



XZ Solutions B.V.

AML Policy

Version 2.0.

Version Approval

Date
30.08.2024

Version
2.0

1. Mission Statement

This document is intended to outline the XZ Solutions B.V. (the Company) Anti-Money Laundering Strategy in order to ensure that:

- Statutory and regulatory obligations to prevent money laundering are met, taking positive action in order to minimize risk of the Company's services being used for the purpose of laundering the proceeds of criminal activity or terrorist financing.
- The Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with illegal activities. We will seek to terminate any relationship where conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities.
- Any such termination shall follow the reporting of the suspicions and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations to avoid any risk to the Company.
- The Company complies with the obligations of relevant national and international legislation and regulation, adherence to Financial Action Task Force (FATF) recommendations and EU Directives on the prevention of money laundering and terrorism financing, National Ordinance on Identification of Clients when Rendering Services, National Ordinance on the Reporting of Unusual Transactions, Kingdom Sanction Act, Sanctions National Ordinance, National Decree for general measures, National Ordinance extension of validity sanctions decree, the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the National Ordinance on Identification when Providing Services (NOIS)
- The Money Laundering Reporting Officer (MLRO) will act as Key Official on behalf of the Company and is responsible for:
 - Receiving and assessing internal suspicion reports
 - Taking reasonable steps to access any relevant "know your customer/business" information
 - Making external reports to relevant national and international authorities
 - Obtaining and using national and international findings concerning countries with inadequacies in their approach to money laundering prevention
 - Taking reasonable steps to establish and maintain adequate arrangements for awareness and training
 - Monitoring the day-to-day operation of the Company's Anti-Money Laundering policies
 - Responding to reasonable requests from regulators and law enforcement
 - Making compliance reports to senior management at least annually
- The Company is committed to high standards of anti-money laundering compliance and requires management and employees to adhere to these standards in preventing the use of its products for money laundering /terrorist financing purposes.

2. Definitions of Money Laundering and Terrorist financing, Legal and Regulatory Framework

The Legal and Regulatory Framework is set by, without being limited:

- Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (4th Money Laundering Directive)
- Payment card Industry (PCI) Data Security Standard V1.2 (October 2008).
- applicable AML laws and regulations in Curaçao, including the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the National Ordinance on Identification when Providing Services (NOIS)

The 4th Money Laundering Directive defines money laundering as:

1. The conversion or transfer of property, knowing that such property is derived from criminal activity or from participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.
2. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity.
3. The acquisition, possession or use of property, knowing, at the moment of receipt, that such property was derived from criminal activity or from an act of participation in such activity.
4. The participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to points 1, 2 and 3.

The 4th Money Laundering Directive defines terrorist financing as:

the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.

There are often three acknowledged phases:

- Placement – the physical disposal of cash or other assets derived from criminal activity
- Layering – the separation of the illicit proceeds from their source by layers of transactions intended to hide the origin of the funds
- Integration – supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appear to be personal transactions. However, even simple possession of criminal property may constitute an offence. Criminal property is defined as property which is, or represents, a person's benefit from criminal conduct, where the alleged offender knows or suspects that it is such.

The 4th Money Laundering Directive contains the following provisions:

- More risk-based approach – all gambling operators (not just casinos) will be required to undertake customer due diligence on all transactions over 2,000 EUR.
- Operators will have to develop, update and implement suitable written risk assessments, policies and procedures as well as processes for testing their effectiveness. Must be documented and made available to regulators and independent auditors.
- Staff must be fully screened and trained in AML.
- Must conduct enhanced due diligence where the risk profile of a customer indicates high risk and for domestic and foreign politically exposed persons. Simplified due diligence permitted for low-risk customers.

- Evidence of higher risk which are set out in Directive Annexes include size and frequency of transactions, customer residence in countries with significant corruption and crime and payments received from unknown parties.
- Records must be kept for a minimum of 5 years.

3. Risk Based Approach

The risk-based approach recognizes that the ML/FT risks faced by each sector and each subject person are different and allows for resources to be invested and applied where they are most required. The risk-based approach envisages the application of checks that are proportionate to the assessed risk. The cornerstone of the risk-based approach is the risk assessment which must be carried out at different stages of a subject person's activities. This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

4. Responsibility

The MLRO and the Key Official are responsible for ensuring the Fraud Control, KYC and AML Procedures whilst the CFO is responsible for the Payout Management Procedure. They are also responsible for ensuring the plan is kept up to date and that employees are aware of the procedure.

5. KYC Procedure

Know Your Customer Procedures are followed to achieve the following objectives:

- Allowing only legitimate customers to register an account (Ex: Minors, Sanctioned Persons or Players from Sanctioned countries are not allowed to register a gaming account).
- Build the risk profile associated with the customer.
- Confirming that customers are who they say they are.
 - Monitoring customer accounts and transactions for illegal activities.
 - Blocking duplicate accounts.
 - Identifying possible PEP & Sanctioned customers.

5.1. Registration

Before being able to play on the site a customer needs to first register an account. On the registration page the customers are asked for the following details:

- Email address. In order to validate the email address of the player and email with a link to validate the email address will be sent to the email address listed in the registration. A player will not be allowed withdraw funds unless the email is validated.
- Mobile number
- Full name
- Date of Birth
- Address

Once the above information is received the fraud department will screen the information for any false or suspicious information, possible duplicate/Self-excluded accounts, Politically Exposed

Persons and sanction lists.

The IP address from where the traffic originated is tracked by the Company's back office software. Should traffic originate from countries which are on the list of restricted countries, the account will be blocked.

Should the checks (Manual or automatically done by the system) indicate that a duplicate account has been registered, the account is suspended until further checks are made to determine whether this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

5.3. Age Verification

No customers under the age of 18 can register an account. The system does not allow persons under 18 to register an account.

The Company uses SumSub tool for age verification processes.

5.4. Duplicate accounts

Players are only allowed to hold one account. When a player registers, the details are checked for possible duplicate accounts. Should the checks indicate that a duplicate account has been registered; the account is suspended until further checks are made to determine whether or not this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

Should the fraud management department have any doubts about any of the information submitted at registration stage or have any doubts whatsoever, further identification verification should be carried by requesting supplementary documents from the player. The documents requested are:

- scan of identification document e.g. id card or passport
- scan of credit card (if required)
- valid proof of address e.g. utility bill (not older than 6 months)

Should the fraud department still not be satisfied, they should ask for further documents. If in doubt the MLRO should be consulted.

5.4. Due Diligence

Player KYC and due diligence shall be ongoing and conducted on a risk-sensitive basis in situations, which by their nature, represent a higher risk of Money Laundering or Financing of Terrorism. The Fraud & Payments Manager is responsible for setting out a matrix which scores risk according to criteria which influence the risk rating.

5.5. Standard Due Diligence

The following events will trigger the standard due diligence procedures and the account will need to be verified further:

- *Request to change account details like address, email etc.*
- *Attempts to withdraw using a method other than the one used to fund the account*
- *Accumulated transactions (Deposits and/or Withdrawals) above 2,000 Euro or 4,000 NAF*
- *Customer's activity raise suspicion.*
- *There are doubts about the veracity or adequacy of previously obtained customer identification data.*

Verification will take place by either of the following:

1. *Third party verification*
2. *Submission of the following documents:*
 - *scan of identification document e.g. id card or passport.*
 - *valid proof of address e.g. utility bill (not older than 6 months)*
 - *Proof of payment method ownership*

5.6. Enhanced Due Diligence

In cases where players, products or transaction are deemed to be of higher risk Enhanced Due Diligence (EDD) procedures should apply. The following events should trigger the EDD procedures:

- Player is a PEP (Politically Exposed Person)
- duplicate IPs
- IP shifting
- country of origin associated with higher credit card fraud
- attempts to create multiple accounts
- attempting to withdraw funds without using the funds to play
- splitting a withdrawal in several lower amount withdrawals in order to avoid hitting the verification threshold etc.
- Sudden changes in account activity
- For every account deemed as High Risk an Enhanced Ongoing Monitoring of the business relationship will be conducted.
- Player is deemed as VIP.
- The registered country is not part of the FATF white list.

In situations where EDD check is required the customer has to submit ID, utility bill and bank statement and proof of the source of funds for Enhanced ID Check within 30 days. If the customer does not send these documents within 30 days, the gaming account will be blocked from all transactions.

5.7. Record Keeping

The Company will keep the following records:

- transaction documents
- due diligence information
- information relating to suspicious transactions
- MLRO reports
- training in relation to AML matters, and
- policies and procedures

This information could be required on a timely basis by regulatory authorities. The documents as outlined should be kept for 5 years from the date of the transaction or the date of completion of any related transaction. Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years from the date the person concerned ceases to be a registered customer or from the date of the customers most recent activity. These records can be kept in documentary or electronic format.

5.8. Politically Exposed Persons (PEPs)

A Politically Exposed Person is someone who has been entrusted with a prominent public

function, such as a senior political figure. Individuals who are closely related to this person, for instance, immediate family members and close associates, are also considered as PEPs. PEPs are classified as a money laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

As a general rule within the daily work flow every client that has been identified as high-risk, EDD measures will be applied, and also additional checks are made to identify if the client is a PEP. EDD measures are applied to the customer identified as PEP and the close associates, in compliance with the directive.

The current PEP lists are consulted in order to identify a customer as PEP. Once established as PEP, the following steps are taken:

- Obtain the approval from risk management to maintain the business relationship.
- EDD measures are applied.
- Ongoing monitoring of the customer's / business partner activity.

6. Monitoring Transactions for signs of Money Laundering and Terrorist Financing

6.1. Suspicious Transactions.

There is a number of events which might raise suspicions of money laundering, and which require further scrutiny. The following are a few examples:

- Customer does not cooperate in the carrying of customer due diligence.
- Customer attempts to register more than one account with the same licensee.
- Customer deposits considerable amounts during a single session by means of multiple prepaid cards.
- Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposits, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer displays suspicious behavior in playing games that are considered as high risk.
- Artificially splitting a withdrawal to remain "below the radar".
- Unexplained or unclear source of wealth e.g. student playing large volumes of money the source of which cannot immediately be ascertained.
- Sudden changes in account activity e.g. the volume of transaction increases suddenly.

Any suspicions of Money Laundering should be reported internally to the MLRO. These reports should be document by means of an Internal Suspicious Transaction Report. The MLRO will then investigate the report and decide if it is necessary to escalate the report to the responsible authorities.

6.2. Tipping off.

It is extremely important that at no point is the customer to be informed that he/she is being investigated or that any transactions he/she made were flagged for suspicious activity. Such an action would qualify as “tipping off”. Tipping off could unnecessarily alarm the client if following investigations, it turns out that there is no suspicious activity going on, but more importantly it could forewarn anybody conducting criminal activity of the investigations and could prejudice investigations. If forewarned of an impending investigation a criminal could destroy evidence incriminating them. Tipping off is a criminal offence. No unnecessary staff should be informed of the suspicions; it is sufficient to initially just inform the MLRO. It is also important not to take any action which might indicate to the person being investigated of the suspicions e.g. suspending account for no immediate apparent reason.

6.3. Suspected Fraud/Money Laundering involving employees.

ML/FT activity and/or fraud can also be conducted by employees of the Company. Should any activities of Company employees raise suspicions of ML/FT or fraud, the same procedure should as with customer transactions should apply. The suspicious activity should be reported to the MLRO by means of an Internal Suspicious Transaction Report whilst avoiding tipping off and involving any unnecessary employees.

6.4. Failure to report.

One should always keep in mind that failure to report a suspicious transaction when there are “reasonable grounds to suspect” ML/FT activities is also a criminal offence.

7. Employee Training and Screening

7.1. Training

It is imperative that staff receive appropriate and regular training as to their responsibilities with regard to:

- customer due diligence measures
- record-keeping procedures
- internal reporting procedures
- policies and procedures on internal control, risk assessment, risk management, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to money laundering or the funding of terrorism
- relevant regulation in each jurisdiction where a license is held; and
- the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

Records are kept of all training given to staff together with confirmation that they have reached the necessary level of understanding and competence.

7.2. Screening

Staff who are dishonest present a fraud and business risk to remote gambling operators. The Company ensures that there is in place appropriate procedures for due diligence when hiring

employees.

This could include reference checks, credit record checks and other vetting measures including verification of information given during the recruitment phase, and confirmation of identity.

To summarize, employees should:

- be identified and verified
- be screened to ensure their probity
- receive appropriate training

8. Additional Monitoring Tools

Covery Solution

The Company applied tools provided by Covery Solution to protect its online business from various types of fraud and reduces operational overhead. Covery Solution brings together event chain analysis, feature engineering, rule management and machine learning to obtain the most accurate results. Covery Solution analyzes the global base of fraudulent and reliable identifiers and makes an automated decision whether an event should be accepted, rejected or whether it requires individual attention.

SumSub System

The Company applied tools provided SumSub System for lawful purposes of remote identity verification, fraud prevention, enforcement of AML/CFT laws and regulations, internal risk management and due diligence procedures, and other similar purposes (including AML Screening: International Sanctions, PEPs, Watchlists and Adverse Media).

9. Know Your Business – KYB

The Company applies KYB procedures in order to verify the identity of the business partners. This includes checks on background of business partner, its directors and the beneficial owners (and all individuals/entities in a holding structure of the business partner), with whom the Company contract or intend to contract.

The Company requests from each suppliers, providers and contractors with the KYB procedure:

- Company corporate ownership chart indicating all companies in the shareholding structure up to UBO/UBOs. If ownership is exercised through one or more companies, it is necessary to provide company certificates for each company up to UBO/UBOs;
- Extract from Register of equivalent document (corporate certificates) indicating directors, shareholders, registered address;
- Memorandum and Articles of Association of the company;
- Passport copies in regard to all UBOs and Directors indicated in the corporate structure;
- Utility bills or other evidence of residential address not older than 3 months in regard to all UBOs and Directors indicated in the corporate structure.

The Company reserves the right to request further documentation and information that the MLRO considers necessary to identify background of the suppliers, providers and contractors.

10. Reporting

The Nominated Money Laundering Reporting Officer is responsible to ensure that, when appropriate, the information or other matter leading to knowledge or suspicions, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the relevant authority. The MLRO will liaise with the relevant law enforcement agency on the issue of whether to proceed with a transaction or what information may be disclosed to customers or third parties.

The MLRO acts independently.

Any member of staff that has a suspicion that a customer is engaged in money laundering should report the matter to MLRO whose task is to decide whether it should be reported to authorities, which can also provide guidance on how to deal with suspicious customers. These reports will be delivered via an internal form, which will be kept on record even though the MLRO decide to not take the reported activity further.

The Board will also be responsible for ensuring this policy is implemented and that risk assessment is regularly updated. The Board complies as a minimum yearly report covering operation and effectiveness of the Company' policies and procedures to overcome the threat of ML. The Board should respond promptly to any reasonable requests for information made by a Regulator or law enforcement authorities.

APPENDIX A: SUSPICIOUS TRANSACTION REPORT

INTERNAL STR FORM	
Company details	
Company Name	
MLRO Name	
Date of STR	
Is Company currently refraining from carrying out a transaction because of this STR?	
Approximate aggregate amount of funds involved in Euro	
Is there a particular crime you deem relevant to this STR?	
Please provide, in chronological order, a brief explanation of the circumstances which gave rise to this STR, including reference to sanctions lists/ open-source information/ intelligence databases, transaction activity, customer behavior, where applicable	
Details of person involved in STR	
Name	
Title	
Gender	
Date of birth	
Country of birth	
Nationality	
Identification document type	
Identification document number	
Expiration date of identification document	
Residential address	
Country of residence	
PEP?	
Listed on a sanction list? Provide links and attach	

soft copy of information obtained	
Subject of a criminal investigation? If yes, please indicate which country, if known	
Business relationship information with person involved in STR	
Current status of business relationship	Active/ never initiated/ terminated/ termination in process
Date when established	
Date when discontinued	
Account information	
Account number	
Balance	
Date opened	
Date closed	
Date suspended or blocked	
Additional comments	