

ANTI-MONEY LAUNDERING (AML) POLICY

Udwin B.V. (reg. 147117)

Address: Korporaalweg 10, Curaçao

Version: 1.4

Change History

Date	Ver.	Author	Summary Changes
September 2023	1.0	Udwin B.V.	First Version
December 2023	1.1	Udwin B.V.	New version of AML Policy
17.08.2024	1.2	Udwin B.V.	New version of AML Policy
31.01.2025	1.3	Udwin B.V.	New version of AML Policy
23.05.2025	1.4	Udwin B.V.	New version of AML Policy

Note: This policy is subject to review at least once every 12 months or upon any material change in regulatory obligations, operational processes, or identified risks.

Next Scheduled Review: May 2026

Contact information:

Name: Everhona Francisca Makaya

Position: Money Laundering Reporting Officer (MLRO)

Phone: +599 9 696 7068

Email: compliance@xcm.cw

Table of Contents

Table of Contents	3
1. Introduction	4
2. Scope	4
3. Definitions.....	6
4. Risk Assessment.....	8
4.1 Breakdown.....	8
4.2 Risk-based approach	9
4.3 Risk categorization.....	10
4.4 Risk score calculation	11
4.5 Customer Due Diligence level.....	12
5. Customer Due Diligence and Enhanced Due Diligence Procedures	13
Customer Due Diligence (CDD):	13
Threshold Approach	15
Ongoing Monitoring	15
Enhanced Due Diligence (EDD):	16
Identifying Suspicious Behaviours	18
6. Player Account and Fund Management.....	19
7. Suspicious and Unusual Activity Reporting & Compliance Management	21
8. Record Keeping	25
9. Training and Awareness	25
10. Ongoing Monitoring	26
11. Review and Audit	27
12. Policy Approval and Implementation.....	27
13. Sanctions, PEPs, and Adverse Media Screening	27
APPENDIX 1	29

1. Introduction

At Udwin B.V., our commitment to the highest standards of integrity and transparency in our operations is unwavering. This Anti-Money Laundering (AML) Policy reflects that commitment. We recognize that the online gambling sector, due to its virtual and cross-border nature, is potentially susceptible to financial malpractices including money laundering and terrorist financing. As such, we view it as our duty, not just as a legal obligation but as a moral one, to ensure that our platform and services are not used as a medium for such activities.

This policy outlines the measures, controls, and procedures we have instituted to detect, prevent, and report any attempt to use our services for money laundering or any related illicit financial activity. By adhering to this policy, we aim to uphold the trust our stakeholders place in us and fulfill our regulatory obligations, in particular, those set out by the applicable AML legislation and regulations.

This policy applies to all employees and outsource staff undertaking anti-money laundering, responsible gambling and anti-fraud procedures to the extent connected to their direct responsibilities, including senior management.

2. Scope

This Anti-Money Laundering (AML) Policy is crafted in compliance with, and with respect to, a comprehensive array of legislation and directives that govern the online gambling sector, both within Curacao and internationally. These laws and regulations aim to safeguard the industry, its stakeholders, and the public from the risks and consequences of money laundering and related financial crimes. The primary legal and regulatory instruments to which Udwin B.V. adheres include:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update August 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update August 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);

- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025;
- The FATF Recommendations, set forth by the Financial Action Task Force, which serves as the global standard for tackling money laundering, terrorist financing, and related threats to the financial system.

Udwin B.V. is committed to complying with both the letter and spirit of these laws, directives, and guidelines. The principles outlined in these instruments guide our daily operations, our risk management, and our customer relationship protocols, ensuring that our business practices are not just legally compliant but also ethically sound.

The Company continuously monitors and evaluates updates to all relevant Decrees and Regulations to ensure its internal policies and procedures remain fully compliant with evolving legal requirements.

3. Definitions

To ensure clarity and consistency throughout this AML policy, it is essential to define key terms and concepts central to our operations and our commitment to combat illicit financial activities. The following definitions provide a foundational understanding for all stakeholders:

Money Laundering

Money laundering refers to the process of making illicitly-obtained proceeds appear legal or 'clean'. Typically, it involves three stages:

1. **Placement:** At this initial stage, the 'dirty money' is first introduced into the financial system. This can be done through various means such as bank deposits, purchases of assets, or using the money for gambling.
2. **Layering:** This is the most complex phase wherein the illicit money is separated from its source by creating complex layers of financial transactions. The purpose is to confuse and cloud the paper trail, making detection and attribution difficult.
3. **Integration:** At this final stage, the 'cleaned' money is integrated into the legitimate economic and financial system and is used to acquire legal assets or finance other legal business ventures.

Terrorist Financing

This refers to the act of providing or collecting funds, by any means, directly or indirectly, with the intention or in the knowledge that they would be used to support terrorist acts or organizations. Unlike money laundering, which seeks to legitimize illicit proceeds, terrorist financing deals with legitimate funds used for illegitimate purposes. It can involve funds raised from both legal sources, like personal donations and profits from legitimate businesses, and from illicit sources such as drug trafficking or fraud.

Financing of Proliferation

Refers to the act of providing financial resources for the creation, acquisition, ownership, development, export, transportation, brokerage, transfer, storage, or use of nuclear, chemical, or biological weapons, as well as the materials and delivery systems associated with these weapons. This includes any funding that supports the spread and availability of these highly destructive weapons and their related components.

Understanding these definitions and their implications is crucial for our employees, partners, and stakeholders, as they guide our daily operations, decision-making processes, and overall strategy in ensuring Udwin B.V.'s platform remains resilient against financial malpractices.

Customer Due Diligence (CDD)

CDD refers to the process by which relevant information about a customer is obtained and evaluated for any potential risk for the business. This involves verifying the customer's identity

based on reliable, independent source documents, data, or information. The primary aim is to ensure that customers are genuinely who they claim to be, thereby preventing any misrepresentation.

Enhanced Due Diligence (EDD)

EDD is a more comprehensive set of procedures for customers, especially those presenting a higher potential risk for money laundering or terrorist financing. This can involve deeper scrutiny of any given transaction, understanding the source of funds, and additional identification measures. EDD is typically applied in situations where the risk associated with a business relationship or transaction is deemed higher, such as with transactions involving high-net-worth individuals or those from high-risk jurisdictions.

Politically Exposed Persons (PEP)

A PEP is an individual who holds or has held a significant public position or function, either domestically or internationally. Due to their status and influence, they are considered to present a higher risk for potential involvement in bribery and corruption by virtue of their position. PEPs include heads of state, senior politicians, senior government, judicial or military officials, top executives of state-owned corporations, and important political party officials. Relationships with family members or close associates of PEPs can also pose risks and are thus often subject to the same scrutiny. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,
- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state-owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organisation.

Family member of PEP means a close relative, in particular

- the spouse or civil partner,
- a child and the child's spouse or civil partner and
- both parents.

Financial Intelligence Unit (FIU)

A Financial Intelligence Unit (FIU), or FIU Curaçao (in Dutch: Financiële Inlichtingen Eenheid) is a central, national agency responsible for receiving, analyzing, and disseminating financial information and intelligence to combat money laundering, terrorist financing, and other illicit financial activities. FIUs play a pivotal role in the global framework to protect the integrity of financial systems by preventing and mitigating the potential use of financial channels for illicit purposes

As we progress through our operational and transactional dealings, it is essential that these terms and their associated processes are clearly understood and consistently applied. They provide a framework for Udwin B.V.'s approach to identifying, assessing, and mitigating potential risks, ensuring that our platform remains trustworthy and compliant with regulatory standards.

4. Risk Assessment

Within the risk-based framework, The Company will undertake risk profiling of all customers from the time they are registered for the potential money laundering/terrorism financing risks. It is important to note that the Company's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by GCB and FIU;
- Our own internal evaluation of our overall business risk assessment, and our knowledge and experience with our customers.

4.1 Breakdown

At Udwin B.V., we are dedicated to continually identifying, evaluating, and mitigating potential risks associated with online gambling, especially in the context of money laundering and terrorist financing. Here's a breakdown of our risk assessment approach:

- **Holistic Understanding:** We acknowledge that risks in the online gambling sector can emerge from various channels – be it customers, products, geographic areas, or delivery methods. To that end, our risk assessment extends across all facets of our business, ensuring no potential vulnerability goes unaddressed.
- **Dynamic Risk Profiling:** We understand that risks are not static. As the global landscape changes, new threats may emerge while old ones evolve. Hence, our risk profiling is a dynamic process, allowing us to adapt to the changing nature of threats, both known and emergent.
- **Customer Segmentation:** Different customer profiles may represent different levels of risk. By segmenting our customer base, we can apply a more tailored approach to our

due diligence processes. High-risk customers, such as Politically Exposed Persons or those from high-risk jurisdictions, might require more intensive scrutiny.

- **Products and Services Review:** Not all gambling products or services carry the same level of risk. We undertake regular reviews of our offerings to ascertain which might be more susceptible to money laundering activities and adjust our controls accordingly.
- **Geographical Considerations:** Certain jurisdictions or regions pose heightened risks due to their economic, political, or regulatory environments. We maintain a watchful eye on our dealings in such areas, ensuring we adhere to both local and international standards.
- **Technology Utilization:** In an era defined by technological advancements, we leverage cutting-edge tools and software to aid in our risk assessments. This not only enhances the accuracy of our evaluations but also ensures a swifter response to any detected anomalies.
- **Regular Updates:** To remain efficient and effective, our risk assessment protocols are reviewed and updated periodically. This ensures that our strategies align with the best practices in the industry and the most recent regulatory guidelines.

Through diligent risk assessment, Udwin B.V. aims to stay ahead of potential threats, ensuring the safety of our customers and the integrity of our operations. By proactively addressing vulnerabilities and adopting a culture of continuous improvement, we endeavor to be a beacon of trust and reliability in the online gambling sector.

4.2 Risk-based approach

The Company undertakes to prevent and combat money laundering and terrorist financing following a risk-based approach. A risk-based approach the Company summarised as covering the following areas:

- **risk identification and assessment** – identifying the money laundering risks facing the Company, given its customer, product, and services profile and having regard to available information, and assessing the potential scale and impact of the risks
- **risk mitigation** – identifying and applying adequate measures to mitigate the material risks facing the Company
- **risk monitoring** – putting in place management information systems (MIS) and keeping up to date with changes to the risk profile through changes to the business or to the threats, and
- **documentation** – documenting the risk assessment and strategy and having policies and procedures covering the above and achieving effective accountability from the board and senior management.

The Company employs a risk-based approach to evaluate and monitor the typical transaction volumes and amounts associated with its customers. If unusual or suspicious behavior is detected, additional checks or enhanced due diligence (EDD) may be performed to confirm that the activity corresponds with the customer's profile and to address potential risks.

4.3 Risk categorization

A core component of our risk assessment strategy at Udwin B.V. is the classification of our customers into distinct risk categories. This structured approach enables us to apply resources efficiently, focus our monitoring efforts, and ensure that our controls are proportionate to the level of risk presented. Our customer risk categorization is as follows:

- **Low Risk:** Customers falling into this category typically present a minimal risk of money laundering or terrorist financing. This could be due to their transaction patterns, source of wealth, or other demonstrable factors. Routine CDD processes are usually sufficient for this category, but we remain vigilant to ensure that any change in behaviour or transaction pattern is swiftly detected.
- **Medium Risk:** Customers in the medium risk category exhibit characteristics or transaction behaviours that, while not overtly suspicious, warrant a heightened level of scrutiny compared to the low-risk group. They may have business connections in high-risk jurisdictions, display irregular transaction patterns, or engage in higher-volume transactions. For these customers, we often employ periodic enhanced monitoring to ensure their activities align with their profile.
- **High Risk:** The high-risk category comprises customers who, due to various factors, present a substantial potential risk for money laundering or terrorist financing. This can be attributed to their status (e.g., Politically Exposed Persons), connections to high-risk regions, the nature and volume of their transactions, or other associated risk indicators. Customers in this category are subjected to Enhanced Due Diligence (EDD) measures, more frequent account reviews, and continuous transaction monitoring. Any unusual activity is promptly investigated, and necessary actions are taken to mitigate potential threats.

By segmenting our customer base into these defined risk categories, Udwin B.V. ensures that our monitoring and control measures are both efficient and effective. This stratified approach helps in tailoring our resources and processes according to the risk level, ensuring that high-risk entities receive the attention they warrant without overwhelming our systems with unnecessary procedures for lower-risk customers.

It is crucial to note that our categorization is fluid – customers can move between categories based on their activities, profile updates, or changes in the external environment. Regular reassessments ensure our classifications remain current and relevant, bolstering our efforts to maintain a secure and compliant platform.

4.4 Risk score calculation

The purpose of this procedure is to pick up minor incidents of ML/FT behaviour that by themselves may not warrant suspicion but, if combined with other behaviours, can do so. A player will be scored by the internal CMS system according to part of the factors above, and a risk score will be assigned. Each factor will generate a score, and the overall risk score will be a sum of the individual scores. The more negative the score, the higher the risk. Note that these factors, the scores and the thresholds are internal, and will be adjusted as we improve and update the RS Calculation.

Indicator	Description	Score
individual status		
PEP	A customer considered to be PEP	100
Adverse media	A customer was mentioned in negative news or information the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/blacklists	50
geographical location		
Not at home	A customer whose IP location is different from their registered address	20
High-risk country resident	A customer resides in a High-risk country	30
gambling behaviour		
Large sums no play	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50
Large sums big losses	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (EUR 5000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets	25
Big changes in money	Dramatic changes in terms of volume and size of player deposits or staking activity	20
Several gaming accounts	A customer is trying to register several gaming accounts	30
transactional behaviour		
Smurfing	A customer making multiple deposits or withdrawals of small amounts without no objective reasons	30
Spending above wages	A customers spend is outside of their affordability	20
No withdrawals	Player has never requested a withdrawal	-20
Withdrawal without playing	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
payment methods the player is using		
Card switching	A customer opening an account and registering several different cards and making transfers between them	20

High risk payment methods	A customer uses high-risk payment methods	30
fraud red flags a customer triggered		
VPN	Customer used a VPN	30

Once the score is calculated, a risk level is assigned:

<u>CMM Score</u>	<u>Risk Category</u>
0-20	Low
21 - 40	Medium
41 - and higher	High

Not all factors can be automatically included in the CRA calculation due to technical or practical reasons, but we do monitor for these risks in other ways. For example, we check for VPN usage or multi-accounting at the point of registration, we have a separate alert for players who use cards under a different name, and all withdrawals are checked before approval and payment.

4.5 Customer Due Diligence level

The level of customer due diligence (CDD) conducted on a player will depend on the risk score assigned to the player as follows:

	Low	Med	High
Verify ID and address with docs	X	X	X
Collect additional personal details	X	X	X
Collect Source of Funds/ Wealth info		X	X (with documentation)
Ongoing monitoring	X	X	X (Enhanced)
Additional measures to address any other risk identified			X
Report suspected cases of ML/FT	X	X	X

The frequency of customer reviews is determined by their assigned risk classification, which considers factors such as location, transaction behavior, and sources of funds. High-risk customers, including those from high-risk jurisdictions or exhibiting suspicious activity, are

subject to more frequent monitoring. Medium-risk customers undergo periodic reviews, while low-risk customers are reviewed at extended intervals.

5. Customer Due Diligence and Enhanced Due Diligence Procedures

At Udwin B.V., we recognize the significance of establishing and maintaining comprehensive Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures. These processes are cornerstones of our commitment to combating money laundering and terrorist financing. By understanding our customers better, we can effectively anticipate, identify, and address potential risks associated with their activities.

Customer Due Diligence (CDD):

The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

- identification – establishing identity by collecting information from the customer.
- verification – proving a customer is who they claim to be by obtaining and validating documents or information which supports this claim of identity, which come from a reliable and independent source.
- determining the identity of the beneficial owner and taking necessary measures to verify their identity, ensuring the casino fully understands who the beneficial owner is.
- gaining an understanding of the purpose and intended nature of the business relationship and collecting additional information where required.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing:

- a) Last name(s)
- b) first name(s)
- c) date of birth
- d) address (street, no., ZIP code, city)

Verification:

To verify the identity of our customers, a government-issued document containing photographic evidence is required. Acceptable documents for this purpose include but are not limited to:

- Passport

- Identity card
- Travel document
- Other documents as designated by the Government

Proof of Address Verification:

For establishing a customer's address, Udwin B.V. accepts the following:

- Utility bill for a service installed at the residence issued within the last 3 months
- Correspondence or any other document from a central or local government authority, department, or agency dated within the last 3 months
- A currently valid lease agreement

Key requirements for these documents are:

- The document must be valid and unexpired
- They should be clear, legible, and of high quality
- Mobile phone bills are not acceptable

The Company retains the right to close an account if verification processes reveal that any provided information is false or misleading. This applies to documents found to be fraudulent, tampered with, or acquired through unauthorized means. Additionally, all submitted documents must adhere to internationally recognized standards. Should a customer fail to provide the required documentation or submit documents that do not meet the necessary criteria, the Company may impose account restrictions until compliant documentation is provided.

Restrictions:

For the integrity of our platform and to ensure regulatory compliance, the following restrictions apply:

- Individuals below the age of 18 are prohibited from registering on the site
- Persons identified as Politically Exposed Persons (PEP), under Sanctions, or listed in specific blacklists, including but not limited to : the Consolidated United Nations Security Council Sanctions List, Consolidated list of persons, groups and entities subject to EU financial sanctions, Office of Foreign Assets Control Sanctions List, Her Majesty's Treasury Sanctions List, the Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29), the Ministerial Regulation "Libya" (N.G. 2015, 28), the Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27);, the Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30), and the Ministerial Regulation "Yemen" (N.G. 2015, 65) are barred from accessing our platform
- Existing customers with current exclusions on the site are restricted
- Any individuals displaying signs of fraudulent activities or associated red flags

Threshold Approach

The Company may apply CDD measures in relation to any transaction that amounts to EUR 2000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked, engage in occasional transactions exceeding this threshold, raise suspicions of money laundering or terrorist financing, or if the casino has doubts about the accuracy or completeness of previously collected customer identification information. If the EUR 2000 threshold is met and CDD is incomplete, the customer will be prevented from depositing or withdrawing funds. If the customer does not provide the required documentation when needed, the account will be closed after 30 days, and a report of unusual activity will be filed if there is a reasonable suspicion.

“Transaction” consists of the wagering of a stake, including:

- the deposit of funds required to take part in remote gambling
- the collection of winnings, including
 - the withdrawal of funds deposited to take part in remote gambling or
 - winnings arising from the staking of such funds

The transactions are considered linked if they are part of the overall activity undertaken by a customer during a single period of being logged on to the operator's gambling facilities. However, this example is not exhaustive, and the Company considers other circumstances in which transactions are linked using a risk-based approach.

Consideration will need to be given as to whether there are other circumstances in which transactions are linked, such as, whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions in order to circumvent the C/EDD requirements.

For the purpose of the CDD triggered by the threshold, the Company applies verification using risk-based approach.

Ongoing Monitoring

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining fresh identification when existing documents have expired. (This can be done on a risk-sensitive basis.)

- Questioning the data and information the Company have have whenever inconsistencies are noticed.
- General review and update from time to time, on a risk sensitive basis.
- Checking if transactions match with the documents and information available at the Company about the customer and the origin, customer's assets
- Updating the respective documents, data, or information at appropriate intervals.

To keep all the customers information up to date, the Company apply CDD procedure every 6 months from the date of the successful complete verification of each customer and on a risk-sensitive basis.

Enhanced Due Diligence (EDD):

The Company applies enhanced customer due diligence measures (hereinafter – EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

EDD is applied in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company as one where there is a high risk of money laundering or terrorist financing;
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information and the Company proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,
- if the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer makes the wagers,

- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) only with the consent of the Compliance Officer.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD, comprising of (depending on the case):

- undertaking Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed)
 - sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter)
 - sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent)
 - inheritance (Certified copy of will including the value of heritage)
 - sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor).
- Establishing the source of the customer's funds to be satisfied that they do not constitute the proceeds from crime.
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements.
- Undertaking increased continuous monitoring of the business relationship.
- The suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

Undertaking the EDD on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back in each case to an account.

Meaning of Source of Funds

The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.

Meaning of Source of Wealth

The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired. This assessment identifies whether the customer's wealth originates from a single income stream, such as salaried employment, or multiple sources, such as business activities, investments, or inheritances. Greater attention is given to customers with multiple income streams or unverifiable sources of wealth, with the level of checks adjusted accordingly based on the nature and complexity of the information obtained.

Identifying Suspicious Behaviours

In the context of our Anti-Money Laundering (AML) efforts, recognizing potential suspicious behaviours or "red flags" is imperative. It's worth noting that the presence of such indicators does not directly translate to illicit activity; rather, they are prompts for further investigation. Should these investigations not yield satisfactory explanations, our procedure necessitates the submission of an internal report to the Compliance Officer.

The potential suspicious behaviours to be vigilant for include, but are not limited to:

- Customer Cooperation: Reluctance or consistent avoidance in providing necessary details during Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) processes.
- Multiple Account Activities: Attempts by a customer to create multiple accounts on the platform.
- Disproportionate Transactions: Instances where the customer deposits large amounts, places minimal or no bets, and then requests significant withdrawals, seemingly disregarding any winnings or losses.
- Inconsistent Gaming Patterns: Marked alterations in a customer's gaming behaviours, such as executing transactions vastly differing from their usual patterns.
- Inter-Account Transfers: Inquiries or attempts to move funds across different accounts within the same gaming network without clear justification.
- Discrepant Wealth Display: Transaction amounts that starkly contrast with the known financial capacity, wealth, or income of the customer.
- Third-party Transactions: Requests or attempts to transfer funds to accounts registered under different names or to receive withdrawals to previously unused accounts.

- Multiple Payment Methods: Opening an account and associating it with several distinct payment cards or methods, followed by frequent transfers amongst them.
- Indifferent Losses: Consistently depositing and subsequently losing significant sums, in a manner that suggests indifference to the losses.

The recognition of any such behaviour warrants immediate attention, with the subsequent steps determined based on the specific context and any additional information gathered.

6. Player Account and Fund Management

Procedure for Account Closure

There are numerous reasons for why the Company will want to close a customer's account:

- Fraud
- Cheating
- Bonus Abuse
- Allowing a third person to use their account
- Under-aged gambling
- Problem gambler
- Being abusive to staff
- Commercial concerns
- CDD failure
- Terms and Conditions breach

The concern of this Company Policy is the reason that there is a suspicion or knowledge that the customer is involved in ML/FT.

By law the Company must end the business relationship with the customer unless we have obtained appropriate consent for it to continue and even then it is precautionary to close the account.

Due to the laws on Tipping Off the Company cannot inform the customer that we have concerns regarding ML/FT, thus account closure must be done sensitively.

The Compliance Officer will need to consider whether if an SAR was submitted as part of the concern about the player's behaviour whether appropriate consent should have been requested.

Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached, and is accordingly required to cease transactions and terminate the business relationship with the customer.

Player Account Balance

Each player has a wallet with funds from which bets are deducted, and winnings added. All funds deposited by the player or owed by the Company are credited to the player's corresponding account. The player can top up the funds in his account by depositing through the cashier on the site and then use these funds to place bets. Bets are deducted from his account balance, and winnings are added to the account balance.

The player can withdraw withdrawals of available funds in the player's balance. The Company do not offer credit to players. A player may not transfer funds to another player.

Payment Methods

Payments shall only be accepted and made from accounts held with licenced financial institutions or through licenced payment providers.

No cash deposits/withdrawals will be effected between the Company and its players.

Player Deposits

After registering, a player may then deposit funds into their account through the cashier on the site.

In order to facilitate these deposits, the company has integrated with a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself.

The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the player's balance.

Player Withdrawals

A player with an available balance will be able to request a withdrawal of the funds via the cashier on the site.

The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

Withdrawal Payouts

In remitting funds to the player, we will, where possible, remit the funds directly into the account where the funds originated from.

Provided that where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

Verification and Conditions

The Company enforces measures to ensure that all deposits and withdrawals align with the customer's registered account information.

Verification of Cardholder's Name: The name on the payment method, whether a card or bank account, must match the name registered on the player's account. Any discrepancies will trigger a review process, during which the Company may request additional documentation or suspend transactions until verification is complete.

Handling of Inconsistencies: If inconsistencies are identified between the player's account details and the payment method, the Company reserves the right to conduct further checks. This ensures the legitimacy of the payment method and its proper association with the player.

Minimum Wagering Activity: To prevent the abuse of bonuses or promotional offers, the Company may impose minimum wagering activity requirements before processing withdrawals.

7. Suspicious and Unusual Activity Reporting & Compliance Management

At Udwin B.V., every employee must report to the Compliance Officer if there is suspicion or knowledge of money laundering, funding of terrorism or if the funds being used on the Company's website are the proceeds of criminal activity.

The Compliance Officer will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a SAR should be submitted to the Financial Intelligence Unit (hereinafter – FIU).

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the FIU.

The Compliance Officer assess all the circumstances and the customer or others more questions if needed. The choice depends on what is already known about the customer and the transaction and how easy it is to make further enquiries.

The Company is required not only to report suspicious transactions but also to report unusual transactions. Such transactions may be recognized using objective or subjective indicators provided by the FIU Curaçao and must be reported upon identification.

Role of the Money Laundering Reporting Officer (MLRO)

The MLRO serves as the linchpin in our commitment to maintain a robust anti-money laundering (AML) framework. Appointed by the senior management, the MLRO holds the critical responsibility to:

- Receive and review all internal suspicious activity reports.
- Decide upon the need for further investigation or reporting to external bodies.
- Serve as the primary liaison with the Financial Intelligence Unit (FIU) and other regulatory authorities.
- Ensure continuous training and awareness for staff on AML procedures and standards.
- Regularly review and update AML policies and procedures in line with evolving regulatory expectations.

Red Flags Indicators

Red flags are not intended to automatically result in filing a SAR with the FIU, however are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be made to the Compliance Officer.

The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant, 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 enquires about the possibility of moving funds between accounts belonging to the same gaming group.

- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he never deposited with.
- Customer opening an account and registering several different cards and making transfers between them,
- Customer depositing large sums, then places minimal bets, then withdrawing all their funds,
- Customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

Internal Suspicious Activity Reporting

All employees hold a fundamental responsibility to monitor and report any suspicious customer activity. Upon observing questionable behaviour or transactions, employees must immediately alert the MLRO using the stipulated Internal Suspicious Activity Report Form. This obligation stands even if there's disagreement from higher-ups. The Internal SAR encompasses:

- Customer details
- Staff statements regarding their suspicion
- All associated documentation

Upon receipt, the MLRO undertakes the following:

- Acknowledges the report, proceeding with a thorough investigation if needed.
- Assesses all data, determining whether law enforcement notification is essential.
- If a concern persists, a SAR is submitted to the FIU.
- Senior management remains informed of all decisions and subsequent actions.

External Reporting to FIU

Post an internal review, the MLRO evaluates whether the FIU should receive a SAR. This decision considers the nature and scope of suspicious activity, focusing on patterns hinting at money laundering or fraud, like recurring suspicious behavior, multiple chargebacks, or identity theft instances. Before deciding on the SAR's submission, the MLRO must answer key questions pertaining to the nature, origin, and potential ramifications of the suspicious activity.

Reporting Procedure

The Company is obliged to submit a suspicious activity report to the FIU, through the user interfaces on the FIU's website or by mail (if possible), without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

When the Company decides whether it is necessary to submit SAR, it takes the following factors into account, including but not limited to:

- the purpose and nature of the transaction,
- peculiarities in the customer,
- the financial and business background of the customer,
- the origin of the assets contributed or to be contributed.

The Company doesn't execute suspicious transactions, except in cases where it cannot postpone the transaction or if the postponement could hinder the prosecution of an alleged criminal offense. In this case, the Company submits SAR immediately.

The same reporting obligation applies to any unusual transaction that meets the objective or subjective indicators defined.

Tipping-off Policy

Maintaining the confidentiality of any SAR's submission or even its potential submission is paramount. Tipping-off, or revealing that a SAR is under consideration or has been submitted, can critically jeopardize investigations. Thus, it's forbidden to:

- Indicate to customers that transactions are delayed due to pending reports or that an external investigation might be underway.
- Reveal any ongoing law enforcement investigations to customers.

Udwin B.V. remains steadfast in ensuring a compliant and transparent operational environment, prioritizing both internal and external reporting mechanisms.

8. Record Keeping

At Udwin B.V., ensuring that accurate and comprehensive records are kept is paramount to both our regulatory obligations and our commitment to integrity. All pertinent documentation and customer information are securely stored for a period of five years. This duration has been chosen in accordance with regulatory requirements, ensuring that, should the need arise, a comprehensive audit trail is available for any given transaction or interaction.

In safeguarding these records, we strictly adhere to data protection regulations. All stored data is encrypted and protected against unauthorized access, loss, or damage. Access to this data is restricted to authorized personnel only. Our IT infrastructure, including our backup systems, are routinely audited to ensure the integrity and security of all stored data.

9. Training and Awareness

At Udwin B.V., we believe that our employees are the first line of defence against money laundering and terrorist financing. As such, we have established a rigorous training program designed to equip our team with the necessary knowledge to recognize and respond to suspicious activities.

All new employees undergo a comprehensive induction training that covers the fundamentals of AML and CTF (Counter-Terrorist Financing). Additionally, we conduct refresher courses annually, ensuring that our staff stays updated on the latest regulations, trends, and best practices in the industry.

To complement formal training, ongoing awareness initiatives are in place. These include monthly newsletters, regular workshops, and access to updated resources on our internal portal. By fostering a culture of vigilance and continuous learning, we aim to uphold the highest standards of regulatory compliance and ethical conduct.

Training Methodology:

- **Content Creation:** Our training modules are crafted using our established and approved policies, collated into accessible documents and engaging presentations.
- **Delivery Mechanism:** Existing staff, from management to junior levels, will receive training either in a structured classroom setting or via online platforms.
- **Induction Program:** All new hires will undergo a comprehensive AML induction training to ensure immediate familiarity with our standards.
- **Assessment and Feedback:** Post-training, employees will take a questionnaire to gauge comprehension. Areas of ambiguity or frequent mistakes will prompt specialized retraining sessions.

- Continuous Learning: Periodic refresher courses will be offered, incorporating any new updates or addressing areas of concern from previous sessions.
- Policy Updates: Any changes to our AML policies will be promptly communicated through group emails, ad-hoc sessions, and subsequently integrated into regular training materials.

Core Training Focus Areas:

- Understanding of all relevant laws and regulations.
- Clarity on the company's stance, policies, and procedures against money laundering and terrorist financing.
- Emphasis on individual responsibilities, both under the law and as per company procedures.
- Recognizing, handling, and reporting suspicious activities.
- Insight into current trends, techniques, and methodologies employed in money laundering and terrorist financing.
- Awareness of inherent risks faced by the company.
- Ensuring compliance with data protection norms.

Specialized Training Sessions:

- As part of our continuous commitment, specialized training sessions will delve deeper into areas like fraud prevention and detection, tailored to the specific roles and responsibilities of the attendees.
- Regular updates and additions will keep the content fresh and aligned with the latest industry standards and threats.

Recordkeeping:

Our Money Laundering Officer is responsible for meticulously documenting all training initiatives. This includes tracking attendees, content, trainers, and scheduling future training sessions. Whenever there's a shift in our policies or the legal landscape, we guarantee prompt and thorough training to keep our team prepared and informed.

10. Ongoing Monitoring

Monitoring our business relationships is not a one-off task but an ongoing commitment. Udwin B.V. has invested in cutting-edge systems designed to continuously oversee all transactions and customer interactions. These systems are equipped with algorithms that detect unusual patterns or anomalies which may suggest suspicious activity.

Beyond automated monitoring, we have a dedicated compliance team that conducts periodic manual reviews of high-risk accounts and transactions. This multi-pronged approach ensures that potential issues are identified promptly and dealt with appropriately.

Risk assessments, methodologies, and other related procedures are reviewed bi-annually. These reviews take into consideration changes in the regulatory environment, emerging trends in money laundering and terrorist financing, and feedback from our staff and external auditors. Any identified gaps or areas of improvement are addressed immediately, ensuring that our monitoring mechanisms remain robust and effective.

11. Review and Audit

At Udwin B.V., we understand the dynamic nature of the anti-money laundering landscape and the importance of adapting our practices to remain compliant and effective. Therefore, our AML policy is subject to regular review, at least annually, and more frequently if there are significant changes in our operating environment or regulatory landscape.

In addition to our internal reviews, we engage reputable third-party auditors to perform comprehensive evaluations of our AML controls. These external audits, conducted if necessary, ensure that our practices not only align with regulatory requirements but also adhere to international best practices. The outcomes of these audits are communicated to our senior management and relevant adjustments are made promptly.

12. Policy Approval and Implementation

This AML policy has been reviewed and approved by Udwin B.V.'s senior management team, affirming our collective commitment to preventing money laundering and terrorist financing activities through our platforms.

Once approved, the policy is disseminated to all departments and staff members via our internal communication channels, including email, intranet, and departmental meetings. To ensure complete comprehension and adherence, training sessions are conducted for all relevant personnel, and resources are made available for ongoing support. We encourage open communication and feedback, enabling continuous refinement of our policy and practices.

13. Sanctions, PEPs, and Adverse Media Screening

The Company uses KYC software tool to check all new customers at the registration stage against the PEP and Sanctions databases. In addition, if a customer's total deposits or transactions exceed €2,000 within any 30-day period, a PEP check is triggered immediately.

Furthermore, the Company also regularly checks the whole customer database every six months to ensure existing customers have not changed status.

Any new or existing customer found on the Sanctions database, or a PEP or relative of such will have their account rejected or closed.

In case of identifying a PEP, responsible staff will send a report to Compliance Officer who in turn will send a report to the senior management. The Compliance Officer will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the Compliance Officer will reject registration or close the account and informed the senior management about the decision taken.

Approved:

Date: 23.05.2025

Xecutive Corporate Management B.V.

APPENDIX 1
**«COUNTRIES AND TERRITORIES EXCLUDED
FOR REGISTRATION»**

In alignment with our Anti-Money Laundering (AML) policy and in compliance with international regulatory requirements, certain countries have been identified as posing heightened risks. Consequently, we have placed restrictions on registrations from these countries. Below is a list of countries from which registration is prohibited. This list is not exhaustive and might also include other countries that may have been banned due to various reasons. It is also maintained to ensure the integrity and security of our operations, and is updated as necessary based on our ongoing risk assessments and external advisories.

1. Afghanistan
2. American Samoa
3. Aruba
4. Australia
5. Belgium
6. Belize
7. Bonaire
8. Bosnia and Herzegovina
9. Burma/Myanmar
10. Burundi
11. Central African Republic
12. Curaçao
13. Democratic People's Republic of Korea
14. Democratic Republic of the Congo
15. Denmark
16. Egypt
17. Eritrea
18. Estonia
19. France
20. French Guyana
21. Greece
22. Greenland
23. Guadeloupe
24. Guam
25. Holy See (Vatican City)
26. Iran (human rights)
27. Iraq
28. ISIL and Al-Qaida
29. Italy
30. Ivory Coast
31. Kuwait
32. Lebanon
33. Libya
34. Lithuania
35. Malaysia
36. Maldives

- 37. Mali
- 38. Marshall Islands
- 39. Martinique (.FR)
- 40. Netherlands
- 41. Occupied Palestinian Territory
- 42. Puerto Rico
- 43. Qatar
- 44. Somalia
- 45. South Sudan
- 46. Sudan
- 47. Syria
- 48. USA
- 49. US Minor Outlying Islands
- 50. US Virgin Islands
- 51. Yemen
- 52. Zimbabwe