

INVESTAN N.V.

VIRTUAL ASSET COMPLIANCE POLICY

Version: 1.0

Last Update: 2024-12-10

Applicability: Investan N.V.

Owner: MLRO

Approver: CEO

INTRODUCTION

The gambling markets (both land-based and online casinos) are evolving rapidly to accept cryptocurrency payments, but regulators are struggling to keep pace with the technology changes and put adequate safeguards in place to guard against potential money laundering risks. This research seeks to review the global landscape in relation to the acceptance of cryptocurrencies in the wider gambling sector and provide some insight to gaming regulators considering the adoption of cryptocurrency, how cryptocurrencies can be used and the associated regulatory controls that can be implemented.

Cryptocurrency is defined as a form of virtual asset that uses cryptography to secure financial transactions and is intended to be used as a new and alternative payment method. Cryptocurrencies run on a distributed public ledger called blockchain which provides a publicly available record of all transactions through the use of public keys. The driving force behind the development of these alternative payment systems was to remove a single point of failure (i.e.: the banks) by using peer-to-peer networks to verify and authenticate transactions on a publicly available blockchain. A transaction is considered verified once a miner solves a cryptographic (mathematical) puzzle. This peer-to-peer verification network enhances the transparency of transactions and theoretically eliminates the need for a central approving authority. Cryptocurrency transactions are supported by wallets (hot or cold) and accompanied by a public and private key. Hot wallets indicate that the user's private key is stored online and cold wallets indicate the private key is stored offline.

Nevertheless, there is a high probability that cryptocurrency and other virtual assets may be used for the purposes of money laundering and terrorist financing.

The primary purpose of this Virtual Asset Compliance Policy (hereinafter – the “**Policy**”) is to ensure that the Company is in compliance with the FATF Recommendations and Guidance, including FATF Guidance for a Risk Based

Approach to Virtual Assets and Virtual Asset Service Providers (“FATF Guidance”) as applicable to the remote gaming sector.

The present Policy is implemented as part of the Company’s wider AML/CTF obligations. The Company is committed to implementing a risk-based approaches to assessing, managing and mitigating the risk factors related to the use of Virtual Assets.

GENERAL REGULATION

Cryptoassets include Virtual Assets that can be used as a means of payment or for other financial activity within a remote gaming operation or environment.

Not all Cryptoassets are Virtual Assets, for example, NFTs (such as digital collectibles) are unique assets that are distinguishable from each other and so do not have the fundamental fungible quality of various means of payment. That is such NFTs are not primarily a financial instrument or asset. NFTs may also be used within remote gaming environments as part of a reward, collectible or other closed loop benefit for customers without thereby meeting the definition of a Virtual Asset for the purposes of this Policy.

The Company is responsible for ensuring that where a Cryptoasset is within the classification of a Virtual Asset, all applicable legal and regulatory requirements are followed.

The Company permits deposits and withdrawals using Virtual Assets, all withdrawal requests permitted using Virtual Assets must be made using the same Virtual Assets to either the Wallet addresses that have been used by a customer to make deposits or, where there are security concerns or other justifiable and credible reasons, to a new Wallet address that is operated by a regulated VASP. The Company shall ensure that the reasons for use of such alternative Wallet address are documented.

ONGOING MONITORING

The Company implements robust monitoring mechanisms to track transactions involving Virtual Assets including those conducted via VASPs and Self-hosted Wallets. Any suspicious activities or transactions that raise concerns regarding the SOF or destination of funds shall be promptly reported to the competent authorities. Regular audits and reviews of Virtual Asset activities involving customers shall be conducted to ensure compliance with regulatory requirements.

The Company is planning to resort to specialized screening third-party providers and software for the purposes of:

- ✓ Monitoring incoming Virtual Asset deposits for potential links to sources associated with illicit activities;
- ✓ Detecting illicit sources of Virtual Asset funds and transactions associated with criminal activities;
- ✓ Flagging suspicious patterns or behaviors indicative of involvement in illicit activities.

The Company shall maintain records of illicit activity monitoring activities and outcomes.

The MLRO shall have full access to information and records of the company that the Director considers necessary to evaluate internal reports received.

If the MLRO considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO is responsible for:

- ✓ Submitting the necessary information to the FIU;
- ✓ Recording the disclosure in the register of disclosures.

- ✓ Dealing with subsequent production or account monitoring orders if there are any.

Furthermore, the Company takes responsibility to collaborate with law enforcement agencies and regulatory bodies in investigations related to illicit activities and transactions with the use of virtual assets.

ANONYMOUS TRANSACTIONS PROHIBITION

Virtual Assets, Wallets and VASPs that are known to be used for the concealment or obfuscation of identity or the SOF (including so called mixing and tumbling services) are prohibited within the gaming ecosystem. The Company actively prevents the use of such identity and source concealment tools for remote gaming transactions and takes all the necessary measures to identify and address any attempts to circumvent transparency measures.

First of all, Customers will not be able to register with fictitious names or anonymous accounts.

When registering with a website owned by the Company, the account will not be opened unless the requested identity details (shown above) are completed in full. Duplicate accounts will not be allowed, and checks will be made at the time of registration.

Fictitious names will not be allowed. Obvious fictitious names will be identified at the time funds are deposited to the account and the account will be terminated.

A participant whose account is terminated shall be advised by email unless it is in relation to a matter reported to the FIU, in which circumstances please be advised accordingly by the MLRO.

RISK FACTORS

Generally, according to the cybersecurity and virtual asset guidelines, the following factors might be considered red indicators for the risk of money laundering and terrorist financing:

1. **Anonymiser software, IP mixers, coin mixers and anonymity enhanced Virtual Assets:** these tools are designed to obfuscate the origin and destination of virtual assets, making it difficult to trace transactions. Their use may indicate an attempt to conceal illicit activities such as money laundering or terrorist financing.
2. **IP does not match registration details provided:** If the IP address used for transactions or account access is from a different geographical location than the one provided in the customer's registration details, it may suggest an attempt to hide the true location of the user, raising suspicion of fraudulent activity.
3. **Significant transactions in Virtual Assets where the frequency or value is unusual:** Large or frequent transactions that deviate from the customer's typical transaction behavior or profile may indicate suspicious activity. This could include sudden large purchases or sales of VAs that are inconsistent with the customer's known financial situation or history.
4. **Transactions involving Virtual Assets that are not plausible given the information known about the customer:** Transactions that do not align with the customer's known business activities, income level, or stated purpose for using VAs can be a red flag. For example, a customer with a modest income making large Virtual Asset transactions without a clear source of funds.
5. **Source of wealth is unclear or cannot be verified:** If the origin of the customer's funds is unknown or cannot be reasonably verified, it increases the risk of those funds being derived from illegal activities. This includes situations where the customer is unable or unwilling to provide sufficient information about how they acquired their wealth.
6. **Transactions involving jurisdictions with weak AML/CFT controls:** Engaging in transactions with countries known for weak regulatory oversight

or high levels of corruption can increase the risk of money laundering and terrorist financing.

7. **Rapid movement of Value:** Quick successive transfers between different VASPs and Wallets especially across different jurisdictions, may indicate layering which is a common money laundering technique used to obscure the origin of funds.
8. **Use of anonymous payment methods for funding Virtual Asset transactions:** The use of payment methods that offer anonymity can be a red flag, as they make it difficult to trace the source of funds.

PREVENTIVE MEASURES

The Company shall implement risk mitigation strategies to address the threat posed by illicit transactions and sources of funding, including:

- Enhanced due diligence measures for Virtual Asset deposits that are deemed to be higher risk.
- Regular training for staff on identifying and responding to illicit activity risks.
- Collaboration with cybersecurity experts to strengthen platform defenses against criminal infiltration.

Some of the key safeguards in terms of AML/CTF with the use of virtual assets include:

- ✓ **Customer Verification.** Customers must be registered and have completed the customer identification processes and the wallet address must be verified as part of the customer identification procedures;
- ✓ **Payments:** Fiat and crypto payments shall be maintained separately and cannot be interchanged, the deposit method must be the same as the withdrawal method and the Company must also maintain logs of failed deposits and withdrawals. Crypto payments would only be allowable on approved online betting platforms, no live events of phone bets.

- ✓ **Responsible gambling limits** are applicable in fiat regardless of if the payment is made in crypto. Initial guidance would suggest limits of \$2,000 per month. Maximum wager limits are also set at \$5,000 per transaction.
- ✓ **Company shall hold wallets in the cryptocurrencies** traded with sufficient funds on hand to pay out any winnings and record the exchange rate at the time of the transaction.
- ✓ **Transaction monitoring** shall be conducted on a regular or real-time basis.
- ✓ **Conversion rates** must be up-to-date for value-based thresholds/alerts;
- ✓ **Consideration** shall be given to setting lower thresholds for CVC/VC than for fiat transactions
- ✓ Monitoring shall include **in-game play, deposit frequencies and transaction patterns** rather than focusing only on value in, value out.

In certain cases, highlighted by the risk assessment, the Company may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the Company. Participants who pose an additional risk will be recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO.

The Company also recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

Consequently:

- The management shall retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the Company shall engage with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.

- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

STAFF TRAINING

It is key to effective AML/CFT arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering.
- Staff are aware of their personal legal obligations.

The steps adopted by the group to ensure staff have appropriate awareness and training are as follows:

- ✓ All new staff will receive AML/CFT induction training, to include:
 - The provisions of the AML/CFT code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - Their personal obligations under the AML/CFT Code and associated personal liabilities for non-compliance.
 - The internal reporting procedures detailed in the AML/CFT Manual.
- ✓ AML/CFT refresher training shall be delivered at least annually for all staff and key persons
- ✓ The MLRO shall provide ad hoc information about news and developments.
This will be targeted as appropriate.
- ✓ The MLRO shall send periodic reminders of the need to report certain matters.