the beneficiary VASP must have verified the necessary data and <u>needs to confirm if the received data is consistent.</u>
Actions required	Obtain the necessary information from the originator and retain a record. Screen to confirm that the beneficiary is not a sanctioned name. Monitor transactions and report when they raise a suspicion.	Obtain the necessary information from the ordering VASP and retain a record. Screen to confirm that the originator is not a sanctioned name. Monitor transaction and report when it raises a suspicion.

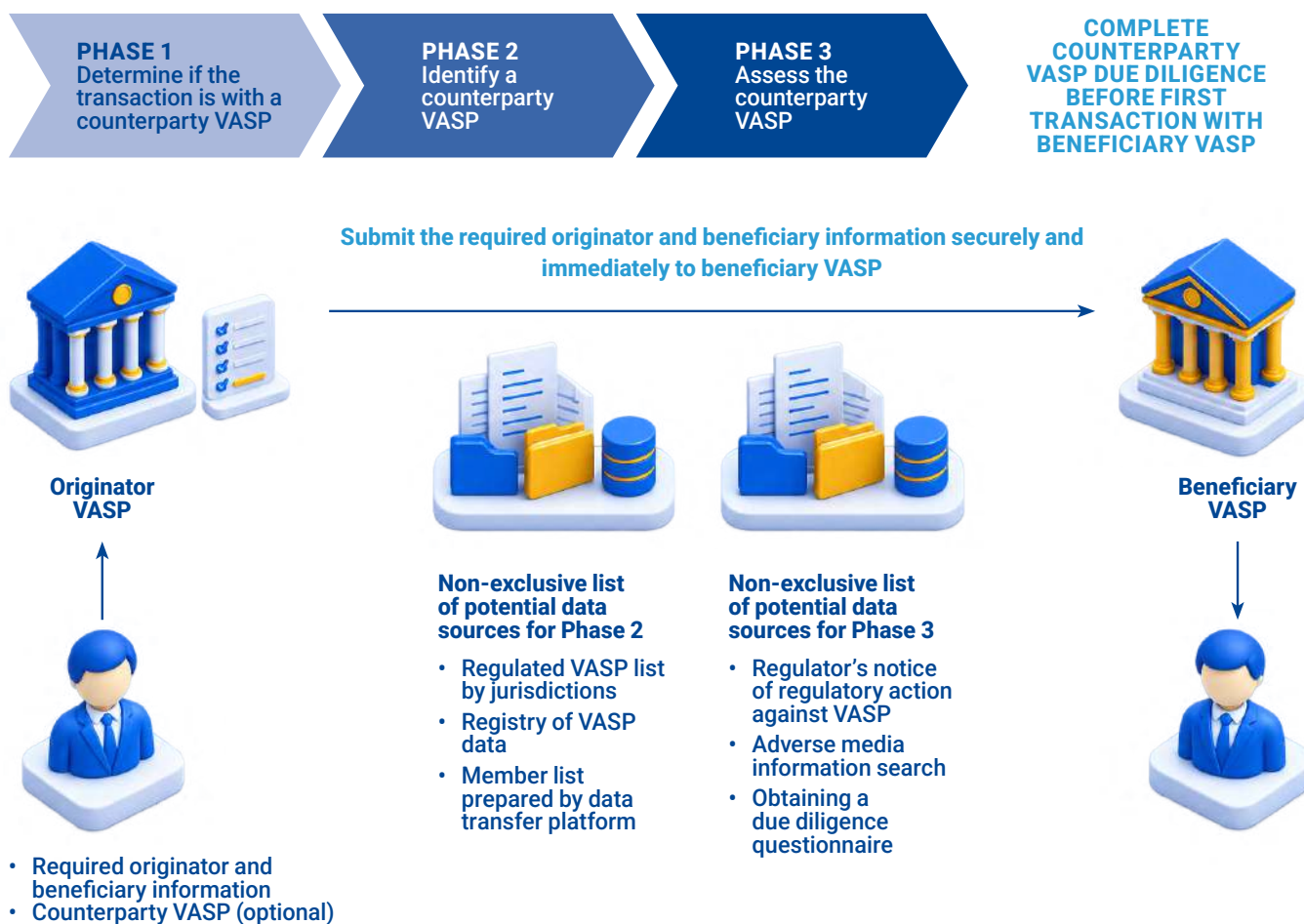
Source: FATF

2.4.1 COUNTERPARTY VASP

As the next figure explains, before sending Travel Rule information to the receiving VASP, the sending VASP should verify that the recipient is indeed a VASP and that it is not owned or controlled by criminals or sanctioned individuals or beneficial owners. Thus, the sending VASP should conduct CDD on their counterparty VASP (Phase 2 in the figure) to ensure that its ownership and control is acceptable before the Travel Rule information can be submitted to them. In this case, the sending VASP may require the counterparty VASP to share its legal and beneficial ownership information. The FATF recognises that commercial registries and beneficial ownership registries may be helpful for this purpose, in addition to other sources, such as a national list of licensed VASPs.



Figure 5. Process to check counterparty VASP before submitting Travel Rule information



Source: FATF

2.4.2 TRANSACTIONS WITH UNHOSTED WALLETS

Importantly, VASPs should collect the required originator and beneficiary information even when conducting a transfer between their user and an unhosted wallet, and in such case check the ownership of unhosted wallets for STR and TFS purposes before conducting the transaction.

As for recipient VASPs receiving transfers from an unhosted wallet, they should obtain from their own customer the identity information on the originator of the transfer, as there is no sending VASP to submit the Travel Rule information.

2.4.3 PROPOSALS TO REDUCE RISKS

Because users may engage with unlicensed VASPs or unhosted wallets, countries could reduce these risks by requiring licensed VASPs to only engage in transactions with (i) licensed/registered foreign VASPs and/or compliant with the travel rule, or (ii) foreign VASPs that in their countries are both licensed/registered and compliant with the Travel Rule.

In addition, the 2026 FATF “Targeted Report on Stablecoins and Unhosted Wallets” proposes also harsher measures, including to prohibit or deny licenses to platforms that allow transfers to unhosted wallets, or in the case of stablecoin issuers, to apply “whitelisting” and “blacklisting”. These work by “adding an access control list to the stablecoin smart contract; if the wallet address sending/receiving the stablecoin is not on the access control list, the transaction is automatically rejected. CDD requirements, either performed directly by the stablecoin issuer or by an approved third-party provider, can be included as part of the pre-approval process and periodically repeated as necessary to fulfil ongoing due diligence obligations...[or blacklisting,] where the stablecoin issuer adds a deny control list to the stablecoin smart contract; if the wallet address ending/receiving the stablecoin is on the deny control list, the transaction is automatically rejected”¹. Similar requirements could be imposed on VASPs in case they are going to send or receive transactions from “unknown” wallets, although implementation of these white and blacklists for VASPs may be more challenging than just amending a smart contract.

2.5 Politically Exposed Persons (PEPs)

FATF R.12 expects countries to require VASPs to have appropriate risk management systems in place to determine whether users or their beneficial owners are domestic or foreign politically exposed persons (PEPs) or related or connected to them. In such case, they should take additional measures such as identifying the source of funds.

In this case, beneficial ownership registries may help determine and verify the identity of the beneficial owners of users to check if they are local or foreign PEPs.

2.6 Targeted Financial Sanctions (TFS)

FATF Recommendations 6 and 7 require countries to screen transfers to ensure they do not involve sanctioned individuals. These should also cover transactions with virtual assets. Related to the travel rule mentioned above, identifying users and their beneficial owners, both the user of a VASP and the counterparty of a transaction, enables VASPs to screen transactions and apply corresponding freezing actions, if applicable.

¹ Page 25.



EU AML/CFT
GLOBAL FACILITY

3. TRANSPARENCY ISSUES



**Funded by
the European Union**

3. TRANSPARENCY ISSUES



As explained before, beneficial ownership information can help enforce FATF requirements including:

- VASP licensing and registration by countries
- Conducting CDD on counterparty VASP by each VASP for Travel Rule purposes
- Conducting CDD on their customers by each VASP
- Using collected beneficial ownership information to check for TFS and STR purposes by each VASP
- Applying correspondent banking requirements to a VASP'S nested accounts (accounts held by Exchange Brokers who have their own customers).

FATF R.24 and R.25 on beneficial ownership transparency requirements for legal persons and legal arrangements can become a source of beneficial ownership information to help both country authorities as well as VASPs obtain and verify beneficial ownership data.

In essence, R.24 & R.25 require countries to ensure availability and access by competent authorities to adequate, accurate and up-to-date information on legal owners and beneficial owners of legal persons (e.g. companies, foundations, partnerships)

and legal arrangements (e.g. trusts, fideicomisos, fiducies, waqfs).

In the case of legal persons, R.24 requires countries to establish a multipronged approach and ensure access to beneficial ownership information directly from the entity, from obliged entities and establishing a beneficial ownership registry or equally effective alternative mechanism. In the case of legal arrangements, local trustees (or equivalent) should collect beneficial ownership and make information on request to authorities, although they may also establish trust registries, or expand beneficial ownership registration also for trusts.

3.1 Secrecy challenges that prevent identifying the beneficial owner

3.1.1 FOREIGN ENTITIES AND OTHER UNREGISTERED ENTITIES

While VASPs and their customers may be organised as local or foreign entities, beneficial ownership

registries tend to cover only very few types of entities. Many of them cover only legal persons (but not trusts), or only companies. In addition, entities not considered legal persons (e.g. limited partnerships) may remain outside the scope.

While the 2022 revision of R.24 expanded beneficial ownership registration also for foreign legal persons that create money laundering risks and have a link to the country, it is up to each country to decide what that link will be. The FATF offers some suggestions, such as having local assets, engaging in operations with obliged entities, having local investments, employees or being a tax resident. However, it is not necessarily the case that a foreign entity that is operating as a local VASP or that opens an account with a VASP will be covered by local beneficial ownership registration requirements.

3.1.2 BEARER SHARES

Bearer shares are instruments that give ownership rights over a company to whomever is holding the paper-based bearer share at any given time. That makes it impossible for authorities to know who the owner is. The revised R.24 prohibits issuing new bearer shares and requires mitigating measures for pre-existing bearer shares such as converting them, registering them or immobilising them with a custodian. However, not all countries are complying with these obligations. While many countries prohibit local companies from issuing bearer shares, they tend not to prohibit or control whether foreign companies that issued bearer shares are directly or indirectly holding interests in the country's local companies.

3.1.3 NOMINEES

Nominees are individuals, or entities, who professionally or informally offer their name to appear as the legal owner of entities. The main challenge created by nominee individuals, is that they may appear as the real beneficial owner, unless one knows that they are just nominees. The revised R.24 proposes measures to address the risk of nominees, such as prohibiting them, requiring them to obtain a license/registration, or notifying their status to the entity and to the commercial register and to identify their nominator.



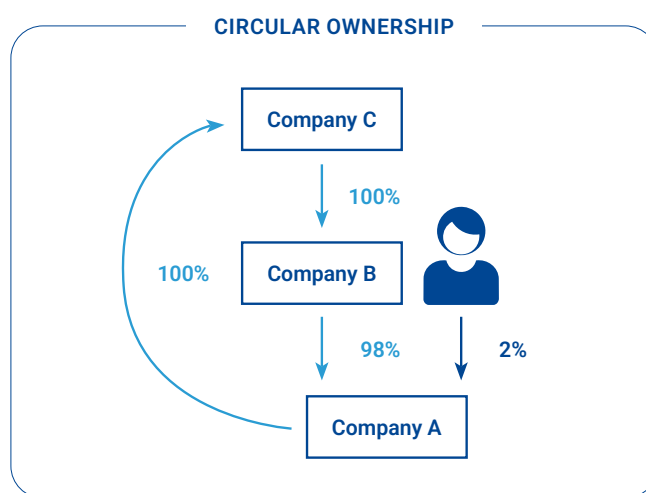
3.1.4 COMPLEX OWNERSHIP STRUCTURES

All of the challenges mentioned above may be combined to exacerbate the secrecy challenges that prevents identifying and confirming the beneficial owner of

a structure, especially if they involve many layers of entities, circular structures, pyramidal structures with fragmented ownership, the combination of trusts and legal persons as described below.

A circular structure may give the impression that there are no beneficial owners because no one passes the threshold (even though an individual with just 2% may be the only natural person in the structure). Likewise, a complex and long ownership chain involving foreign layers may become a circular structure where no individual exists at all (only companies owning each other).

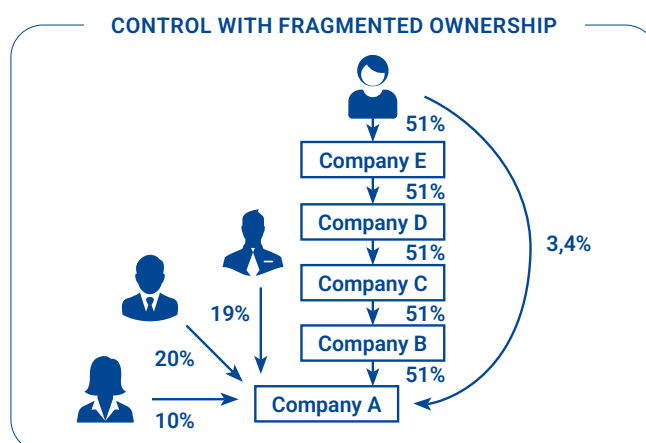
Figure 6. Circular ownership structure



Knobel, A., "Complex ownership structures", TJN, 2022

A pyramidal structure giving full control to an individual on top of the chain may be disguised (unless the full ownership chain is disclosed). In such case, the individual may claim not to be a beneficial owner for having even less than 5% of the shares, indirectly.

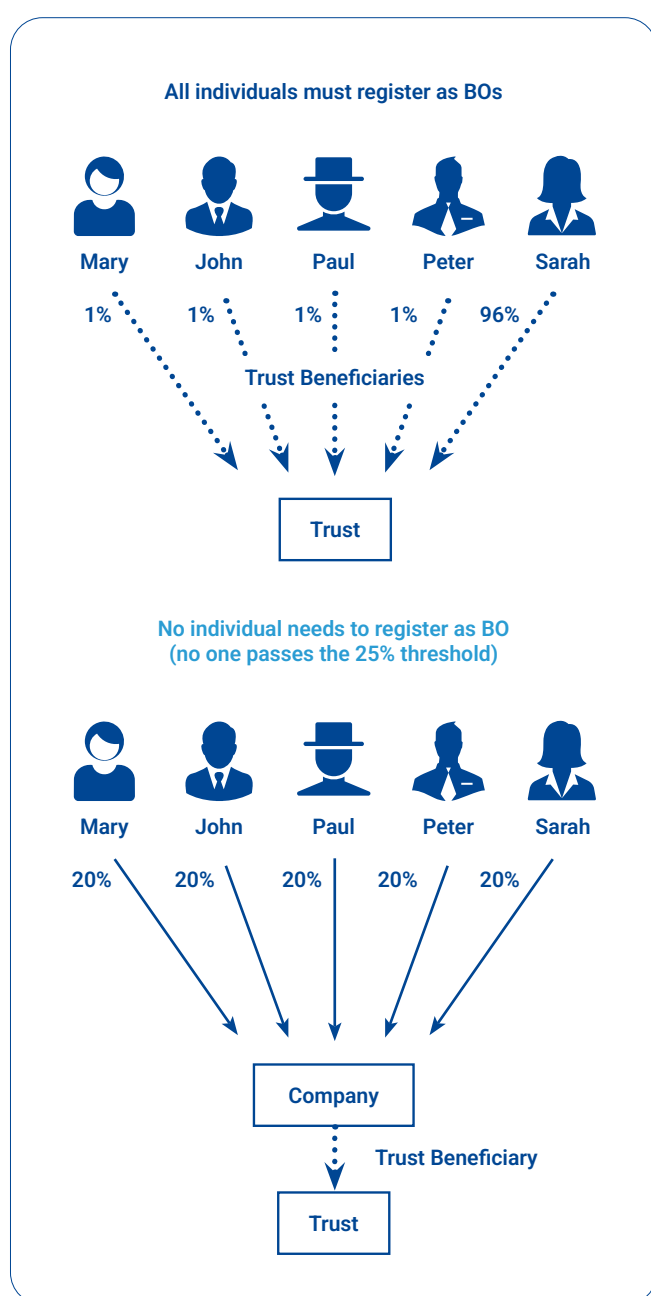
Figure 7. Pyramidal structure



Source: Knobel, A., "Complex ownership structures", TJN, 2022

Trusts and companies can be combined to prevent individuals from being identified. In the case of trusts, thresholds do not apply: all individuals should be identified as beneficial owners of the trust. However, by interposing a company as a trust party, thresholds are de facto imposed. This way, individuals who would have been identified if directly being parties to the trust, avoid registration for not passing the threshold to be identified as the beneficial owner of a company.

Figure 8. Combination of legal persons and trusts



Source: Knobel, A., "Complex ownership structures", TJN, 2022

3.1.5 TYPES OF ENTITIES USED FOR VIRTUAL ASSETS: PURE DAOS AND HYBRIDS

While the above cases referred to the combination of different types of common legal persons such as companies, in the virtual world, especially for DeFi applications, a non-entity structure can also be used: the decentralised autonomous organisation (DAO).

3.1.5.1 Pure DAOs

DAO stand for decentralised autonomous organisation ("DAO") which is rather a new type of online organisation using rules set out in computer code, rather than a real legal structure like a company or partnership. The goal of DAOs is to offer a more equitable and transparent business structure, relying more on technology than on humans' discretion and institutional intermediaries. DAOs are intended to offer participants with interests (tokens) in the DAO the opportunity to vote to determine the direction of the organisation's activities and governance, without necessarily knowing who these individuals are (as long as they prove to own the token to vote).

In case of a pure "DAO", it must be up to authorities and courts to determine who should register and how should be held liable, for instance if the DAO is found to be engaging in illegal activities, such as facilitating money laundering. In such case, authorities will first need to determine what is the closest entity type that looks like that specific DAO, especially to determine liability. For example, courts and experts have proposed that the DAO could be considered an "unincorporated association", a general partnership, or a trust.

3.1.5.2 Hybrids

Although DAOs could remain in the virtual world, whenever they interact with the real world or engage in transactions that could require regulation, they may need to organise in some type of legal entity, so they may incorporate a company such as an LLC. This process is called "wrapping" the DAO and it facilitates accountability, limiting liability of members, and complying with tax and other obligations.

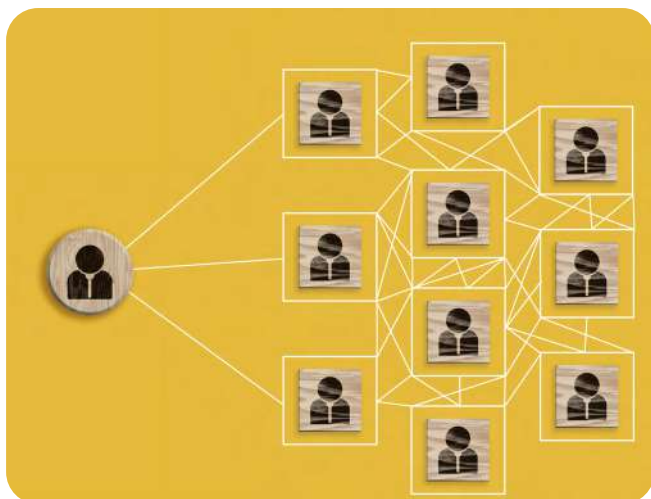
Hybrid DAOs usually choose specific types of entities or a combination thereof, including a US LLC, a purpose trust (e.g. from Guernsey), a Cayman "foundation company", or a private-interest foundation (e.g. from Panama) or a DAO-LLC from some US States (e.g. Wyoming).

From a beneficial ownership perspective, the wrapping of a DAO facilitates the determination of beneficial

owners and controllers, as entities tend to have more centralisation and specific roles, as well as country guidelines on who to register. However, beneficial ownership transparency should not limit itself to identifying the beneficial owners of legal structures, as there may be more individuals with control over the DAO even if they aren't part of the incorporated legal entities related to the DAO structure.

3.1.5.3 The DAO Structure

Most DAOS will have at least the DAO for governance (code establishing rules and processes for token holders to propose measures or projects, and cast a vote to approve them) and a Treasury DAO, that contains a number of different types of virtual assets. The DAO treasury's virtual assets are held on-chain in one or more wallets (which may be a multi-signature wallets) which are controlled by smart contracts.



The DAO structure may then involve a combination of legal entities and residual DAO structures. On the one hand, in a "fully wrapped DAO", a legal entity such as an LLC includes all the DAO functions. Token holders are members (or shareholders) in the entity, and even though they may vote on-chain, the legal entity's managers or directors will actually (manually) undertake actions.

Alternatively, the DAO may continue pure, except for the treasury functions and other managerial issues, which would be done through a legal entity (e.g. LLC) to protect the managers from liability. Although token holders may also be considered to have control (because they vote), they would lack the benefit of limited liability for not being members of the legal entity.

In a more complex case, the structure may involve a separate legal entity (or purpose trust) for each of the main activities of the DAO: one entity/purpose trust for protocol security, one for grant distribution (e.g. token holders voting to fund or invest in a specific project), one for property holding, and one for protocol liquidity. Each separate legal entity will conduct these activities on behalf of the DAO (based on what the token holders voted to do).

3.1.5.4 The beneficial owners of a DAO

Although there are not necessarily rules on who should be identified as a beneficial owner of a DAO, there are some indicators that may be used. While many functions may be automated via smart contracts, humans are likely to continue to be involved in some roles, such as software development (to fix or update the code itself), legal advice, tax, accounting, etc. In this case, it may depend on the different level of control by these individuals, or their number of tokens (e.g. above 25%).

Participants in a DAO often include:

- **Managers**, such as multi-signature signers, usually oversee treasury or other wallets, deploy code changes to smart contracts, and manage voting by token holders. Although DAOs are supposed to be fully decentralised and automated, founders/developers may retain more control or be in charge of specific activities, e.g. Treasury, updating the code, or complying with tax and registration requirements. These may be based on retained rights or the number of tokens that they hold.
- **Software developers**, are the group of people who set up the organisation and will have a high degree of control over the DAO's governance (e.g. update the code) and operations, and likely obtain profits. (In non-DAO contexts developers have limited power because even if they change the code, users may decide not to download the updated version but to keep using the previous version. In contrast, in the case of a DAO, the developers, following the decision of the DAO, should update the code that will affect the DAO itself and all token holders).
- **Token holders**, are usually majority held by founders and developers, though others may also acquire them. A governance token is a virtual asset that grants voting powers or rights to the holders of those tokens. Holding more

governance tokens is likely to mean greater voting power.

- **Other contributors/operators**, such as miners/validators to support and validate transactions in the distributed ledger (e.g. blockchain)

Recent US case law gave some examples of who may be subject to lawsuits or enforcement actions, without referring to the issue of beneficial ownership. In the case on Ooki DAO, the lawsuit was directed against the DAO (understood as an unincorporated association) rather than against individuals, although the court considered the actions in the US of the DAO's founders to establish the court's jurisdiction:

"one of the bZeroX's co-founders, Kyle Kistner, took actions on behalf of Ooki DAO while Kistner was in the United States and during the period alleged in the complaint, and that Kistner knew that the Protocol was being offered to every person in the United States. ...

the other co-founder, Tom Bean, advertised the Ooki Protocol via his Twitter account while he was in the United States and during the relevant time period".

In the case of Tornado Cash, the Court found that founders, developers, and the DAO were all an entity that could be subject to OFAC sanctions:

"The entity is composed of its founders, its developers, and its DAO.... The founders and developers 'mostly do[] research and publish[] the code to GitHub.... The DAO, on the other hand, is responsible for governing the platform, which includes "[a]ll deployments, protocol changes, and important decisions.'.... Utilizing this structure, Tornado Cash has been able to place job advertisements, maintain a fund to compensate key contributors, and adopt a compensation structure for relayers, among other things.... Substantial evidence supports the argument that founders, developers, and DAO constitute '[a] body of persons who have combined to execute [the] common purpose' of developing, promoting, and governing Tornado Cash"

CONCLUSION – The registration, licensing and identification of VASPs and their customers will also depend on the type of entity and its control and ownership structure. The usual shortcomings of beneficial ownership transparency (e.g. beneficial ownership registries with limited scope, lack of verification, etc.) are exacerbated by the use of foreign entities, "exotic" entities unknown to the local legal framework (e.g. a Cayman company-foundation, a purpose trust or a private-interest foundation) and even more by the wide use of DAOs in the DeFi ecosystem. Countries may need to upgrade their beneficial ownership systems to address these new challenges.

3.1.6 FATF VIRTUAL ASSET RED-FLAG INDICATORS ON ANONYMITY

The FATF report of 2020 on **Virtual Asset Red-flags**¹ contain indicators on anonymity that could increase secrecy in relation to virtual assets' features, in addition to the schemes to hide the beneficial owner using corporate structures mentioned above.

The FAFT red-flag indicators on anonymity include:

- Using anonymity-enhanced cryptocurrency (AEC) or privacy coins such as Monero.²
- Moving a virtual asset that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange.

- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, and use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of virtual assets cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- Transactions making use of mixing and tumbling services
- The use of decentralised/unhosted, hardware or paper wallets to transport virtual assets across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS)

¹ <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf>

² According to the Binance Consent Order, Monero's protocol includes features that prevent tracking by using advanced programming to purposefully insert false information into every transaction on its private blockchain (concealing sender data and completely hiding all transaction amounts), sending funds to an auto-generated, one time use only, wallet known only to the transacting parties, and wallet addresses on Monero's private blockchain are selectively visible only when an observer has obtained a private view key.

that suppress or redact the owners of the domain names.

- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.
- A large number of seemingly unrelated wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent
- Using virtual asset ATMs/kiosk
- 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.
- 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
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer's VA address appears on public forums associated with illegal activity.
- A customer is known via publicly available information to law enforcement due to previous criminal association.



EU AML / CFT
GLOBAL FACILITY

4. Typologies & CASE STUDIES RELATED TO CUSTOMER due diligence AND beneficial ownership



**Funded by
the European Union**

4. Typologies & Case Studies related TO CUSTOMER due diligence AND BENEFICIAL OWNERSHIP

As described by the FATF, virtual assets continue to be used by criminals and organised crime groups. Hackers use social engineering techniques and malicious coding to access wallet infrastructure and manipulate transaction data. In money laundering cases, criminals use unregistered VASPs, over-the-counter traders, mixers, bridges, and a large number of wallets in complex transaction patterns. In international cases, money laundering networks may collect funds in one country and give the equivalent in another country by swapping virtual assets for cash. Criminals are becoming more sophisticated and professional, offering scam-as-a-service activity.

As for terrorism financing, terrorist groups use virtual assets for fundraising and to move funds across jurisdictions to benefit from the increased anonymity, to diversify sources and to move funds more rapidly.

In this context, there are specific typologies and case studies on how CDD processes and information can help solve cases, while the lack of any CDD requirements may directly enable financial crimes using virtual assets.



4.1 Case study 1: Binance

Binance was subject to different proceedings by US authorities in relation to money laundering and other violations that culminated in a Consent Order for billions of dollars. As reported by [the US Treasury](https://home.treasury.gov/news/press-releases/jy1925)¹:

The U.S. Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), and IRS Criminal Investigation (CI), has taken unprecedented action to hold Binance Holdings Ltd. and its affiliates (collectively, Binance) accountable for violations of the U.S. anti-money laundering (AML) and sanctions laws that protect American national security and the integrity of the international financial system. Binance is the world's largest virtual currency exchange, responsible for an estimated 60% of centralized virtual currency spot trading...

The violations include failure to implement programs to prevent and report suspicious transactions with terrorists – including Hamas' Al-Qassam Brigades, Palestinian Islamic Jihad (PIJ), Al Qaeda, and the Islamic State of Iraq and Syria (ISIS) – ransomware attackers, money launderers, and other criminals, as well as matching trades between U.S. users and those in sanctioned jurisdictions like Iran, North Korea, Syria, and the Crimea region of Ukraine. By failing to comply with AML and sanctions obligations, Binance enabled a range of illicit actors to transact freely on the platform...

FinCEN's settlement agreement assesses a civil money penalty of \$3.4 billion, imposes a five-year monitorship, and requires significant compliance undertakings, including to ensure Binance's complete exit from the United States. OFAC's settlement agreement assesses a penalty of \$968 million and requires Binance to abide by a series of robust sanctions compliance obligations, including full cooperation with the monitorship overseen by FinCEN.

¹ <https://home.treasury.gov/news/press-releases/jy1925>



In addition, in a 2025 Lawsuit, a group of families of American and Israelis held hostage by Hamas sued Binance in relation to aiding terrorism.¹

This case study illustrates many relevant issues for virtual asset regulation: identifying the entities part of a VASP group, their location and beneficial owners or controllers for sanctioning purposes, as well as illustrating the ways in which a VASP may deliberately fail to comply with CDD and other AML obligations.

4.1.1 IDENTIFYING ENTITIES PART OF THE VASP GROUP FOR SANCTION PURPOSES

Authorities determined that “Binance.com” would encompass Binance Holdings Limited, Binance (Services) Holdings Limited, and Binance Holdings (IE) Limited based on the following indicia²:

- affiliated through common ownership and control by the same individual, and
- is involved—through ownership of intellectual property, provision of technology services, or employment of personnel—in the coordinated operation of the Binance.com convertible virtual currency (CVC) exchange, (public face through

which they provide financial services to customers).

- The CEO of the Binance.com business is the same individual who beneficially owns these legal entities.

4.1.2 IDENTIFYING THE LOCATION OF THE VASP AND CONNECTIONS TO DIFFERENT JURISDICTIONS

The VASP may be connected to a country based on the country of incorporation of the entity, the location of its CEO and other managers or the location of its servers.

The lawsuit by the hostages’ families³ describe the follow situation in relation to Binance’s location and that of its CEO: Binance was incorporated in the Cayman Islands as a limited liability company in 2017 and owned by Zhao. In September 2017, following China’s ban on cryptocurrency exchanges, Binance relocated servers and operations from Shanghai to Japan. In March 2018, Japan’s Financial Services Agency issued a warning that Binance was operating without required licensure. That same day, Zhao announced Binance would relocate to Malta. In February 2020 Malta Financial Services Authority (“MFSA”) issued a definitive public statement clarifying that Binance “is not authorized by the MFSA

¹ <https://www.nytimes.com/2025/11/25/business/binance-hamas-terrorism.html>

² Footnote 1 of the Consent Order.

³ Pages 16-18.

to operate in the cryptocurrency sphere and is therefore not subject to regulatory oversight by the MFSA. As of 2025, Binance's principal servers run in a server farm in Japan. Binance's leadership operated from various countries. Zhao himself has been a digital nomad living in Canada, Singapore, and United Arab Emirates.

4.1.3 IDENTIFYING BENEFICIAL OWNERS AND CONTROLLERS OF THE VASP GROUP FOR SANCTION PURPOSES

The 2025 Lawsuit against Binance went against two individuals based on their roles, interests and de facto functions (including without any formal roles or interests), including⁴:

[Changpeng Zhao](#) because was ultimately tied to all entities part of the lawsuit as their beneficial owner. Even after stepping down as CEO, Zhao has retained an overwhelming ownership interest in Binance and, on information and belief, continues to wield significant influence over its business decisions.

[Guangying "Heina" Chen](#) is a close associate of Zhao who, despite not holding any formal title visible to the public, has long functioned as Binance's de facto

Chief Financial Officer. Chen was an early co-founder of Binance and initially held herself out in 2017 as the legal representative and 80 percent shareholder at the firm's original entity in Shanghai, China. When Binance set up its U.S. affiliate (Binance.US), Chen was listed as the signatory on its corporate bank accounts.

4.1.4 DELIBERATE LACK OF CDD, STR FILING AND OTHER AML OBLIGATIONS DESPITE CLAIMS TO THE CONTRARY

a) Failing to block customers from specific jurisdictions

Binance was supposed not to offer services to US persons and to apply measures such as geographic ringfencing to ensure US persons would not use its services. (For other cases, this restriction could be based on not allowing users from high-risk jurisdictions, blacklisted jurisdictions, etc).

According to the Consent Order⁵, Binance claimed to block customers determined to be based in the US and to employ secondary manual control during KYC process to check for US persons. However, in reality:



⁴ Pages 21-23 of the Lawsuit.

⁵ Page 10 of the Consent Order.

- There was no blocking of users with US IP
- It was enough for users to “self-certify” they are not US persons (Binance allowed this even when it had data that they were indeed US persons)
- No secondary manual control applied

In addition, in the case of Iran (a country under US sanctions), according to the Consent Order¹ Binance processed over 1 million transactions with an aggregate value in excess of \$500 million between U.S. users and users accessing the platform via an Iranian IP address, including designated/sanctioned customers such as:

- EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks;
- An individual associated with the sanctioned IRGC;
- IranVisaCart, which exploited Binance’s policies for opening multiple accounts with weak or no KYC.

b) Actively help customers from specific banned jurisdictions to circumvent restrictions

Although Binance actions referred to the prohibition for US customers, the strategies could equally apply to high risk or blacklisted jurisdictions. According to the Consent Order², Binance senior management discussed how to facilitate the evasion of its own ringfencing by certain U.S. VIP users, including:

- U.S. VIP customers who had already provided Binance with KYC documentation proving a US nexus were contacted “privately” to obtain new KYC docs from offshore jurisdiction (e.g. by first setting up offshore entity).
- U.S. VIP customers who had not yet completed their KYC (but who were identified as being U.S. users based on their IP address) were encouraged to “change their IP” with a VPN before they used their services.
- Binance internal records referring to the US in the country field record would be changed to “Unknown”.
- Not requiring supporting documentation, e.g. a US passport.
- Advising customers to lie on the registration form and instead of their real country of residence, e.g. US, to select another country, such as Cayman Islands.

c) Exchange brokers to avoid restrictions

As described by the Consent Order³, Binance allowed that any entity registered with Binance.com as an Exchange Broker was able to open an unlimited number of sub-accounts (sometimes around 1,000) and let sub-customers use the sub-accounts to trade without registering with Binance or without Binance applying extensive verification of sub-account users or of the exchange broker’s KYC program. In fact, some exchange brokers advertised offering “simplified KYC” for Binance and that they did not require complex registration procedures.

d) Lack of CDD for low-risk accounts (that were not low risk)

According to the Consent Order⁴, Binance had a type of customer, “Tier One” (also referred to as “no-KYC”) who could open accounts with only an email address (no CDD), conduct virtual asset-to-virtual asset transactions, and withdraw up to 2 bitcoins/day that at some point was worth USD 130,000. In this context, one supplier complained that it was not possible to monitor and screen transactions (e.g. for TFS purposes) with just an email but no names of the account holder.

e) Allowing high-risk customers

According to the Consent Order⁵, Binance allowed many high-risk customers to operate such as Russian VASPs (e.g. Garantex) sanctioned by OFAC. For instance, Binance processed hundred millions in US dollars in transactions for a Russian citizen who pled guilty to money laundering (including after guilty plea). It also processed millions of US dollars for a VASP that allowed its users to “cash out” at a Russian bank designated by OFAC and that had substantial exposure to the Russian darknet market Hydra Market.

f) Lack of appropriate personnel, training and supervision

According to the Consent Order⁶, the chief compliance officer (CCO) hired one year after the required deadline was not qualified for the role because he lacked knowledge of AML/CFT obligations and had little-to-no experience designing and overseeing an AML/CFT program.

In addition, AML training for personnel was insufficient.

¹ Pages 48-50.

² Page 11.

³ Pages 21-23.

⁴ Pages 23, 31-36.

⁵ Pages 36.

⁶ Pages 40-42.

⁷ Pages 42-53.

⁸ Page 46 of the Consent Order.

⁹ Page 47 of the Consent Order.

¹⁰ Pages 70-71 of the Lawsuit.

¹¹ Page 124 of the Lawsuit.

¹² <https://bit.ly/4y6w0X2>

There was no training on Binance products and services nor on risks such as: the “No-KYC” accounts, when the same person opens multiple “No-KYC” accounts, structuring to evade Binance’s two bitcoin threshold, or how to detect suspicious transactions involving AECs.

Finally, there were no audits of Binance AML Program. The first test considered only virtual asset-to-flat transactions, and only for customers who went through KYC (so it excluded no-KYC accounts) The first test involved a sample of only 31 accounts.

g) No STR filing

According to the Consent Order⁷, Binance did not file any STRs (this was a deliberate policy), even though FinCen later identified 100,000 suspicious transactions that Binance should have filed including cases of ransomware, high-risk jurisdictions, darknet market & scams, and child sexual abuse.

4.1.5 FINANCING OF TERRORISM

In the case of organisations designated by the US as terrorist organisations, including ISIS, Hezbollah, Palestinian Islamic Jihad (PIJ) and Hamas, the Consent Order and the Lawsuit identified cases where these organisations used Binance and compliance officers failed to file STRs or block the accounts, but rather tipped off customers and helped them take their funds, or cases where Binance failed to identify the high-risk and possible terrorist links despite public information. For instance:

- A third-party service provider alerted Binance on Hamas-associated transactions, but Binance filed no STR. Instead, the CCO attempted to influence how the provider reported on Binance’s conduct.⁸

- After a third-party service provider flagged accounts associated with ISIS and Hamas, the CCO instructed compliance personnel to “[c]heck if he is a VIP account, if yes, to...[o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him”.⁹
- Binance Account No. ***9799 was registered by the son of a Hezbollah commander. The phone number listed to Binance Account No. ***9799 (+96138----) links to the Facebook profile with clear indications of relationship to Hezbollah.¹⁰
- Binance Account No. ***5345 belonged to a 25-year-old PIJ operative in Gaza. Although the accountholder appears to have been a resident of Gaza, Binance actively processed 792 distinct IP address logins for this account over a 4-year period (between 2020 and 2025) including logins that were physically impossible without VPN masking.¹¹

4.2 Case study 2: Ilya Dutch Liechtenstein

This case study refers to the hack of the VASP Bitfinex by Russian-American Ilya Dutch Liechtenstein and his wife Heather Morgan. The hack involved stealing 120,000 bitcoins that at one point were worth US\$ 4.5 billion.¹²

From a CDD perspective, it is interesting that while the scheme showed a high level of sophistication (in terms of transactions, number of VASPs) and arguments to pass CDD procedures, the ownership structures of the accounts seemed rather simple and it appears that Ilyia and his wife, always used their real name and photo, even when the account was held by a different LLC or email account.

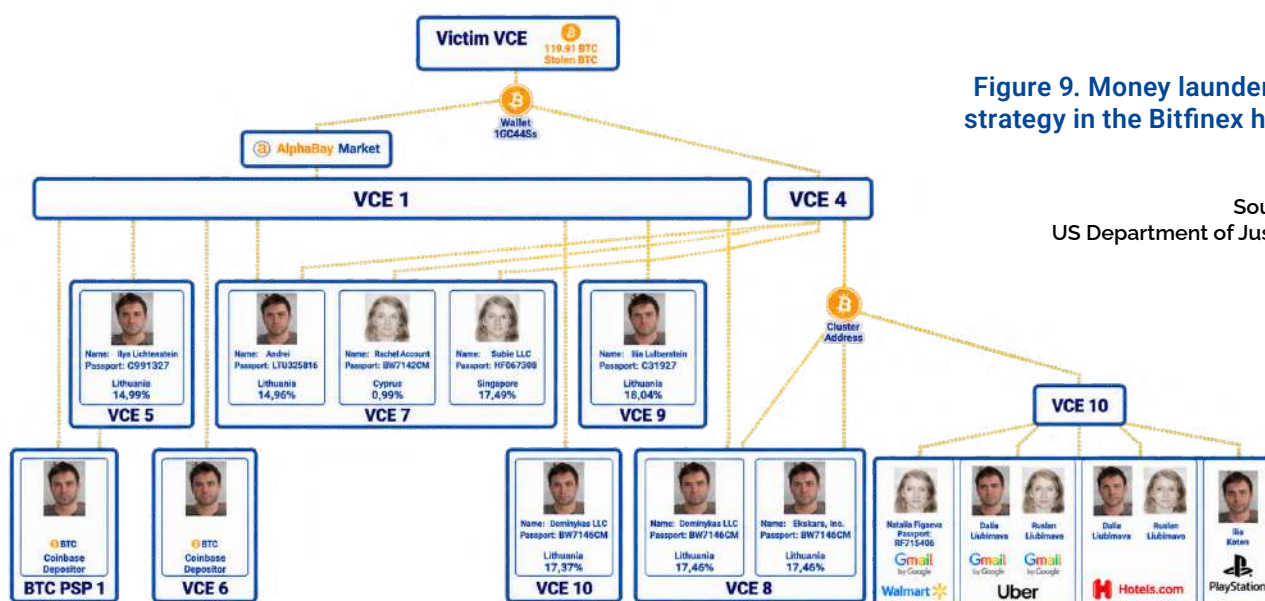


Figure 9. Money laundering strategy in the Bitfinex hack

Source:
US Department of Justice

For cases when accounts were opened with just an email, investigators used different indicia to link the accounts, such as:

- same email style
- accessed by same IP address
- created around the same time
- same trading patterns (hopping & convert into Monero), and
- abandoned when requesting additional KYC.

Although the arguments to convince compliance officers weren't always successful, especially when additional information was requested, the original explanation seemed well prepared. These included:

- *Hi, I'm a tech entrepreneur and [BTC] early adopter since acquiring my first BTC in 2011. I'm looking to diversify a bit ahead of the ETF decision and sell about 100BTC. Please let me know the next steps to move forward. All trades I would execute are from my own personal funds, the LLC is simply there to manage my trading.*
- *"SalesFolk has some B2B customers that pay with cryptocurrency". [Investigators were not able to locate anything on the SalesFolk website referencing accepting or dealing with cryptocurrency (companies that do offer virtual currency as a payment method or in conjunction with another service often advertise it to attract more business.)].*

Additionally, I also have some personal cryptocurrency of my own that I would like to sell to finance the development of some new software that we are beginning to build. Because the company is an LLC taxed as an S corp it has pass-through taxation and I am the sole owner. I was going to use some of my personal crypto to fund out new software projects.

"SalesFolk is not a financial institution: [SalesFolk's customers are] just B2B companies buying software and/or sales/email marketing consulting services from us, typically around \$8500 or less per contract/invoice, so we haven't been doing any KYC on them. "My boyfriend (now husband) gifted me cryptocurrency over several years (2014, 2015.), [sic] which have appreciated. I have been keeping them in cold storage.

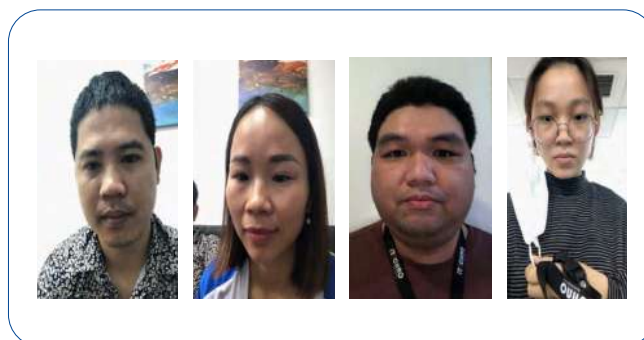
4.3 Case study 3: professional investment scam

This case relates to a professional investment scam where scammers, through various means of manipulation, convince victims to deposit more and more money into financial "investments" using cryptocurrency. In truth, these investments are fake. All victim money is under the control of—and ultimately stolen by—criminal actors, usually overseas. As a result, victims typically lose all money they invested.

In this case, KYC information was useful to relate accounts and discover that there was a full call center venue dedicated to the scam:

- Coordinated transaction activity
- Identical transaction counterparties
- Matching account naming conventions
- List of overlapping identical IP addresses, and
- Similar know-your-customer information (including Asian registrants, photos with same background and camera, and company tag) -> suggesting same scam "call center"

Figure 10. Photos showing same background, individuals and same company badges



Source: US Department of Justice



EU AML/CFT
GLOBAL FACILITY

5. COMPLEMENTARY SOURCES OF INFORMATION ON VIRTUAL ASSETS



**Funded by
the European Union**

5. Complementary sources of information on virtual assets



The FATF contemplates licensing or registration of VASPs, at least for local ones and optional for foreign ones offering their services to local users. These VASPs should collect basic and beneficial ownership information on their users. Competent authorities should have access to this information upon request, as well as whenever VASPs file STRs. However, it may be challenging to ensure compliance, especially by foreign VASPs. For this reason, competent authorities could also rely on two additional sources of information on virtual assets, based on tax and AML cooperation.

Tax authorities may obtain access to information on virtual assets from two different sources: the global automatic exchange of information on virtual assets based on the OECD's crypto-asset reporting framework (CARF) and based on local disclosure regimes requiring taxpayers to report their virtual assets, following the example of Brazil.

5.1 The OECD's Crypto-asset reporting framework (CARF)

In order to complement the OECD's Common Reporting Standard (CRS) for automatic exchange of bank account information, the OECD has developed a new parallel standard for countries to exchange with each other information on ownership, income and value of virtual assets: the crypto-asset reporting framework (CARF).

The CARF is very similar to the CRS. It relies on "reporting crypto-asset service providers" (RCASPs) - which are similar and overlapping with VASPs - to identify their users (customers) and these users' tax residence, so that the virtual asset information on each taxpayer will be sent to the corresponding tax authority where the user is (tax) resident. In practice, local RCASPs will report to their local tax administration information on each of their virtual asset users (as long as they are resident in a country

participating in the CARF). The tax administration will collect and sort information to then share it automatically with the corresponding country of residence (as long as these countries are participating in the CARF).

The next table identifies the countries that will be participating in the CARF and their starting date.

Jurisdictions undertaking first exchanges by 2027 (48)

Austria, Belgium, Brazil, Bulgaria, Cayman Islands, Chile, Colombia, Croatia, Czechia, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, San Marino, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Uganda, United Kingdom.

Jurisdictions undertaking first exchanges by 2028 (27)

Australia, Azerbaijan, Bahamas, Bahrain, Barbados, Belize, Bermuda, British Virgin Islands, Canada, Costa Rica, Cyprus*, Hong Kong (China), Kenya, Malaysia, Mauritius, Mexico, Mongolia, Nigeria, Panama, Philippines, Saint Vincent and the Grenadines, Seychelles, Singapore, Switzerland, Thailand, Türkiye, United Arab Emirates.

Jurisdictions undertaking first exchanges by 2029 (1)

United States.

Jurisdictions identified by the Global Forum as relevant to the CARF that have not yet committed to implement the CARF (5)

Argentina¹, El Salvador, Georgia, India², Viet Nam.

tax residence of the beneficial owner. Virtual asset information regarding each beneficial owner will also be shared automatically with the tax administration where the beneficial owner is resident.

An entity is classified as “passive” when most of its income or assets are related to passive income, such as rent, interest, dividends, etc. In contrast, an entity is classified as “active” (and thus need not identify its beneficial owners) whenever the entity’s income or assets are mostly related to an active business, such as selling goods or services. An entity may be considered “active” based on its status as a state-owned entity, international organisation or other special cases.

The definition of “beneficial owner” used in the CARF (and CRS) is based on the FATF definition, and RCASPs (VASPs) may either use CDD information to determine the tax residence, or otherwise require a self-certification by the user (customer).

■ Identification of local RCASPs (VASPs)

Similar to VASPs, RCASPs are in essence, any individual or entity that, as a business, provides a service effectuating exchange transactions of crypto assets (for fiat or other crypto-assets or goods) for or on behalf of customers (e.g. as counterparty, intermediary, or by making available a trading platform).

Because RCASPs may have links to different countries, the CARF establishes hierarchical rules to determine when a RCASP must report information in each participating country:

- I. an Entity or individual resident for tax purposes in the jurisdiction;
- II. Both: an Entity that (a) is incorporated or organised under the laws of the jurisdiction, and (b) either has legal personality in the jurisdiction or has an obligation to file tax returns or tax information returns to the tax authorities in the jurisdiction with respect to the income of the Entity;
- III. an Entity managed from the jurisdiction (key personnel, customer support centre);
- IV. an Entity or individual that has a regular place of business in the jurisdiction

The CARF contemplates strategies to identify local VASPs (similar to the FATF suggestions) to ensure that they are collecting and reporting to the tax administration the information required to be shared by the CARF. Although the CARF also relies on local

Last update: 4 December 2025

Similar to the CRS, whenever the user (holder) of virtual assets is an entity, and this entity is classified as “passive”, then the RCASP (VASP) must identify the beneficial owners of these entity-user and the

licensing for AML purposes, additional sources could be:

- Identification of VASPs by taxpayers who report their holdings and income related to virtual assets for purposes of income tax, value-added taxes or wealth tax.
- Requiring VASPs to file returns, including nil returns (in case they indicate that all of their users (customers) are locals, and thus not subject to automatic exchange via CARF)
- Requiring local VASPs to file notifications when another entity of the same VASP group is already reporting information for CARF purposes but in another jurisdiction.

■ Virtual asset information to be reported

The CARF contemplates the following virtual asset information on each user (customer) and beneficial owner to be reported and shared automatically among participating countries:

- Identification of RCASP where the user has an account (e.g. virtual assets)
- Identification of users and beneficial owners that are resident in the country
- Identification of the specific virtual asset (e.g. bitcoin).
- For each virtual asset (e.g. bitcoin), the exchange transaction type, the aggregate amounts paid or

received, the total units and the total number of transactions:

Examples of Exchange Transaction types:

- Acquiring BTC with USD (paying in USD)
- Selling BTC and getting USD in return
- Acquiring BTC using ETH (paying in ETH)
- Selling BTC and getting ETH in return

Examples of Transfer Transaction:

- Retail purchase (above USD 50,000)
- Transfer to wallet not held by an Exchange (e.g. unhosted wallet)

■ Access to CARF information for AML purposes

Similar to the CRS and most methods to exchange tax information, CARF information can in principle be used for tax purposes only. However, in many countries, tax administrations may be considered “reporting entities” that must also file STRs with the financial intelligence unit.

In addition, there is one possibility for tax authorities to share CARF (or CRS) information for AML purposes. In principle, the CARF, the CRS and most methods for exchange of tax information are based on the Council of Europe/OECD Convention on Multilateral Administrative Assistance in Tax



¹ https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/convention-on-mutual-administrative-assistance-in-tax-matters/status_of_convention.pdf

Matters. More than 140 jurisdictions are parties to this Convention.¹

This Convention on Multilateral Administrative Assistance in Tax Matters contains confidentiality provisions and restriction of use for tax purposes in Article 22. The same confidentiality and restriction of use for tax purposes applies to exchanges based on bilateral agreements (rather than based on multilateral conventions). The OECD Model (Bilateral) Tax Convention contains very similar provisions in Article 26. However, both articles contain one exception that can be used to share information for AML purposes. In essence, tax authorities may share information with other local authorities when: (i) the sending jurisdiction authorises this additional use/share, and (ii) both jurisdictions allow this additional use in their own domestic laws.

The OECD Commentary to the Model (Bilateral) Tax Convention mentions the case of sharing information for AML purposes explicitly:

The last sentence of paragraph 2 therefore allows the Contracting States to share information received for tax purposes provided two conditions are met: first, the information may be used for other purposes under the laws of both States and, second, the competent authority of the supplying State authorises such use. It allows the sharing of tax information by the tax authorities of the receiving State with other law enforcement agencies and judicial authorities in that State on certain high priority matters (e.g. to combat money laundering, corruption, terrorism financing). When a receiving State desires to use the information for an additional purpose (i.e. non-tax purpose), the receiving State should specify to the supplying State the other purpose for which it wishes to use the information and confirm that the receiving State can use the information for such other purpose under its laws. Where the supplying State is in a position to do so, having regard to, amongst others, international agreements or other arrangements between the Contracting States relating to mutual assistance between other law enforcement agencies and judicial authorities, the competent authority of the supplying State would generally be expected to authorise such use for other purposes if the information can be used for similar purposes in the supplying State. Law enforcement agencies and judicial authorities receiving information under the last sentence of paragraph 2 must treat that information as confidential consistent with the principles of paragraph 2.

In conclusion, it is possible for financial intelligence units and law enforcement agencies to obtain virtual asset information held by locals in foreign VASPs,

as long as they can meet the requirements for tax authorities to share this information, assuming also that the country is participating in the CARF.

5.2 Local information disclosure regimes

Countries may start requiring locals to also report information on their virtual assets, as a way to complement and cross-check information that should have been collected by locally-licensed VASPs, and obtained via automatic exchange of information based on the CARF.

The tax administration may be best placed to establish such a reporting framework on all local users, especially for all those considered local taxpayers.

For instance, since 2019 Brazil has been requiring local VASPs and local taxpayers to report their holdings of virtual assets. Normative Instruction 1888/2019 established two different reporting frameworks (complementary, rather than overlapping) to submit information to the tax authorities:

- Local VASPs are required to report annually the account balance of virtual assets and monthly all the transactions in the VASP.
- Local taxpayers are required to inform monthly transactions involving virtual assets above a threshold (ca. USD 5,500) that do not take place through local VASPs: transactions through foreign VASPs and transactions involving P2P.

To better understand the purpose (and tax relevance) of the transaction, Brazil reporting framework requires the disclosure to identify the type of transaction such as:

- Purchase/ Sale (Exchange)
- Donation
- Rent (temporarily holding) / Loan / Guarantee
- Payment with virtual assets for goods and services
- Issuance / Mining
- Involuntary loss

■ Statistics

Brazil has been publishing statistics on the reporting of virtual assets. Among the published data, one crucial feature is that the owners or holders of virtual assets are predominantly entities, rather than individuals. This suggests that there

is a crucial need to ensure beneficial ownership transparency is properly implemented to identify the beneficial owners of these corporate holders of virtual assets.

Figure 12. Value (in Brazilian currency) of virtual assets held either by individuals (persona fisica or PF) and entities (persona juridica or PJ).



MINISTÉRIO DA
FAZENDA



MÊS/ ANO	Declarações (Valores em milhões de R\$)							Total Geral
	Com uso de exchanges no exterior			Sem o uso de exchanges			Exchanges	
	PF	PJ	Subtotal	PF	PJ	Subtotal	Somente PJ	
12/2024	504,64	4.635,19	5.139,83	247,01	7.725,99	7.972,99	38.786,62	51.899,45
01/2025	449,97	3.675,73	4.125,70	403,30	7.407,38	7.810,68	35.406,82	47.343,19
02/2025	234,70	4.336,06	4.570,76	293,52	6.834,47	7.127,99	23.704,44	35.403,20
03/2025	234,50	5.251,97	5.486,47	59,42	7.000,01	7.059,42	24.888,52	37.434,41
04/2025	319,01	4.401,36	4.720,37	103,30	7.093,84	7.197,14	24.407,51	36.325,02
05/2025	267,01	4.603,20	4.870,21	115,26	6.551,35	6.666,61	23.296,05	34.832,88

Source: Brazil tax administration

CONCLUSION

Although the CARF and disclosure regimes have a tax purpose, the vast amount of information on ownership (including beneficial ownership) on virtual assets could equally be used by the AML authorities for analysis and red-flagging related to money laundering and the financing of terrorism, as well as by law enforcement (including for asset recovery).

The tax administration may thus become an ally in the AML world, especially if it is a source to complement data (not collected by local VASPs) but also if there is duplication of reporting (e.g. both by taxpayers and VASPs in order to cross-check information).

If tax authorities already hold information on owners of virtual assets, it may be possible for FIUs and law enforcement to first ask them for information, to avoid the risks that a VASP may tip off its customers about specific investigations, if the FIU asks the VASP directly.



EU AML/CFT
GLOBAL FACILITY

6. How the EU Global Facility can Help



**Funded by
the European Union**

6. How the EU Global Facility can Help

Based on the explanations of this report, and the general work and expertise of the EU Global Facility, we may assist countries in:

- Reviewing the beneficial ownership framework (laws, regulations, guidance, registration form) and proposing an expansion of scope to cover VASPs and customers of VASPs, as well as more complex entity types (e.g. purpose trust, private-interest foundations)
- Assessing the technical implementation of beneficial ownership registries to allow for proper

discrepancy reporting and access to information by authorities dealing with virtual assets and VASPs

- Assisting with the licensing and registration process for VASPs
- Reviewing the KYC/CDD supervision for VASPs to ensure they are properly identifying customers and their beneficial owners
- Assisting with the National Risk Assessment regarding virtual assets risks and vulnerabilities
- Improving AML and Tax cooperation, to foster local sharing of information.





EU AML/CFT
GLOBAL FACILITY



**Funded by
the European Union**



THE EUROPEAN UNION'S GLOBAL FACILITY ON
ANTI-MONEY LAUNDERING AND
COUNTERING THE FINANCING OF TERRORISM

www.global-amlcft.eu



EU Global Facility on AML/CFT



**Funded by
the European Union**

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the EU AML/CFT Global Facility and do not necessarily reflect the views of the European Union.