

Crypto Risk Policy

DOCUMENT CLASSIFICATION	Policy
DOCUMENT REF	012026
VERSION	V.1
DOCUMENT STATUS	Valid
RELEASED DATE	01.04.2026
DOCUMENT OWNER	WinHolding B.V

1. Introduction

In relation to payment carried out in crypto currencies one must understand that such holds increased risk for Money Laundering, Terrorist Financing including and not limited to also crimes related to tax evasion.

Stages of money laundering with the use of Virtual Financial Assets ML in relation to Virtual Financial Assets (hereinafter referred to VFA or VFA's) has adapted a different channel of manifestation. Illicit funds (in any currency) can enter cryptocurrency markets in two ways thus leading to the stages of ML as briefly described hereunder:

Phase 1

A criminal may purchase digital currency via:

- A bank account from a basic digital exchange; or
- By cash or debit card at a digital currency ATM

Basic digital exchanges are generally preferred, as bitcoin ATM companies are regulated as money service businesses (MSBs), which requires they maintain AML programs.

Phase 2

Primary coins (basic exchange) are exchanged to privacy alt-coins which are highly anonymous. This process is termed "Bitcoin Mixing".

Phase 3

Layering is then carried out through multiple privacy coins, exchanges, and digital addresses (advanced exchange).

Phase 4

Privacy coin holdings are then exchanged for primary coins, which can then be transferred back to a basic exchange, where funds may be withdrawn to a connected bank account. This process is termed "bust-out" integration.

2. Understanding Red Flags

The following are red flags in relation to the VFA industry (none exhaustive list):

2.1 Financial

- Onboarding new Clients carrying out one-off transactions exceeding the threshold of 2,000 Euro deposits or withdrawals or equivalent;
- Clients carrying out large one-off transactions;
- Clients transferring significant amounts of cash through a retail establishment or funds generated through retail activities;
- Clients making frequent transactions to the same individual/group of individuals;
- Client transacts in patterns that are not in line with their profile;
- Large transactions that have no apparent economic or visible lawful purpose;
- Transactions with no apparent logical, economic or legal purpose;
- Unusual patterns of the transactions;
- Complex or unusually large transactions;
- A transaction that is likely to be related to ML/FT due to the origin of the funds;

- Transaction mechanism being incoming or outgoing payments multiple inward payments;
- Loss-making transactions where the loss is avoidable or obvious;
- Clients whose chainanalysis links to high risk wallets;
- Movement of funds between accounts, institutions or jurisdictions without reason;
- Large payment on account of fees with instructions terminated shortly after and the Client requesting the funds are returned;
- SOW/SOF:
 - Situations where the source of funds cannot be easily verified or where the audit trail has been broken/layered;
 - Clients who may have used tumblers to disrupt the origin of funds;
 - Frequent and unexplained movement of accounts to different entities as established from the SOW/F;
 - Clients who appear not to have a regular job are receiving regular transfers and will not provide information on the source of funds.

Customer & Interface

- The unwillingness of Clients to produce evidence of ID or the production of unsatisfactory evidence of ID;
- Clients are on-boarded Non-Face to Face;
- Obstructive or secretive Clients;
- Where the customer is, or appears to be, acting on behalf of another person, made more concerning if there is an unwillingness to give the name/s of the person/s they represent;
- The use of third-party wallets;
- Asset transfers where there is a variation between the account holder's identity and requesting personal;
- The level of anonymity or preferring anonymity;
- Instructions outside our usual range of expertise;
- Cases or instructions that change unexpectedly or have no logical reason, especially where:
 - The Client has deposited funds with us, and the origin of the account is unknown;
 - The transfer of assets changes at the last moment;
 - You are asked to return assets or send assets to a third party.

Product

- Unknown origin and source of the coin, and where it has been derived from;
- The use of ALT coins or the conversion thereof.
- DeFi Address risks posed by DeFi protocols that allow peer-to-peer transactions without intermediaries, complicating compliance with AML/CFT rules.

Geographic

- Client originating from high-risk jurisdiction;
- Change of IP or use of VPN;
- Transactions Involving high-risk jurisdictions (e.g. Iran, Uzbekistan, Turkmenistan, Pakistan, Sao Tome and Northern Cyprus, kindly follow jurisdiction risk assessment).

The company has implemented a system that will detect those individuals that, based on the customer profile, are deemed to fall outside the 'Norm', and such Clients will be outrightly refused or reported if deemed necessary. Criminals are always developing new techniques, so this list can never be exhaustive. We are to remain vigilant, and if new typologies are identified are to be raised with the MLRO.

3. Wallet Screening

The Client will be questioned on the type of wallet being used (selected via a dropdown), and the hash of the wallet will be held and verified against a third-party provider:

- Multi-signature wallets are to be verified, and each individual holding keys shall be treated as a beneficial owner of the account and will need to be verified.
- Those custodial wallets which are not subject to any verification shall be assessed, and if they are likely to pose a high risk of ML/FT will be placed on a list of providers for whom the wallet will be black listed. All wallets depending on the activity limits and thresholds, shall be scrutinised for ownership and illicit activity.
- If the Client indicates a wallet that is not held on his behalf, such will be scrutinised.

The wallets are to be screened:

- At onboarding prior to establishing the business relationship;
- When the Client is depositing funds; or
- When the Client is transferring funds out of the system.

Screening of wallets is conducted using third-party provider system and helps to understand where the funds are received and sent to. This is to ensure further that funds are not remitted to wallets which have links to financial crime and will ensure complete plotting of the transaction and that when funds are transferred out of the system they are processed to the same wallet used to deposit (closing the loop).

If there is an alert on any wallet it will be reported immediately to the MLRO.

Note: Each time a client deposits form a new wallet the above is conducted on each wallet added; Client shall be questioned on the type of wallet & hash of the wallet shall be verified against third-party provider wallet screening. If the client is using multiple wallets this is a potential ML/FT concern and will be taken into account in the CRA and raised to the appropriate authorities if required.

4. Risk assessment

In the policy above the risk assessment does cater for the risks associated with the involvement of crypto currencies.

5. Blacklisted Wallets (non-CAP)

The company takes a heavy stance on blacklisted wallets, whether blacklisted or sanctioned by Authorities or blacklisted by the company. The company uses an internal automated system by third-party provider, which automatically detects any transaction emanating from or being sent to blacklisted wallets. If such a transaction is detected, the payment will be frozen, and funds will not be transferred.

6. The Use of Privacy Coins

The use of privacy coins that may render the Client anonymous are strictly prohibited. The wallets the Client is to deposit are to be screened upon the inception of the account using software

that will generate a report which will influence the Client's risk score. The company shall adopt a clear-cut approach meaning that if a high-risk wallet is identified, the wallet and the Client will not be allowed on the platform and shall be banned from further interaction.

The company is currently obtaining a third-party verification provider which shall be part of the onboarding process. All tokens offered on the platform will have to go through a financial instrument test, along with an internal audit of the token for AML/CFT purposes.

7. Travel Rule

The travel rule requires all financial institutions to pass on certain information to the next financial institution in transfers exceeding 2,000 Euro or equivalent involving more than one financial institution. The company shall hold and pass on the following information when the travel rule is triggered. Note the information the company passes on depends on if they are acting on behalf of the originator or beneficiary:

- a. The official full name of the originator and the beneficiary;
- b. The address of the originator's and beneficiary's hosted wallet. Where no such address is available, the VFA service provider of the originator shall instead transmit the unique transaction hash identifying the particular transfer of VFAs in the related distributed ledger; and
- c. The originator's permanent residential address, or the originator's identity reference number, or his date and place of birth.

In those situations where VFAs transfers to another financial institution and the transfer does not exceed 2,000 Euro or equivalent in value and the transfer does not appear to be linked to any other transfer of VFAs which together would exceed 2,000 Euro or equivalent in value, the company shall transmit only the information referred to in paragraphs (a) and (b) above.

The company will refrain from carrying out the transfer where there is a suspicion of ML or the FT (and report the transaction to the FIAU) or the VFAs were acquired by means of cash or anonymous electronic money for which the company prohibits both such will be scrutinised in the wallet screening and source of wealth and funds.

8. The Travel Rule: Beneficiaries and the Further Enforcement of Due Diligence Measures

Where the company is involved in a VFA transfer the company is to verify the accuracy of the information held on the beneficiary prior to making the VFAs received available to them. The said verification is to be carried out based on data, information and documentation, the requirements for which is explained in the 'Onboarding of New and Prospective Clients' section above.

The company shall adopt and implement measures, controls, policies and procedures to:

- detect whether the fields in the system used to transmit the information have been filled in using characters or inputs admissible in accordance with the conventions of the system.
- carry out real time monitoring so as to detect whether information required is missing in part or in full.
- determine on a risk sensitive basis whether to execute, reject or suspend a transfer of VFAs in relation to which the information has not been made available in whole or in part.

9. Considerations on Reporting Missing Information

The company has strict obligations to report any transaction or activity the company knows, suspects or otherwise has reasonable grounds to suspect to be linked to money laundering or the funding of terrorism, or any other reporting obligations that the company or the service provider of the beneficiary may have under any other law.

If the company is subject to missing information from the user or instances where a user is reluctant to provide information following a request, such shall be reported to the MLRO or Deputy MLRO only in those indicated in the paragraph above. Hence, if any of the required information is not provided the company shall have a strict obligation to investigate the activity of the user to assess if a report to the authorities is required.

Conclusion

The above are the company's policies AML and CTF, as well as the information required in relation to our KYC services. This policy will change according to the company's business practices and will be accordingly updated.