

ULTRASOFT N.V.

Anti-Money Laundering (AML) Policies

Contents

1	Definitions and Abbreviations	3
2	AML/CFT Policy	6
3	Objectives	6
4	Scope.....	7
5	Regulatory Framework	7
5.1	National regulations	7
5.2	International regulation	8
6	Risk assessment	8
7	The business partner risk assessment – an ongoing process	10
7.1	Risk categorization and risk factors	10
7.1.1	Low risk customer attributes	11
7.1.2	Medium risk customer attributes	11
7.1.3	High risk customer attributes	12
7.2	Initial onboarding form	12
8	Checks	13
9	Closed loop policy	14
10	PEP Screening	14
11	Enhanced Due Diligence (EDD)	15
12	Ongoing Monitoring / Screening	15
13	Scope and Employee Compliance	16
14	Record Keeping	16
15	Law Enforcement or Regulatory Authorities' requests. Monitoring and Reporting	16
16	Policy Review	17
17	Contact Information	18
18	Appendix 1. Payment risk matrix	18

Revision History

Version 1.0

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
2.0	May 1, 2025	eMoore N.V.	Compliance function	May 1, 2026	-

1 Definitions and Abbreviations

Anti-Money Laundering (“AML”)	All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Caribbean Financial Action Task Force (“CFATF”)	An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gafic.org)
Combating terrorist financing (“CFT”)	Combating the Financing of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Counter proliferation Financing (“CPF”)	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
Counterparty	Any business counterparty of the company with whom an agreement has been signed.
The Company	Ultrasoft N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 159485.

Employee	Any person working for the Company.
Financial Action Task Force ("FATF")	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)
Financial Intelligence United ("FIU")	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of unusual transaction reports (UTR) and other information regarding potential money laundering or terrorist financing.
Know Your Client ("KYC")	The mandatory process of establishing the identity of a counterparty and the verification thereof.
Money Laundering ("ML")	A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
Politically Exposed Persons ("PEP")	A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family members and close associates, are also considered 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.
Prohibited Countries	Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on

	which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC.
Proliferation Financing ("PF")	The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Service	Services provided by the B2B operator as outlined in the agreement with the Counterparty.
Terrorism Financing ("TF")	The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Unusual transaction	Any financial or operational activity conducted by a counterparty that is inconsistent with their known behavior, business profile, or legitimate operations, and may indicate potential fraud, money laundering, or regulatory evasion.

2 AML/CFT Policy

ML, TF and PF are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Entities involved in ML, TF and PF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such entities must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures.

PF may involve the financing for the sale, transfer, export, of weapons of mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a significant threat to international peace and security, as identified by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CFT measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

3 Objectives

This Policy outlines the AML/CFT/CPF strategy of the Company in order to:

- ensure that statutory and regulatory obligations to prevent ML, TF and/or PF are met, taking positive action to minimize risk of the Company's products and services being used for the purpose of laundering funds and using proceeds of criminal activity, or terrorist financing;
- ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML, TF and/or PF;
- terminate any relationships where the Counterparty conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and
- comply with the Company's AML/CFT/CPF obligations based on national and international regulations.

4 Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

5 Regulatory Framework

5.1 National regulations

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

1. The National Ordinance on Money Laundering (P.B. 1993, no. 52);
2. The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2024 no.41(N.G.2017, no. 92) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
3. The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G.2024 no.41 (N.G. 2017, no. 99) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
4. The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
5. Kingdom sanction act (N.G. 2016, no. 54)
6. Sanctions National Ordinance (N.G. 2014, no. 55) together with all related amendments thereto and all related National decrees containing general measures and Ministerial Decrees with general operations;
7. National Ordinance on the Obligation to report Cross-border Money Transportation N.G. (2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

5.2 International regulation

As a member of the FATF and of the CFATF, Curaçao is meeting international standards by regularly implementing these standards in its national legislation. On an international level, the FATF plays an important role in the combating of ML and the TF and proliferation of weapons of mass destruction.

The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

6 Risk assessment

The possibility of online gaming being used by criminals to assist ML, TF and/or PF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

- i. identifying the ML, TF and PF risks relevant to the Company;
- ii. assessing the level of risk.
- iii. understanding the impact of the risk;
- iv. designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- vi. recording what has been done and why.

In view of the above, the Company has conducted a risk assessment to identify and analyze the AML risks faced by the Company and to ensure that the identified risks are properly mitigated and resources adequately invested.

Business risk assessment

The following table provides an overview of the AML risks identified when rendering services:

Risk ID	Risk Description	Likelihood	Impact
AMLBB001	Failure to verify ultimate beneficial ownership (UBO) of client operators	4	5
AMLBB002	Inadequate onboarding checks for B2C operator clients	4	4
AMLBB003	Delayed or inaccurate suspicious activity reporting (SAR)	3	5
AMLBB004	Inadequate monitoring of client transaction patterns	4	4
AMLBB005	Failure to screen clients against PEP and sanctions lists	3	5
AMLBB006	Poor documentation and record-keeping of AML processes	3	4
AMLBB007	Staff unaware of AML red flags due to inadequate training	4	4
AMLBB008	Clients operating in or serving high-risk jurisdictions	4	5
AMLBB009	Lack of periodic risk assessment updates	3	4

AMLBB010	Inconsistent application of enhanced due diligence (EDD)	4	5
AMLBB011	Failure to identify nested or layered corporate structures	3	4
AMLBB012	Technology gaps in detecting AML patterns or anomalies	3	4
AMLBB013	Manual AML reviews causing backlog and exposure	4	4
AMLBB014	No central system for tracking AML case management	4	4
AMLBB015	Failure to update AML policy in response to regulatory change	3	5

Mitigation strategy and residual risk towards AML risk

The following tables show the Mitigation strategy to be implemented and the effectivity rate, followed with the activities to reduce residual risk, the risk score, the residual risk score and the residual risk level.

Risk ID	Mitigation Strategy	Mitigation control effectiveness
AMLBB001	UBO verification tools, document validation checks	6
AMLBB002	KYC automation, onboarding checklist enforcement	6
AMLBB003	Automated SAR generation, MLRO escalation triggers	7
AMLBB004	Deploy real-time monitoring, anomaly detection	6
AMLBB005	Integrate global watchlist screening system	6
AMLBB006	Centralized document repository, audit trails	6
AMLBB007	Mandatory AML training, annual refresher sessions	5
AMLBB008	Jurisdiction screening and geo-fencing alerts	6
AMLBB009	Annual risk assessment with change indicators	5
AMLBB010	EDD workflow automation and exception monitoring	6
AMLBB011	Legal structure validation tools, hierarchy mapping	6
AMLBB012	AML analytics system, pattern recognition models	5
AMLBB013	AML case load dashboard, triage prioritization	5
AMLBB014	Case management platform with status tracking	6
AMLBB015	Subscription to legal updates, internal SOP refresh	5

Risk ID	Activities to reduce Residual risk	Risk score	Residual risk score	Residual risk level
AMLBB001	Enhanced onboarding for corporate entities, automated UBO check tools	20	14	Medium
AMLBB002	Revise checklist, enforce KYC preconditions	16	10	Medium
AMLBB003	Expand alert criteria and update SAR triggers	15	8	Medium
AMLBB004	Link client activity to benchmarked patterns	16	10	Medium
AMLBB005	Daily sanctions screening updates, audit logs	15	9	Medium
AMLBB006	Quarterly record reviews and audit sampling	12	6	Low
AMLBB007	Introduce AML e-learning tracking system	16	11	Medium
AMLBB008	Monitor country risk shifts and client exposure	20	14	Medium
AMLBB009	Integrate auto-risk rating engine	12	7	Medium
AMLBB010	Deploy EDD case monitoring reports	20	14	Medium
AMLBB011	Include corporate mapping in onboarding forms	12	6	Low
AMLBB012	Deploy unsupervised learning models	12	7	Medium

AMLBB013	Expand analyst team and triage support	16	11	Medium
AMLBB014	Centralize workflows with escalation paths	16	10	Medium
AMLBB015	Quarterly review of regulatory horizon and SOPs	15	10	Medium

Risk Appetite and Thresholds.

Ultrasoft N.V. has a defined risk appetite with respect to AML/CFT/PF exposures. Residual risks scored as **‘High’** will be escalated to the MLRO for review and approval. Where mitigation is deemed insufficient, the client relationship may be suspended or declined.

Any **medium-risk** clients must be subject to enhanced due diligence (EDD) procedures, while low-risk clients may follow the standard due diligence process.

7 The business partner risk assessment – an ongoing process

Ultrasoft N.V. operates in a number of different jurisdictions, which often have differing Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) requirements. Prospective and existing Business Partners are normally considered to have been engaged or to engage with Ultrasoft N.V. (“the Company” or “We”) to make use of the company’s remote gaming services or supply the company with a service. Therefore, a “normal” business partner will not be automatically suspected of having registered to carry out money laundering or financing of terrorism.

We conduct KYB (know Your Business) checks as an important part of our risk mitigation, regulatory compliance, strengthening business relationships, and protecting business reputation. These checks help us identify and avoid potential risks related to fraud, money laundering, and other financial crimes. They also ensure businesses comply with legal requirements, fostering transparency and trust in business relationships.

A KYB check is a process the Company uses to verify our partners' identity (clients, suppliers or other companies we engage with). It involves checking various components such as business registration, licenses, physical address, source of funds, and more to assess risk and ensure compliance with international regulations.

Initial research and data gathering is the first stage, the Company will collect detailed information about the prospective business partner. This includes legal name, physical address, contact information, and information about corrupt business owners and key management personnel.

During the verification stage, the Company uses the information provided to validate the collected information. This is typically achieved by cross-referencing the data with reliable sources, such as government databases, financial institutions, or trusted third-party data providers.

As soon as the data has been verified, the company will consider several factors, including the partner’s identity, location, industry, financial health, and management. The resulting risk profile can guide subsequent decision-making regarding potential partnerships or collaborations.

7.1 Risk categorization and risk factors

The customer’s risk assessment will result in assigning one of three levels of risk to a customer upon reaching €20,500 threshold (calculated on the basis of a rolling period of one hundred eighty (180) days). These will be defined as follows:

- Low risk
- Medium risk

- High risk

These levels will be defined as follows, but one must keep in mind that there will always be cases that may not fit into one specific range. In such cases, a cautious approach should be taken, and additional due diligence and/or consultation should be carried out with supervisors to ensure the assessed risk level of a customer is appropriate.

Main factors that affect the risk assigned to the customer are:

- a) Customer risk
- b) Geographical risk
- c) Transaction and product risks
- d) Delivery channel risk, as well as reputation and nature and behaviour of the customer which might indicate certain the level of risk.

As part of ongoing monitoring and when the trigger events occur the customer risk is to be reviewed and updated to ensure that the risk assigned to the customer is still relevant.

Control Effectiveness Monitoring and Documentation.

The effectiveness of all AML controls is periodically tested through internal audits, walkthroughs, and performance reviews. Weak controls are escalated to senior management for remediation.

All actions taken in connection with the Business Risk Assessment, including the justification for risk ratings, mitigation decisions, and client treatment, are documented in the central compliance system. These records are retained in line with regulatory data retention obligations and are made available for audit or inspection on request.

7.1.1 Low risk customer attributes

- Operators incorporated in a country not considered to have a high risk of money laundering, terrorist financing, corruption, fraud and having completed registration with plausible identification details and complete profile information (onboarding questionnaire);
- Operators with remote gaming licences in reputable jurisdictions;
- Operators accepting deposits from players with low-risk payment methods only (refer to Appendix 1);
- Operators using a limited number of payment methods which are in the Company's name;
- placed reasonable bets on the company's remote gaming products in line with "normal" gaming activity seen from regular customers with the same registration country or funding patterns;
- Operators permitting closed-loop withdrawals whereby the withdrawals are requested to the same payment method from which those funds originate and are not substantially higher than those deposited by the players;

7.1.2 Medium risk customer attributes

- Operators accepting business only from players with valid-looking registrations who register from unusual countries not targeted by the company but that are not countries with high risks of money laundering, terrorist financing, corruption, fraud, etc;
- Operators accepting deposits with low-medium and/or medium risk payment methods only (refer to Appendix 1);
- Operators of whose betting activity is above average for the market trends, but not alarming;

- Operators permitting withdrawals to a different payment method due to payment method inability to receive withdrawals which has been confirmed to be true;

7.1.3 High risk customer attributes

- Operators incorporated in, having links to, or is using payment methods issued in high-risk and/or non-reputable jurisdiction with relation to ML/FT;
- Operators accepting players with an invalid or suspicious registration details, origin IP address not matching customer country;
- Operators with remote gaming licences in non-reputable jurisdictions or operators operating without a remote gaming licence;
- Operators accepting players suspicious of identity theft;
- Operators accepting players who attempted to open multiple accounts;
- Operators accepting players of whose account is used from multiple locations within an unreasonable timeframe or change of pattern from normal usage;
- Operators accepting players identified as a Politically Exposed Person;
- Operators involved/associated with Politically Exposed Persons;
- Operators accepting deposits using third party payment methods or uses high risk payment methods such as quasi-cash payment methods;
- Operators accepting players that deposit unreasonable amounts in relation to their betting activity or when they would still have funds within their account which were available for betting;
- Operators accepting players of whose betting activity is beyond expected betting behaviour in relation to similar players and own funding sources or wealth;
- Operators accepting players who request withdrawals to alternate payment methods rather than to the origin of customer funds or request withdrawals to third party payment methods;
 - Operators who are reluctant to provide due diligence documentation;
- Operators flagged by payment providers, verification providers, law enforcement bodies or other industry collaborative platforms as potentially suspect customers or engaging in fraud, money laundering, terrorist financing etc.

Stress Testing and Scenario Simulation.

To evaluate the robustness of its AML control environment, the Company performs scenario-based stress testing. These simulations are designed to mimic realistic but adverse events, such as the onboarding of a shell company, rapid transactional spike, data breach, etc.

7.2 Initial onboarding form

Prior to entering into an agreement with a business partner ('Operator'), the Company shall commence the onboarding process only after a duly completed Due Diligence Form has been received from the prospective partner.

Basic provision of documentation

Version 1.0

Once a partner has completed the initial onboarding form, the partner is requested to complete the process by providing the following:

For the Operator:-

1. Operator certificate of incorporation or equivalent official document showing name of company, date of incorporation, and current registered office address;
2. Operator memorandum & articles of association;
3. Operator certificate of good standing (from within the past 6 months) or the equivalent;
4. Official document showing current shareholders and directors of the Operator dated within the last 3 months;
5. Copy of Operator ownership structure diagram detailing all associated companies up to the controlling entity/UBO, with ownership displayed in percentages of held shares / voting rights held;
6. Copy of licence/s and/or permits held by Operator;
7. Copy of Operator policies relating to AML / CFT

For other corporate shareholders in the Operator's structure up until the UBO:-

1. Certificate of incorporation or equivalent official document showing name of company, date of incorporation, and current registered office address;
2. Certificate of good standing (from within the past 6 months) or the equivalent;
3. Official document showing current shareholders and directors dated within the last 3 months;

For directors of the Operator:-

1. Certified copy of passport;
2. Certified recent utility bill (issued within the last 3 months)

For natural shareholders or natural UBOs owning more than 10% of the Operator [through voting rights and/or ownership rights]:-

1. Certified copy of passport;
2. Certified recent utility bill (issued within the last 3 months).

The company will accept documents provided in Original/ Certified True Copy. Should the document be originally issued in a language other than English, this must be accompanied by a translation document.

8 Checks

The following checks are done at the onboarding stage of an Operator:

Business registration or license verification: the company shall validate the legality and legitimacy of business activities of the partner business entity by examining its business registration status or other licensing documentation. This step helps confirm that you are dealing with a legitimate, legally recognized business and not a fraudulent entity. This stage can be completed solely on Google Checks and by cross-referencing the data with reliable sources, such as government databases, financial institutions, or trusted third-party data providers.

Sanctions Screening: the company will ensure that prospective business partners are checked to confirm whether the UBOs or individuals within the managerial level are listed on a Sanctions List. The respective individuals will also be continuously screened on an ongoing basis.

PEP Screening: the company will check to confirm whether the UBO or the Directors of the prospective business partner is or is a family member or known associate to a person who is considered a PEP.

Business risk analysis based on location: Geographical location significantly impact a business's risk profile and due diligence further. A company operating in a region known for high corruption levels or financial crime rates may pose a higher risk, and additional due diligence requirements may be required.

9 Closed loop policy

The Company conducts the day to day gaming operations under a stringent closed loop policy on payments effected by and to business partners.

In each case where the closed loop policy is not followed, the Company must obtain proof of ownership of payment methods from the business partner.

Any such secondary payment methods must be a payment method in the partner's name, licensed in the European Economic Area (EEA) and subject to equivalent ML/FT legal obligations, preferably but not mandatory, a Bank Account that is issued in the name of, and country of residence of, the respective entity.

Where the risk assessment following the above checks indicates a risk of fraud or potential ML/FT, the payment should be marked and put on hold whilst further actions are taken, such as:

- Checking the business partner information with payment providers or verification services provided in case of suspected fraud, or
- Placing payment on hold (not visible to the payment provider, no specific note placed into the account stating this) whilst an internal investigation is being carried by the fraud team.

If the payment is legitimate and no further actions need to be performed, the payment will be processed.

10 PEP Screening

All business partners, directors, UBOs and relevant individuals are screened to determine if they are Politically Exposed Persons (PEPs), or closely associated with a PEP. If a PEP is identified, the partner is subject to EDD. Screening is both at onboarding and continuously thereafter.

11 Enhanced Due Diligence (EDD)

EDD is applied to high-risk customers, including PEPs or entities in high-risk jurisdictions. The following documents are required:

- Detailed source of funds and source of wealth declaration;
- Certified copies of ID and proof of address;
- Ownership structure and control diagram;
- Justification for business relationships and financial activities.

EDD is documented and reviewed at least annually.

12 Ongoing Monitoring / Screening

The Company will run, in addition to the Onboarding checks in terms of Section 2, ongoing monitoring and/or screening to the Operator, and these ongoing monitoring and/or screening shall be conducted on a risk-based approach. Based on risk, the Company shall request, from the Operator, updated documentation and/or information, on a yearly basis.

The frequency of due diligence reviews depends on the risk level:

- Low-risk entities: every 12–18 months;
- Medium-risk: annually;
- High-risk: at least every 6 months or upon trigger events.

The following factors shall be investigated and/or conducted on a yearly basis:

Business registration or license verification: the company shall validate the legality and legitimacy of business activities of the partner business entity by examining its business registration status or other licensing documentation. This step helps confirm that you are dealing with a legitimate, legally recognized business and not a fraudulent entity. This stage can be completed solely on Google Checks and by cross-referencing the data with reliable sources, such as government databases, financial institutions, or trusted third-party data providers.

Sanctions Screening: the company will ensure that prospective business partners are checked to confirm whether the UBOs or individuals within the managerial level are listed on a Sanctions List. The respective individuals will also be continuously screened on an ongoing basis.

PEP Screening: the company will check to confirm whether the UBO or the Directors of the prospective business partner is or is a family member or known associate to a person who is considered a PEP.

Business risk analysis based on location: Geographical location significantly impact a business's risk profile and due diligence further. A company operating in a region known for high corruption levels or financial crime rates may pose a higher risk, and additional due diligence requirements may be required.

Depending on patterns observed, the ongoing monitoring processes can be adjusted to focus on specific patterns and trends or to identify any future similar patterns in new Business Partners.

Tipping off a business partner that suspicions have been noted or escalated is a criminal offence with a potential of serious criminal prosecution that may result in high fines, years of jail-time penalties and a tainted criminal record which would limit the employee from further employment within relevant positions.

13 Scope and Employee Compliance

This policy applies to all employees, contractors, and managers of the Company. Everyone is expected to comply fully with AML/CFT obligations.

Failure to comply may result in:

- Internal disciplinary action;
- Suspension or termination;
- Referral to law enforcement for criminal proceedings.

14 Record Keeping

Records of information and documentation obtained produced or obtained are to be kept in the file and a periodical review to ensure valid data is still held is to be performed. Records kept up to a minimum of five (5) years after business relationship is terminated but may be extended at the requirement of the relevant authorities. The following records are to be maintained:

- Agreement with the Operator;
- Up-to-date company structure, including voting rights, UBOs and Directors;
- Good standing certificate and/or equivalent document for the Operator;
- Operator UBO's proof of ID and proof of address;

Electronic data is stored in a secure storage system with immediate access ability controlled with preassigned access control privileges and full back up facilities.

Once the period of obligatory retention requirements expires, the data, in any stored format, is to be disposed of in a secure manner as per industry best practice to ensure adequate data protection.

15 Law Enforcement or Regulatory Authorities' requests. Monitoring and Reporting

The company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies in relation to investigations of a criminal, civil or regulatory nature.

When such requests for information are received, these are to be forwarded in their entirety to the company legal counsel.

Depending on the nature of the request and irrespective of whether the request for information will be handled by the legal counsel or the compliance team, it will be handled in line with the following process:

- Record the receipt of such a request;
- Verify the legitimacy of the requesting organisation and individual making this request;
- Verify the legal basis under which such a request is made;
- Inform the requesting organisation that the request is being looked into and provide the appropriate contact information for the legal counsel;
- Identify the business partner relevant to the request;
- Analyse the business partner's information, including amongst others due diligence, transactions and ongoing monitoring information;

- Re-consider the business partner's risk status considering the received request and take appropriate action depending on the case;
- Identify information that is relevant to the request and following a due assessment of the information, prepare for provision to the requestor, if any; and
- Update the company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.

Monitoring of Unusual Activity & Reporting to FIU: The Compliance Officer is responsible for reviewing transactions that appear unusual. Suspicious Transaction Reports (STRs) are submitted to the Curaçao FIU (MOT) in a timely manner. Tipping-off, as mentioned earlier, is strictly prohibited and may result in criminal liability.

16 Policy Review

The AML Policy is reviewed at least once per year. Earlier reviews may be triggered by:

- Changes in law or FATF recommendations;
- Internal audits;
- Changes in business activities or risk profile.

17 Contact Information

For any questions regarding this policy, please contact:

eMoore N.V.

Legalcompliance Department

Groot Kwartierweg 10, Livestrong Building

Willemstad, Curaçao

Telephone: +599 9 7471401

Email: legalcompliance@the-emgroup.com

18 Appendix 1. Payment risk matrix

FUNDING METHODS

Method	Low	Low - Medium	Medium	Medium- High	High
Bank Transfers (EEA or equivalent Safeguards)	X				
Debit/credit cards issued by banks	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-Licensed payment service providers (e.g. e-wallets)			X		
Non -EEA Licensed PSP (e.g. e-wallets)				X	
EEA-Licensed PSP that can be funded with cash or quasi-cash (e.g. Paysafecard e-wallet)				X	
Prepaid debit cards / vouchers, peer-to-peer transfers					X
Cash					X