

AML/CFT/CFP policy of FarUp Entertainment N.V.

Introduction

FarUp Entertainment N.V., a company registered in accordance with the laws of Curaçao under Registered under no.163294 with registered office at Scharlooweg 39, Willemstad, Curaçao. FarUp Entertainment N.V. is licensed to conduct online gaming operations by the Government of Curacao under license OGL/2024/361/0119

Objective of the AML/CFT/CFP Policy

We seek to offer the highest security to all our client's customers by having adequate steps and means of player verification to ensure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering. We also take into account that depending on the nationality and origin, the way of deposit and way of withdrawing will require different safety measurements.

- EU : "Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering
- EU : "Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering
- Article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);EE: "Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash
- FATF Recommendations (Financial Action Task Force, European Inter-governmental body)AML policy changes and implementation requirements

Each major change of FarUp Entertainment N.V.'s AML policy is subject to approval by the general management of FarUp Entertainment NV. and the Anti money laundering MLRO/Compliance officer.

Definition of Money Laundering

Money Laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or companies action;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;
- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and concealing the commission of any of the actions referred to in points before.
- Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.
- Organization of the AML for FarUp Entertainment N.V.
- In accordance with the AML legislation, FarUp Entertainment N.V.. has appointed the "highest level" for the prevention of ML: The full management of FarUp Entertainment N.V.. are in charge.
- Furthermore, an MLRO (Money Laundering Reporting Officer) is in charge of the enforcement of the AML policy and procedures within the System.
- The MLRO is placed under the direct responsibility of the general management

Definition of terrorist financing

Terrorist financing is defined and understood by the business as:

- Provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used), in full or in part, to carry out acts that are associated with the support of terrorism or terrorist organizations, whether to further their causes or to commit acts of terrorism.

Definition of proliferation of weapons

Proliferation of weapons is understood by the business as

- Provision of funds 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.

Procedure

The AML rules and guidance, including KYC standards will be translated into operational guidance or procedures that are available on the Intranet site of FarUp Entertainment N.V..

Enterprise-wide risk assessment is part of its risk-based approach, FarUp Entertainment N.V. has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to FarUp Entertainment N.V.. and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks. The identification of AML risk categories is based on FarUp Entertainment N.V.. understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it. The EWRA is yearly reassessed.

KYC policy

The objective of our KYC process is to comply with regulatory requirements, prevent the casino from being used by criminal elements for money laundering activities, other fraudulent activity that may result in financial losses to the casino and with the general objective to ensure a safe and responsible gaming environment for our players.

KYC descriptions

- **Simplified due diligence**
This is obtaining personal details from the customer before allowing him to complete the registration process.
- **PEP / Sanctions screening**
The Company must carry out PEP and sanctions checks at the first possible opportunity after registration and at no point further than first deposit. PEP checks are carried out electronically through our service provider Checkin.com who uses DowJones registry.
- **Age verification**
We will only allow use of the website by persons who are at least 21 years of age (or at the age limit for gambling set by the laws of respective country of residence). The user is not allowed to enter a date that would contradict this.
- **Electronic Verification Method – using Bank ID**

The use of an electronic Bank ID (commonly utilised in Scandinavian countries) at the registration phase equates to a strong identification method, which is considered equivalent to a face-to-face registration. Upon conducting a registration using this channel, the company will retain and store all details from the bank ID, the exact details of such information can be extracted.

- **Customer due diligence**

A player shall be named as verified in accordance with customer due diligence when player has provided supporting documents that verify their Identity and residence

- **Additional due diligence**

A player has to verify they are the beneficial owner of the used payment method, or they have to provide additional information related to them such as source of wealth information and corroborating documentation together with online searches and negative string searches with players personal details.

- **Enhanced due diligence**

A player has undergone initial customer due diligence by providing ID, Proof of address, Payment methods used. In this step player is requested to provide source of wealth or source of funds, which is done by requesting source of wealth or funds that verify player is not funding their gambling with illegitimate sources.

Verification steps

- **Simplified due diligence**

Upon registration the following data as a minimum is collected from the user

1. Full name
2. Date of birth
3. Address details
4. Phone number
5. E-mail address

In addition to the above mandatory registration fields the player also needs to validate their registered mobile number which is done via an SMS validation service through our service provider regularly.

- **PEP / Sanctions screening**

As part of our basic due diligence step, all players are in the signup process also checked against PEP and Sanctions lists. Any player who gets a positive match through PEP and Sanctions checks will be extracted from a report where the player and his activity will be

thoroughly investigated. If investigation concludes that it is indeed a real PEP and/or Sanction match, then the account should be permanently closed and any remaining balance will be paid out after the completion of a full KYC and risk assessment. Screenings are carried out using following providers

1. DowJones via our solution provider Checkin.com
2. <https://www.trapets.com> via Zimpler

In addition to the above we are also regularly monitoring for updates on:
<http://mot.cw/web/motweb/motweb.nsf/web/home?opendocument>

- **Customer due diligence**

The customer will undergo due diligence if any of the following criterias are met:

1. The customer requests or attempts to change registered name and/or address details
2. The player is deemed as heightened risk from FRAUD, AML, Bonus abuse or any other perspective
3. The player has reached 2,000 EUR or more in deposits or withdrawals
4. Multiple linked accounts have been identified to the player

If any of the above is triggered on an account, then no further withdrawals will be processed until the verification process has been completed. The regular due diligence process would involve the player and his activity being reviewed and categorized as low, medium or high risk. Depending on the outcome of such a review the level of KYC documentation requirement may vary. The level of KYC documents required from a player is determined by using a risk-based approach however at this point the minimum would always be to verify the Identity and address details with valid and legible documents. Certain exceptions to this process may apply to players deemed as low risk who have been onboarded and verified with "Electronic Verification Method – using Bank ID. If player reaches the threshold of 2000 EUR or total deposits or withdrawals, and they haven't completed the customer due diligence their account will be suspended from making further transactions or wagering. If the player has not provided the required due diligence within 30 days, the business relationship is terminated, and player loses the ability to use their account entirely.

- **Withdrawal KYC Requirements before 2,000 EUR in deposits OR withdrawals**

Before 2K threshold: Closed loop withdrawals can be approved without KYC if:

1. Before 4K threshold: Closed loop withdrawals can be approved without KYC if:
2. A Basic risk assessment has been concluded of account activity and the player has been deemed as low risk from an AML, Fraud and Bonus abuse perspective.
3. A detailed risk assessment has been concluded and recorded in account notes and the player has been deemed as low risk from an AML, Fraud and Bonus abuse perspective.
4. Player is not funding his account using cash vouchers such as Paysafe, and then withdrawing back via bank.
5. No inconsistencies have been identified in registered details or IP-address.

6. A detailed risk assessment has been carried out and been recorded on account where risk has been as LOW from a basic Fraud, AML and bonus abuse perspective.
7. No linked accounts have been identified to the player
8. Not more than 2 different payment methods have been used to fund his account.
9. There are no direct and significant financial risk associated with majority of deposits on account (i.e. N3DS, unsettled deposits)

- **Additional due diligence**

The player will undergo additional due diligence if any of the following criteria's are met:

1. The player has net deposits of more than 10,000 euro in less than seven days.
2. The player has net deposits of more than 20,000 euro in less than 30 days.
3. The player has deposited substantial amounts in a short period of time or is considered higher than low risk for any other reason.

As a general guideline if any of the above criteria are met then we will need to ensure initiating a process to obtain ID, Proof of address, Payment method and Source of income information on file. In addition to this all the players activity will be thoroughly investigated and background checks will be carried out via online searches and negative news string searches.

- **Negative news string searches:**

"NAME OF PLAYER OR COMPANY" "fraud" OR "abuse*" OR "laundering" OR "terrorism" OR "bribe" OR "corruption" OR "embezzlement" OR "organized crime" OR "traffic" OR "scam" OR "smuggle" OR "theft" OR "tax evasion*" OR "insider trading" OR "misappropriate" OR "forgery" OR "counterfeit" OR "liquidation" OR "espionage" OR "cybercrime" OR "hostile" OR "offshore" OR "regulatory" OR "freeze" OR "injunction" OR "watchdog" OR "sanction" OR "political" OR "Romance scam"

- **Enhanced due diligence**

The player will undergo enhanced due diligence if any of the criteria's are met:

1. The player has received a positive match in our PEP and Sanctions screening which is deemed as accurate.
2. Player deposits 5,000 EUR with anonymous payment methods in 24 hours
3. Player deposits 10,000 EUR with anonymous payment methods in 1 month
4. Player deposits 20,000 EUR with anonymous payment methods in 12 months
5. Player is risk rated as high risk due to their activity

Certain exceptions from the above EDD process can be made in cases where player is deemed as low risk, we hold standard due diligence KYC on a player, a proper risk assessment has been done and it is obvious that the high value within a short period of time as an example is a result of a player "recycling"(=re-depositing) previous winnings made on the same account.

If not already carried out in earlier checks which normally would be the case, then we would at this stage also manually do checks to ensure that player is not “A family member of a person performing prominent public functions” or “A close associate of a person performing prominent public function”.

Customer business relationship is terminated, if EED has not been completed within 30 days and if player raises concerns from ML/TF/FP perspective, they are raised to company MLRO for review through internal suspicious transactions reports or reviewed directly by MLRO if customer has been identified by ML/TF/FP risk by AML policies and procedures. MLRO will then make a decision whether to raise the player externally to FIU.

- **Ongoing due diligence**

It is understood that active player accounts will need to be reviewed on an ongoing basis and on a risk-based approach to ensure that the documentation and player profile data held on file is reflective of the present player circumstances.

Accepted documentation

The business accepts below listed documents eligible to be used in CDD for example

- **ID and address documentation**

The business accepts below listed documents eligible to be used in CDD as an example. Documents required to verify Identity cannot be expired and documents required to verify address cannot be older than 6 months.

1. National ID card
2. Driver license
3. Passport
4. Proof of address:
5. Any document provided to verify the users residential details should have been issued in the last three months, example of acceptable documentation:
6. Utility bill
7. Internet/Mobile bill
8. Rental invoice(together with additional match via Online directory)
9. Any government issued document (examples: tax bill, proof of residency document)
10. Copy of bank statement

- **Payment method**

Depending on the payment method used on the account this type of documentation may vary but in general below listed documentation are standard that would be requested and accepted

1. Photocopy of credit card (six first digits and last four digits should only be visible, rest of digits should be blanked out)
2. Screenshot of any e-wallet used

- **Electronic Verification Method – using Bank ID**

The use of an electronic Bank ID (commonly used in Scandinavian countries) at the registration stage equates to a strong identification method, which is considered equivalent to a face-to-face registration. Through this verification we can successfully and securely verify Identity, address and bank account used. Below you will find a list of the data verifiable via the Bank ID authentication: Low risk users onboarded via this channel may be exempt from standard due diligence process requirements which would remove the need to provide copies of physical Identity, Address and Payment related documents. It is clear and understood that copies of physical documentation still may be required for accounts deemed as anything other than low risk or if players have triggered an enhanced due diligence process.

- **Source of wealth information**

The objective of the Source of funds is for us to gain an overview of the players sources of income and to verify that they are aligned with the customers monetary activity with our casino. The player will be asked to answer the following questions:

1. What is your employment status?
2. What is your primary occupation?
3. In which bracket does your annual income fall? EURO: 13000 - 30000, 30001 - 45000, 45001 - 60000, 60001 - 80000, 80001 - 100 000, 100 000 - 150 000 and 150 000+
4. Do you have any other sources of income?
5. Do you own your residential property?
6. The player will also be asked to upload supporting documents in form of:
7. Salary/Wage

- **Source of wealth and source of funds**

Player needs to provide supporting documentation that verifies how they are verifying their gambling. Business accepts the following documentation as SOW/SOF.

1. Employment, then we would need a copy of your payslip and/or employment contract
2. Savings, then we would need a copy of a bank statement showing sufficient balance and affordability (proportionate to your gaming spend)
3. Inheritance, then we would need a copy of Inheritance Confirmations/Wills
4. Gift, then we would need a Deed of Donation

5. Statement showing redundancy settlement or bank statement where incoming retirement funds are visible.
6. Sale of a property, then we need proof of sale and evidence of funds being received from that sale.
7. Sale of an asset, then we need proof of sale (such as an invoice or a signed contract) and evidence of funds being received from that sale.
8. Sale of shares, then we need proof of sale and evidence of funds being received from that sale.
9. We would need to see evidence that player is the owner of the company, and evidence of dividends/profits transferred to his personal account which was used to deposit with us
10. Other (Player need to specify)

Customers account suspension

Player's account can be suspended weather due to pending due diligence documents or they are raining concern of fraud or abuse. For example, gaming account can be suspended by following ways.

1. Suspension of withdrawals
2. Suspension of wagering
3. Suspension of deposits
4. Blocking of specific payment method

Customer business relationship termination

If player does not provide the requested due diligence within the 30 days from the request date or players presented risk exceeds the business risk appetite customer business relationship will be terminated. Business deems blocking players logins, deposits, withdrawals and gameplay as business relationship termination as players overall access to the account is halted.

Country & Geographical risk:

Some countries pose naturally a higher money laundering and terrorist financing risk than others. This is something we have taken into consideration when excluding players from high-risk jurisdictions. All restricted countries from which we do not allow players from are detailed in our terms and conditions §3.2, this list of countries is assessed on a regular basis.

To mitigate this risk, the country's list of the registration process is restricted to make available only those countries that are allowed to register an account. Other restricted or prohibited countries are removed from the registration process.

- All countries accepted have been risk assessed and any jurisdictions with a heightened risk are screened and going through more rigorous due diligence checks.
- Ongoing monitoring of transaction monitoring and player activity
- The risk and fraud team uses both external and internal fraud prevention solutions which combine real time monitoring with aggregated reports for manual review.
- Our internal risk and fraud management system provided by our platform provider Pragmatic solution has 20+ different rules to highlight suspicious activity on player accounts in real time.
- Besides from above we also have via our platform provider and analytic Business intelligence tool "BI+" multiple live reports and aggregated retrospective reports to highlight gaming activity, monetary activity and login activity.
- As an extra layer to the above more traditional fraud prevention systems we also have fraud prevention rules setup with our payment gateway provider PaymentIQ to highlight and reject in real time any suspicious transactions.
- In addition to the above we have also signed an agreement with an external solution provided by FLOWS, this is a tool that allows us to further screen, customize rules and highlight suspicious activity from all new registrations, transactions, and logins from players with our casino. The system is highly customizable and allows us to create our own fraud rules and risk scoring to keep up with any present fraud trend.

Transactional monitoring: Deposits & withdrawals

The Risk & Fraud team and any other trained staff reviews all incoming deposits and withdrawals seven days a week through alerts and daily reports. The monitoring of card deposits and other payment methods with direct financial risk along with large deposits are given preference and extra attention in these checks.

- **Deposit patterns & withdrawal patterns**

The selection of transactions to investigate is done using a risk-based approach where things such as deposit value, country of deposit, country of payment method, KYC level, and deposit pattern is taken into account. Some of the deposit patterns that are checked for:

1. Velocity deposits - Multiple deposits carried out on a single account within a very short time frame
2. Structuring - Instead of making a single deposit of a substantial amount (example 2,000 EUR) the player is depositing ten transactions of 200 EUR in hope that the player won't trigger any single deposit alert and raise suspicion
3. High to low failures: The player makes multiple deposit attempts where he after each failure tries lower and lower amounts.
4. Multiple payment methods - The player is successfully or attempting to make deposits with multiple payment methods

5. Geo data discrepancies - The IP and/or the registered country of the player do not match with each other, or the issuing country of the payment method used.
6. Positive balance top-up - The player is carrying out additional deposits despite having a positive balance
7. Non-closed loop withdrawals - The player attempts to withdraw to a payment method different than that used to fund his gaming account.
8. Substantial deposit/withdrawal amounts - The player has deposited or is attempting to withdraw a substantial amount from his gaming account.
9. "Anonymous" payment method - Substantial deposit with the use of vouchers, prepaid cards, wallets and/or cryptocurrency.
10. Third party usage - Player have used what appears to be a payment method belonging to someone else.

Reports

The below reports are reviewed minimum once per day. All Risk & Fraud staff have been trained and have been provided documented guidance on how to identify inconsistencies, how to identify suspicious activity and how to select accounts to review and how to subsequently carry out a risk assessment of such accounts. Selection of accounts for review in these reports can be based on but is not limited to;

1. Existing fraud/bonus abuse trends,
2. Deposit related numbers
3. First deposit amount
4. Last deposit amount
5. Total deposit value
6. Deposit count
7. Suspicious registration details
8. Age
9. High risk country
10. High deposits/withdrawals
11. High bonus costs
12. Affiliate ID
13. Deposit vs Wager amount
14. high Win ratio and/or high loss ratio.

- **Registration report (Today & Yesterday)**

This report's purpose is to screen all new registrations and carry out risk assessments and as soon as possible take appropriate actions on any account identified as high risk in order to prevent money laundering, fraudulent behavior and subsequent financial losses.

- **First depositors (Today & Yesterday)**

This report's purpose is to screen all players who might have registered a while ago, but never made any deposits until the time of appearing in this report.

- **High withdrawal/deposit report (Today & Yesterday)**

The purpose of this report is to ensure ongoing monitoring and continuous risk assessments of players with substantial deposit or withdrawal amounts within the last 24 hours.

- **Top Winner/losers (Today & Yesterday)**

This report is reviewed to quickly identify large winners and losers, large winnings or losses could be a result of fraudulent funding of account, faulty games, opposite betting etc.

- **High depositor reports**

The purpose of this report is to ensure ongoing monitoring and continuous risk assessments of players with substantial total deposits amounts (2,000 in last 24 hours, 5,000 EUR in last 7 days, 10,000 EUR deposits last 30 days or 50,000 EUR life time deposits)

- **Bonus report**

Report used to identify players with high bonus costs to investigate for potential bonus abuse

- **Manual credit reports**

Report is used to monitor all internal credits done by backoffice users on player accounts to detect fraudulent or incorrect credits

- **Positive balances**

Report is used to monitor all accounts which have been inactive for more than 90 days with a substantial amount left in the gaming account.

Alerts

We have in our platform configured a set of 50+ rules that scan activity by players in real-time and highlight any positive match so that a Risk & Fraud agent or trained staff can carry out a risk assessment of the account.

The rules in place can be automatically configured to take one of the following actions:

1. Highlight a positive match for review but take no other action.
2. Highlight a positive match for review and restrict further deposits.
3. Highlight a positive match for review and restrict any further withdrawals.
4. Highlight a positive match for review and suspend account
5. Or any combination of the above

List of some of the real time alerts in place

Real-time alerts via Flows
Rule 1: 10k in 7 days
Rule 2: 1K in losses last 24H without RG/AML tags
Rule 3: 5k in 24 hours
Rule 4: FTD with phonecode mismatch user
Rule 5: Demographic age rule
Rule 6: IP_CHANGE 3 different countries in the last 7 days
Rule 7: 30K threshold- No KYC
Rule 8: 20K no KYC
Rule 9: 10K no KYC
Rule 9:10K no KYC
Rule 10:50k in 30 days
Rule 11: 20k in 30 days
Rule 12: 1kin 24hrs FTD 7 days
Rule 13: 1kin 24h 80%of LT
Rule 14: 5 failed in 90 min
Rule 15: 1K in 24 hours - NO KYC
Rule 16: 10 dep in 24h - min 300
Rule 17: Consistent IP/Country mismatch
Rule 18: New reg - IP/Country mismatch
Rule 19: FTD 500 EUR
Rule 20: No AFF 100 FTD
Rule 21: Deposit with balance over 1k
Rule 23: Player has SBA tag and has 2X deposit count
Rule 24: SOWREQ monitoring in 7 days
Rule 25: SOW dormant monitoring in 7 days
Rule 26: SOWREQ monitoring in 24 hours
Rule 27: SOW dormant monitoring in 24 hours
Rule 28: SOW monitoring last 30 days
Rule 29: SOWD monitoring last 30 days
Rule 30: Multiple CC attempts
Rule 31: Dutch Prefix Reg
Rule 31: False reg (Prefix/sign up IP check not passed)
Rule 32: Player active again (RG PUSH NOT ACT)
Rule 33:Player with SOWREQ closed account
Rule 34: Player with SOWQ-req closed account
Rule 35: Player with SOWD closed account
Rule 38: Crpyto FTD

Third party usage:

Third party usage” is the wording used to categorize deposits and withdrawals which originates from a payment method who is not owned by the registered player.

Whilst it's true that most third-party usage happens with the owner of the payment methods permission (ex. a Friend/Spouse borrowing the card to player) we do not allow this as with such usage there is a heightened risk of ML and Fraud which we take very seriously to prevent.

Any player identified using third party payment methods will be subject to an in-depth risk assessment where the account may get suspended and where the player is contacted and reminded about our terms and condition §11.3 and subject to KYC requests in accordance with our internal guidelines for third party usage. Any balance left in account is always used to reconcile the third party deposits to eliminate risks.

Game related risk

The company offers only casino products with game types such as slots and table games which in general is considered as lower risk as it involves playing against the house (the casino) and not against other players such as poker where a deliberate transfer of funds can occur between two players.

However, the company recognizes that games such as Roulette and Baccarat do carry a heightened risk for the sessions where you are betting together with other players such as live casino tables. The primary risk in these two game types are “Opposite Betting” whereas two or more players would bet on opposite outcomes and in that way ensuring that funds are transferred one way or another. A typical example of this on the roulette table would be if player A would bet on red and Player B. would bet on black. All new games added to our casino is risk assessed to make sure that monitoring is in place to detect any anomalies or suspicious activity on games classified as higher risk.

AML training

All employees of FarUp Entertainment. have received adequate training in AML to ensure that everyone has basic knowledge and understanding of what Money laundering and terrorist financing is, how an online casino can be used for such said activities and how to report any suspicious activity. More in depth training for all staff involved in Payments, Fraud, AML and Risk Management processes will be conducted on minimum an annual basis.

The training and awareness program is reflected by its usage:

- A more in-depth AML training program in accordance with the latest regulatory evolutions, for all staff involved with Payments, Fraud, AML and Risk Management processes.
- AML learning sessions for all new employees given within the first month of employment. The content of this training program has to be established in accordance with the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML-specialist working in FarUp Entertainment N.V. Risk, Fraud and AML team.

Reporting of suspicious transactions/activity

In its internal procedures, FarUp Entertainment N.V. describes it in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting. Reports of atypical transactions are analysed within the Risk & Fraud team in accordance with the precise methodology fully described in the internal procedures. Depending on the result of this examination and on the basis of the information gathered, the Risk and Fraud team will escalate the transaction by filing a Unusual Activity Report (UAR) to appointed compliance officer

- **Compliance officer**

1. will investigate and decide whether it is necessary or not to send a report to the FIU.
2. will decide whether or not it is necessary to terminate the business relations with the customer.
3. Where money has been received from a bank account, we will approach them with our concerns, or if it is a request for withdrawal, we will approach the bank that holds the account that would receive the funds. This enables us to ensure that we adhere to local Financial Regulations and that the correct authorities are informed.

Reporting of unusual transactions

According to National Ordinance customers who engage in financial transactions equal to or above 2500 EUR are obliged to be reported as unusual transactions to FIU. Compliance officer receives a report that highlights all deposits and withdrawals with equal amounts of 2500 EUR or higher in the past 24 hours. The report is then forwarded for external review to FIU.

Tipping off

- At no time should anyone inform the player that a suspicious transaction has been reported, if a transaction or player has been reported to the compliance officer then that report should not be disclosed to any other staff than to the compliance officer and senior management.
- At no time should anyone indicate to third parties that a particular transaction has been reported as suspicious or that information has been requested by the Police on a particular transaction whether such transaction was reported as a suspicious one.
- MLRO is aware that he may publish information relating with the suspicious transactions/data only to:
 1. The management board of BRAND and employees appointed by the management board.
 2. Financial Intelligence Unit of the relevant jurisdiction
 3. Investigation authorities during the criminal procedure.
 4. Court on the basis of the judgment or regulation.

Auditing

Internal audit regularly establishes missions and reports about AML activities.

Data security

All data given by any user/customer will be kept secure, will not be sold or given to anyone else. Only if forced by law, or to prevent money laundering data may be shared with the AML-authority of the affected state. FarUp Entertainment. will follow all guidelines and rules of the of the latest applicable GDPR Directive.

Record keeping

Records of data obtained for the purpose of identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying out of the transactions or the end of the business relationship. This data will be safely encrypted stored offline and online.

Full Name: Philip M. Humme

Signature: *Philip M. Humme*

Date: February 7, 2025

Position: Managing Director obo Allyant Group B.V.

Title	AML Policy Breckenridge
File name	FarUp_ent_-_AML_C...v1.0.docx__1_.pdf
Document ID	0797a585e9bb9c5a46b1fb9d51b354be9358392c
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History



SENT

03 / 07 / 2025

21:02:59 UTC

Sent for signature to Philip Humme
(philip.humme@allyant-group.com) from
gala.serre@allyant-group.com
IP: 190.13.122.21



VIEWED

03 / 07 / 2025

21:06:58 UTC

Viewed by Philip Humme (philip.humme@allyant-group.com)
IP: 190.13.122.21



SIGNED

03 / 07 / 2025

21:07:36 UTC

Signed by Philip Humme (philip.humme@allyant-group.com)
IP: 190.13.122.21



COMPLETED

03 / 07 / 2025

21:07:36 UTC

The document has been completed.