

Anti-Money Laundering and Prevention of Crime Policy

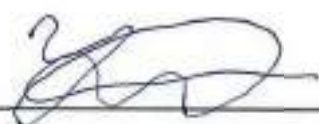
Magic Stones Limited

Version 1.8

Approved by the Board of Directors of Magic Stones
Limited Date of issue: 21.09.2023
Date of revision: 24.03.2025



Mr. Kostiantyn Vatan (UBO)



Mr. Maksym Uhnivenko (MLRO)

Table of Contents

Anti-Money Laundering and Prevention of Crime Policy Magic Stones Limited	1
TERMS AND DEFINITIONS	3
INTRODUCTION	4
Appropriate Legislation	4
MANAGEMENT AND STAFF	5
Senior Management	5
Money Laundering Reporting Officer	5
AML and Anti-Fraud Department	5
Front-office Staff	6
RISK ASSESSMENT	7
Customer Risk and Ongoing Monitoring	7
KYC (Know Your Customer) & CDD (Customer Due Diligence)	9
Customer Status and Deposit limitations	11
Politically Exposed Person (PEP) and Sanction List Checks	11
Screening Process	12
Suspicious Transaction Report	13
Collusion and Cheating	13
RECORD KEEPING	14
Retention of the Records	14
TRAINING AND EMPLOYEE CHECKS	15
Training	15
Employee Checks	15
Auditing	15
TRANSACTION MONITORING	16
Benefits	16
Access and Contents	16
Fraud Risk Block Rule and Fraud Risk Score Rule	16
High-Risk Countries	17

TERMS AND DEFINITIONS

- **AML** – Anti Money Laundering
- **CBCS** – Central Bank of Curaçao and Sint Maarten
- **CDD** – Customer Due Diligence
- **CFT** – Combatting Funding of Terrorism
- **CSAF** – Customer Support and Anti-Fraud
- **DE** – Designated Employee
- **Deposit** – Customer's purchase of the Company's services
- **EDD** – Enhanced Due Diligence
- **FATF** – Financial Action Task Force (www.fatf-gafi.org)
- **FIU** – Financial Intelligence Unit of Curacao
(<http://www.mot.cw/web/motweb/motweb.nsf/web/home?opendocument>)
- **MLRO** – Money Laundering Reporting Officer
- **NORUT** – National Ordinance Reporting Unusual Transactions
- **Principal** – Antillephone, N.V.
- **PEP** – Politically Exposed Persons
- **RBA** – Risk Based Approach
- **SAR** – Suspicious Activity Report
- **SDD** – Simplified Due Diligence
- **STR** – Suspicious Transaction Report
- **Withdrawal** – transferring of the gain
- **Transaction** – each single Deposit or Withdrawal, made by a Customer

INTRODUCTION

The current Anti-Money Laundering Policy is formed and designated to satisfy any applicable statutory requirements of the relevant legislation and to provide direction to Magic Stones Limited registered at H. 3 Chytron street, Flat/Office 301, P.C. 1075, Nicosia, Cyprus, billing agent of Magic Stones N.V. registered at Dr. H. Fergusonweg 1, 4797, Willemstad, Curaçao, operating under the Curacao Gaming License 8048/JAZ2021-006 granted by the Governor General of Curacao (hereinafter referred to as the "Company"), in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism. Money laundering covers wide-ranging circumstances involving any activity concerning the proceeds of any crime. This includes:

- Placement – the received from illicit activity funds are placed into the legal financial sector, e.g., as bets.
- Layering – the criminals make difficult to understand the source of funds by making a lot of transactions.
- Integration – the illicit funds re-enter into the economy as a legal funds, e.g., as bet gains.

To avoid using of the Company's services for turning illegal money raised through criminal activity into legal funds, possessing or transferring the benefit of acquisitive crimes such as theft and fraud, possessing or transferring stolen goods, being directly involved with any criminal or terrorist property, terrorism financing or entering into arrangements to facilitate the laundering of criminal or terrorist property, and criminals investing the proceeds of their crimes, the Company has established and applied this Policy. This document sets out the Company's policies in this area, so that management and staff are aware of their obligations and the procedures that must be followed.

The Policy is updated at least once a year, or more frequently based on the international requirements and legislative changes.

Appropriate Legislation

- Any relevant measures/guidelines which may be issued from time to time by the Government of Curacao related to the Scope of the Policy.
- The FATF Recommendations.
- National Ordinance Reporting Unusual Transactions.
- Netherlands Anti-Money Laundering and Counter-Terrorist Financing Act.
- Anti-Money Laundering Directive 2004/1640 .
- Any relevant measures/guidelines which may be issued from time to time by the Curacao FIU and CBCS.

MANAGEMENT AND STAFF

Senior Management

Senior Management of the Company has the overall responsibility for the AML compliance. Senior Management should ensure that the Company's employees have carried out a risk assessment for the Company business activity and implement policies and procedures to reduce the risk that criminals may exploit the Company's services. Senior management receive and consider MLRO reports and assist, if it is necessary, in implementing any policies recommended by the MLRO.

Money Laundering Reporting Officer

A Money Laundering Reporting Officer (MLRO) is appointed to be the responsible person of the AML/CFT, Risk Assessment, Controls, Policies and Procedures. The MLRO for Magic Stones Limited is Mr. Maksym Uhnivenko. Should this information change, the Company will inform the relevant authorities and update the Policy.

The MLRO has the authority to act independently in carrying out his responsibilities, free to have unhindered access to the relevant gambling operators and law enforcement agencies and is free to liaise with the law enforcement agencies on any question of whether to proceed with a transaction in the circumstances (e.g., in relation to a defense of appropriate consent). The MLRO responsibilities shall include but are not limited to:

- Development and regular revision of AML Policy
- External Reporting of Suspicious Activity or Transactions to the appropriate agencies
- Monitoring and management of compliance with, and the internal communication of, such policies and procedures and connecting with Law Enforcement Authorities
- Managing information requests received from the Authorities
- Promoting internal control
- Risk assessment and management
- Attending regular AML meetings with different stakeholders
- Ensuring customer due diligence measures and ongoing monitoring
- Ensuring the appropriate record-keeping
- Monitoring of relevant staff screening, and ensuring that team members are properly trained on an ongoing basis in their duties and obligations

AML and Anti-Fraud Department

The Company establishes its own Anti-Fraud department to prevent fraud and cyber-crime risks, and also uses external services, e.g., Sum&Substance and NameScan for online KYC and PEP check. Additionally, AML and Anti-Fraud Department uses the following resources in order to check Company's Customers:

- <https://namescan.io/FreePEPCheck.aspx>
- <https://www.cia.gov/resources/world-leaders/>
- <https://www.rulers.org/>

The main responsibilities of AML and Anti-Fraud department are:

- Monitoring the results of the ongoing automatic KYC process
- KYC records keeping
- Detecting, determining, and reviewing of the suspicious and high-risk transactions in the system
- Investigating of the fraudulent and suspicious activities on transactions to prevent losses and engagement in chargeback and refund disputes
- Evaluating of the effectiveness of fraud detection systems and strategies
- Recommending the alternative processes to MLRO if it is applicable

Front-office Staff

Customer Support and Account Management are the departments that face the Company's Customers. As the business unit having direct contact with the Customers, the front-office staff might be influenced by the Criminals to help them to avoid the Company's internal KYC and AML/CFT procedures. That is why it is necessary for the MLRO and the management to provide clear information regarding the relevant KYC and AML/CFT procedures, their importance, to provide the procedures for the reporting of such Customers, and to clarify the personal and the Company's risks in entertainment in the illicit activity.

Front-office staff responsibilities:

- Helping the Customers with KYC process and other issues if it is necessary
- Maintains customer records by updating account information
- Providing compliances (requests for the refunds and other legal issues) to the responsible departments
- Resolves service problems
- Sorting security issues

RISK ASSESSMENT

The Company adopts a risk-based approach and shall carry out a yearly risk assessment to:

- Identify ML/FT Vulnerabilities
- Identify ML/FT Threats
- Identify ML/FT consequences/impact and
- Identify any new requirements

The risk assessment allows the Company to develop a risk profile for the customer and to categorize the ML/FT risk posed by such customer as low, medium, or high. Based on the results of the Risk Assessment and if deemed necessary, to minimize any new risks identified or existing risks being re-classified, the measures, policies, controls and procedures would need to be reviewed and amended accordingly. The risk assessment should also be updated whenever substantial changes to the Company's systems, processes and overall operations are affected. External influences such as changes in legislation and regulatory communications may also cause the need for a risk assessment review.

The risk assessment should also be updated whenever substantial changes to the Company's systems, processes and overall operations are affected. External influences such as changes in legislation and regulatory communications may also cause the need for a risk assessment review. The Risk Assessment and related measures, policies, controls, and procedures are to be stored and to be made readily available for review by the FIU and other interested authorities at any time.

Customer Risk and Ongoing Monitoring

After registration, a customer's activity will undergo ongoing monitoring regarding any changes in the customer's pattern of activity which must be analyzed to determine whether the Company needs to reconsider the customer's risk level depending on the changes in customer's activity and to establish the point of reaching any relevant due diligence thresholds.

AML and Anti-Fraud Department shall (with the help of the Front Office Staff) examine with particular attention, and to the extent possible, the background and reason for any complex or large transactions and any transactions which are inconsistent with a particular customer's past activities, or likely, by their nature, to be related to money laundering.

Appropriate notes are to be recorded at important stages of the customer's monitoring to record any significant event in the customer's relationship and thus substantiate the risk assessment of the customer. All relevant information on a customer will culminate in the relevant customers AML Case-History which will be a living folder which is updated over the life of the relationship with the customer.

KYC (Know Your Customer) & CDD (Customer Due Diligence)

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.

The Company shall use Customer Due Diligence (CDD) to know who the customer is and to build a customer profile so the Company could identify any unusual or suspicious behavior.

In compliance with Anti-Money Laundering Directive 2018/843, the Company shall apply CDD measures when carrying out transactions amounting to two thousand euro (2 000 EUR) or more. The Customer Due Diligence Procedure shall define the procedure used to carry out Customer Due Diligence including timeframes/thresholds when this will be triggered and in which cases Enhanced Due Diligence will need to be performed. As mentioned above, AML Case-Histories are created for customers and developed and enhanced over the course of the business relationship.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period. Should the CDD Procedure not be completed within thirty (30) days of such a request, the customer's account will be considered to have failed completing CDD and thus will be closed, all the rest funds will be refunded. Employees must then consider whether they need to report a suspected instance of ML/FT to the MLRO (via an internal STR). It will be then up to the MLRO to determine if the information available can be considered as sufficient for a STR to be made to the FIU Curacao. Unless an STR has been raised and consent sought to affect a transaction or clearing of an available balance, deposited funds still present on the customer's account will be returned to the deposit method, where it is possible.

The whole KYC&CDD Procedure can be summarized in five consecutive stages:

- 1) Online application and automatic pre-check of the new Customer
- 2) Customer Due Diligence
- 3) Investigation process
- 4) Acceptance or Rejection of the application
- 5) Record keeping procedure

Application

Before being able to play on the website a new Customer must fill the online application to create a personal profile. When filing the application, a client has to provide the following personal details:

- E-mail address
- Telephone number (optional)
- Password

Email address is verified via verification link after application is completed, which is sent automatically to the provided email. The customer will not be allowed to use his/her account unless the email is validated.

Once the above information is received the fraud department will screen the information for any false or suspicious information, possible duplicate/self-excluded accounts, PEPs and sanctioned lists.

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

If 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 will be closed.

Age verification

No customer under the age of 18 can register an account. The system does not allow persons under 18 to register an account. A number of tools are available on the market which can assist in the age and identification verification process e.g. GB Group and 192.com. At the moment the company is in the process of evaluating which tools are most suited for the company needs.

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 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:

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

In a situation when Fraud department remains unsatisfied with information provided, they should ask for further documents. If no doubts the MRLO should be consulted.

Customer Due Diligence

The new Customer can provide deposits up to 2 000 EUR per year in aggregate without additional verifications. Yet the total amount of deposits exceeds this threshold and/or the Customer wishes to make a Withdrawal, he must provide additionally:

- Name and Surname
- Sex
- Date of birth
- Address
- Phone number

The Customer provides these data by filling the corresponding fields in his Personal Account (Profile).

The provided data is checked by AML and Anti-Fraud Department according to this Rules. Should there be any warns or suspicions (e.g., PEP status suspicions or discordancy between the address and the phone number), the EDD procedures should be applied. EDD is also applied if the total year deposit amount exceeds 10 000 EUR.

Not acceptable clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship with the Company:

- Clients who fail or refuse to submit, the required documents and information for the verification of his identity, without adequate justification
- Clients who ask to open or maintain anonymous or numbered accounts or accounts in names other than the client's name stated in official identity documents
- Clients who ask to transfer its initial funds or make ongoing payments in cash
- Account in the name of a third person
- PEP or sanctioned person

Prohibited Countries

The Company does not enter into business relationship with individuals and legal entities of the following countries list:

- Afghanistan
- Albania

- Andorra
- Armenia
- Azerbaijan
- Barbados
- Belize
- Botswana
- Bulgaria
- Cambodia
- Ecuador
- Ethiopia
- Ghana
- Guyana
- Iran
- Iraq
- Israel
- Jamaica
- Kuwait
- Laos
- Mauritius
- Myanmar
- Namibia
- Nicaragua
- North Korea
- Pakistan
- Panama
- Papua New Guinea
- Sudan
- Syria
- Taiwan
- The Bahamas
- Uganda
- USA
- Yemen
- Zimbabwe

EDD (Enhanced Due Diligence)

If provided per online application Customer's data seems to be suspicious, and/or if the AML and Anti-Fraud Department suppose the Customer might belongs to at least one of the non-acceptable categories of the Customers, and/or total amount of the Customer's Deposits exceeds the 10 000 EUR threshold, the EDD should be applied. According to the Company's Enhanced Due Diligence procedures the Customer must provide the following documents:

- Notarized copy of the Local ID with the notarized translation to English, or Notarized copy of International ID, or Selfie with the International ID
- Utility bill in English not older than 3 months to prove the home address
- If the total Deposit Amount per year exceeds 100 000 EUR threshold, the source of funds has to be also provided

If the Customer refuses to provide any of these documents or provides fake documentation, the account must be immediately closed by the Company, and the rest of the funds must be refunded via the same method and to the same source that was used for Deposit. If it is not possible for the viable reason, the MLRO has the right to allow to make a refund to another payment method, that is acceptable for the

Customer by Written Resolution. Such Resolution has to be keeping for 5 years at least after the relationship with the Customer was closed.

All documents should be checked by AML and Anti-Fraud Department team, including automatic check by Sum&Substance and NameScan systems, the Written Resolution regarding the Customer's status has to be provided to MLRO and has to be keeping up at least 5 years after the relationship with the Customer is closed.

Additionally, each client must be checked through the search engines, such as Google.com, Yandex.ru, Yahoo.com or other. The result of such research should be fixed by screenshots or electronical printouts and saved in CRM system.

Acceptance or Rejection

If at this point, the Company has obtained all information necessary to establish to its full satisfaction the identity of a client and the purpose and intended nature of the business relationship, the client will receive confirmation that his application has been accepted.

If the client is declined, he will be informed about the decision of Compliance Department via email used for online application.

Customer Status and Deposit limitations

Each Customer has to be associated with one of the following groups:

- **New Player** – the Customer, who has registered, but not filled the Profile, and provided Deposits for the total amount less than 2 000 EUR per year and has requested no Withdrawals. The total Deposit limit for such Player is 2 000 EUR per year from the date of Registration.
- **Verified Player** – the New Player, who has filled his Profile and was accepted by AML and Anti-Fraud Department. The total Deposit limit for such Player is 10 000 EUR per year from the date of Registration.
- **Enhanced Verified Player** – the Verified Player, who has provided Deposits for the total amount at least 10 000 EUR per year and has successfully passed the EDD check. There is no total Deposit limit for such Player.
- **Active Player** – the Enhanced Verified Player, who has provided Deposits for the total amount more than 10 000 EUR but less than 100 000 EUR per year, made at least 10 Transactions, 1 of which is a Withdrawal.
- **VIP Player** – the Active Player, who has provided Deposits for the total amount more than 100 000 EUR per year. If the total amount exceeds 1 000 000 EUR per half a year, the Support Department must contact this Player and recommend to rest from the gambling and offer a free-will blocking of the Customer's account for the period from 2 weeks to 1 month with refunding of the rest of the funds.
- **Rejected Player** – any Customer that is not acceptable or has failed any DD procedure.

Politically Exposed Person (PEP) and Sanction List Checks

Customers are checked to confirm whether the customer is himself, or is a family member¹ of, or known associate² to, a person that is considered a Politically Exposed Person (PEP). Customers are also to be

¹ The spouse, or any partner recognized by national law as equivalent to the spouse; the children and their spouses or civil partners; and the parents

² 1) a natural person known to have:

- joint beneficial ownership of a body corporate or any other form of legal arrangement with the PEP; or
- any other close business relations with that PEP

2) a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP

screened for presence on the Sanctions List. The Company uses NameScan for these purposes and the following online resources:

- <https://namescan.io/FreePEPCheck.aspx>
- <https://www.cia.gov/resources/world-leaders/>
- <https://www.rulers.org/>

A PEP is an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies
- members of the governing bodies of political parties
- members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization

The Company uses the following lists to check whether the Customer is under the Sanctions:

- The United Nations (UN) Security Council consolidated sanctions list
- The EU's consolidated list of persons, groups and entities
- The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists
- The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list

Customers matching one of these are to be automatically considered as a high-risk profile and the Company has to reject providing the services to such Customers.

Screening Process

The Company shall automatically run the data of newly registered and current players across the screening database, using NameScan and open databases, that are derived from regulatory sources.

Information is uploaded on a daily basis from the following public services for the distribution of sanctions lists:

- OFAC - <https://www.treasury.gov/ofac/downloads/sdn.csv>
- EU - http://ec.europa.eu/external_relations/cfsp/sanctions/list/version4/global/global.xml

The Company deploys two main screening controls to achieve objectives: transaction screening and customer screening. Customer screening is designed to identify targeted individuals during onboarding or the lifecycle of the customer relationship with the Company, whereas transaction screening is used to identify transactions involving targeted individuals or non-cooperation countries. Company also conducts real-time screening of a cross border transactions against Sanctions Lists.

If the database finds that the player is a PEP/FS, the database shall input this data into the Company's back-office system, which is shared with us in the High-Risk Notifications Tab for Review by our CSAF Personnel. This list is reported daily in the High-Risk Notification Tab.

Any Notifications, matches or false positives which are later clear shall be recorded in the PEP Register by the CSAF Personnel.

In addition, once a player triggers the 2 000 EUR deposit threshold, the database will run another PEP check, as soon as possible but not later than 30 days after the threshold is triggered.

Financial Sanctions

Should a player be flagged as potentially being a person listed on a financial sanction list, the CSAF Personnel shall ensure that the player's account shall be immediately blocked and closed. An internal escalation of such a registration is to be made to the MLRO.

Once the appropriate investigation is carried out and it is confirmed that the player is indeed likely to be a person subject to Financial Sanctions, a Suspicious Activity Report ("SAR") will be submitted by the MLRO to the FIU to report the actions taken in respect of the player. Such a report may also request further guidance regarding any funds held within the player's account.

CSAF Action Taken

Should a player be flagged as a current PEP or of having been a PEP previously, the CSAF Personnel shall ensure the following:

- Complete the PEP or FS Register
- Notify the MLRO in accordance with the SAR Procedure
- Block this Customer account with the written notification to the Customer's mail was provided during the Registration process

Suspicious Transaction Report

An internal Suspicious Transaction Report is to be sent directly to the MLRO whenever there is a suspicion, it is known or there are reasonable grounds to suspect that a customer is engaged in ML/FT. Employees shall not divulge to co-workers and especially the customers that an STR has been made as this would be considered as 'tipping-off'. An employee who raises an STR must escalate this directly to the MLRO and must only notify and liaise with relevant team members as shall be described in the 'Internal Suspicious Transaction Report'.

An employee may discuss a case or request assistance from the MLRO in case of uncertainty whether to raise an STR. The employee shall refer to the "Internal Suspicious Transaction Report Procedure" for assistance on STR escalation.

Collusion and Cheating

It is an offence for a person to cheat at gambling, or to do anything for the purpose of enabling or assisting another person to cheat at gambling. A person can be guilty of this offence even if they have not won anything or improved their chances of winning. Cheating may consist of actual or attempted deception or interference in connection with the process by which gambling is conducted, or a real or virtual game, race or other event or process to which gambling relates. To mitigate the risk of customers or members of staff committing this offence, the following systems will be used:

- Internal auditing systems to identify any suspicious activity
- third party payment providers
- Staff (or immediate family members) are prohibited playing on the Website.

There are internal auditing controls in place to identify this which include but are not limited to new account verification, internet history of employee work computers. This restriction is set out in employee contracts and the employment handbook. If any cheating or collusion is identified by the Company or a third party, the relevant customer account(s) will be suspended, reported to the MLRO and an investigation will be commenced. If any Company employee is implicated, he/she will be suspended pending a full investigation.

RECORD KEEPING

The Company must keep all records of business transactions and KYC for at least 5 (five) years from the date that the business relationship ends.

The records that must be kept are:

- The Customer's KYC documents obtained under the Customer due diligence requirements as per the regulations
- The supporting records in respect of the business relationships or occasional transactions that are the subject of customer due diligence measures or on-going monitoring
- Records of when the first client identification and verification took place, and how
- Documents justifying exemption from identification, if applicable
- Senior Management, MLRO and AML and Anti-Fraud Department Written Resolutions

In relation to the evidence of a Customer's identity, the Company must keep the following records:

- A copy of the identification documents accepted, and the verification evidence obtained, or
- References to the evidence of the Customer's identity

The records that the Company keeps must be sufficient to form a complete audit trail for FIU officers to follow from the start of the transaction to the end. This is particularly important should the transaction later become part of an on-going investigation by law enforcement.

There are several different types of records the Company should keep:

- A copy of the evidence of identification presented.
- Details of where the copies of identification can be found, which should be filed and easily recoverable. The Company must keep these records for at least 5 (five) years from the date when the relationship with a client was finished.
- Business records. The Company must keep a record of all transactions, regardless of whether the ID of the client needed to be verified, for 5 (five) years.

All records of disclosures. Letters received from FIU, CBCS, Principal, National Police or any other correspondence with a law enforcement agency should be retained for at least 5 (five) years.

Retention of the Records

Records shall be created for, including but not limited to:

- This AML Policy and any procedures and compliance guides used as a basis for internal procedures
- AML Training
- Due Diligence information
- All investigations related to potential STR's
- Details of monitoring by the MLRO and any delegations of duties by the MLRO
- MLRO reports to senior management
- Internal and external STRs, including reasons for non-escalation/non-submission
- Correspondence between the MLRO and law enforcement, FIU etc.
- Internal reports not acted upon by the MLRO, stating why no further action was taken.

The applicable retention period for Due Diligence and STR/SAR records shall be not less than seven (7) years. For further information on record keeping, employees shall refer to the Due Diligence Procedures.

TRAINING AND EMPLOYEE CHECKS

Training

Upon the commencement of employment, employees that are to be involved with, or connected to, activities that would fall within the scope of the Policy are to be provided with ML/FT training. This training involves general awareness of Money Laundering and Terrorism Funding, guidance on the appropriate measures, controls, policies and procedures in place within the Company; and an assessment to ensure that the employee has understood the key points of this training.

The training described above shall be recorded and a refresher shall be given annually. Employees that are to be involved with, or connected to, activities that would fall within the scope of the Policy are also required to read and acknowledge the AML Policy.

Employee Checks

Employees that are to be involved with, or connected to, activities that would fall within the scope of the Policy, shall be screened before the beginning of their employment to ensure that they are the appropriate fit to occupy positions in which they will participate in the provision of services to the customer.

Due Diligence documentation and where needed, the use of third-party screening providers may be used to assess the appropriateness of potential employees. The Company will conduct restricted and privacy sensitive monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity possibly affecting the Company's operations. Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and Director directly and should they wish to remain anonymous, to do this via an anonymous letter or email service providing as much information as possible.

The "Human Resources Policy and procedure" document shall contain further in-depth information on the related processes, as well as information on whistleblowing.

Auditing

The Company shall endeavor to carry out an internal audit strategy to audit the effectiveness of the level of implementation of these policies within the Company. When these audits are carried out, a report with findings from the audit, together with any recommendations, will be presented to the Board of Directors for their evaluation.

TRANSACTION MONITORING

In e-commerce, the fight against fraud requires maximum levels of know-how, speed, and flexibility. The Company uses effective risk management system that utilizes high-quality BIN and IP data bases which are constantly updated. The Antifraud System offers a real-time service that provides all the necessary analysis information and offers fully customized safeguards for handling dubious transactions.

Antifraud System allows each user to customize interface to perform specific tasks according to their role. Each Fraud Prevention Team member can set and maintain own monitoring criteria and request result report. Each result entry provides link to detailed result report for each transaction checked. Check result detail's view allows to quickly assess and review particular transaction and rules applied therein. Use of the Antifraud System does not, however, guarantee protection against all fraud, it only helps us to thwart it. The Antifraud System can be configured based on the risks or past fraud issues that have been encountered by the Company.

Benefits

Antifraud System enables you to:

- Detect anomalies during transactions
- Identify unusual patterns in fraudulent activity by combining real-time transactional data and historical analysis of customer behavior
- Immediately block attempts by recognized fraudsters
- Notify (or alert) to email about specific risks for the further review
- Protect against non-cooperative countries risks
- Adapt quickly to new fraud techniques by rapidly applying new rules
- Update and refine fraud rules in real time
- Get complete auditing transparency and traceability

Access and Contents

Access to the Antifraud System is provided to the Company's employees strictly under the access point from a unique IP working address or by permission of the Senior Fraud Prevention User or Administrator.

The availability of the functional areas depends on the user's role. For some user's role, the functional areas are limited. Roles typically reflect the list of activities that define a user's day-to-day job responsibilities. In the Antifraud System will be specified four (4) role types:

- 1) **Administrator** – responsible for user access management, reaction/notification configuration and updating dictionaries
- 2) **Senior Fraud Prevention User** – responsible for rule management, reports, statistical analysis, investigation and take necessary actions (such as adding to whitelists, action plan and reporting about suspicious activity to the Head of Compliance Department)
- 3) **Fraud Prevention User** – responsible for reported and potential fraud monitoring, analyzing, investigation and take necessary actions (such as adding to blacklists)
- 4) **Support Team User** – responsible for information checks, view-only access

Fraud Risk Block Rule and Fraud Risk Score Rule

"Fraud Risk Block Rules" are configured to monitor multiple combinations of different limits in a formula, summarizing calculated values for each limit and checking the result against a specified threshold of parameters simultaneously, such as:

- Transaction time
- Customer's historic transaction profile

- Customer statistics profile
- Transaction value (e.g., card number, card network, acquirer, e-mail and IP etc.).

Fraud Risk Block Rules checks that use the transactions history:

- **Logical** - a condition check ensuring that the country determined by the IP address (when present) is the same as the BIN country.
- **Constant** - the check is triggered if the expression describing this attribute becomes true on the substitution of the attribute values in the transaction.
- **Arithmetic** - the difference between two amounts or % ratio between two amounts.
- **List** - the presence (or absence) of a transaction attribute value in a Custom list.
- **Limit** - a condition checks the maximum time (e.g., minute, hour, day, month) amount/transactions for a client or on a specific card number, e-mail, IP address.
- **Statistical** - to compare a parameter value, calculated based on a user behavioral model, with a value that was received from a limit check (min, max, average, total).
- **Presence** – verify 3DS the presence or absence of an attribute in the transaction.

The easiest way to understand "Fraud Risk Block Rules" is to start with examples of potential fraud patterns, see below:

- Already blacklisted value in connection with the same customer
- Customer registration name does not match to the cardholder's name
- High value transaction or transactions by the same customer within 1 day
- Identified fraudster name in connection with cardholder field
- Multiple cardholder names on the same card number
- Multiple cards from different countries by the same customer
- Multiple customer e-mail in connection with the same card and cardholder
- Multiple declined authorizations by the same customer
- Multiple refusals of 3D Secure attempts by the same customer
- Multiple transactions within 1 hour by the customer
- Reduction in transaction by specified card number
- Sharp transactions increase from the same BIN within 1 day
- Customer BIN country does not match to country IP
- High risk of fraud geographical location
- Rapid change of IP address location by the same customer
- Unusual activity in connection with the same IP address

Also, regardless of the mentioned patterns for the potential fraud, there could also occur some new potential fraud pattern, when the fraudsters use the cards. Therefore, the Fraud Prevention Team should always carefully analyze a transaction information and additional information (e.g., verification documents and customer personal account activity).

High-Risk Countries

The list below is considered as fraud high-risk transactions from best practice fraudulent cases experience, though not every transaction related to these countries will be fraudulent. Senior Fraud Prevention User is the person within the Company who is responsible for fraud high-risk countries list update. According to the best practice with fraudulent cases (e.g., massive fraudster attack) the list can be revised and updated whenever a necessary change is observed and at least once a year.

- Argentina
- Australia

- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Ghana
- Guatemala
- Guyana
- Egypt
- Indonesia
- Malaysia
- Mexico
- New Zealand
- Nigeria
- Peru
- Philippines
- Puerto Rico
- Thailand
- Venezuela