

Content

- 1.0** Introduction
 - 1.1** Objectives of the business risk assessment
 - 1.2** Business risk assessment regulatory compliance
 - 1.3** Definition of money laundering
 - 1.4** Definition of terrorist financing
 - 1.5** Risk based approach
 - 1.6** Abbreviation used in business risk assessment
- 2.0** Inherent risk description
 - 2.1** Inherent interface operational risk
 - 2.2** Interface operational risk board
 - 2.3** Interface risk summary
 - 2.4** Inherent geographical risk
 - 2.5** Inherent country risk assessment
 - 2.6** Geographical country risk board
 - 2.7** Inherent geographical operational risk
 - 2.8** Inherent geographical operational risk board
 - 2.9** Inherent geographical risk summary
 - 2.1.0** Inherent product risk description
 - 2.1.1** Inherent payment product risk
 - 2.1.2** Inherent payment product risk board
 - 2.1.3** Inherent game product risk assessment
 - 2.1.4** Inherent game product risk board
 - 2.1.5** Inherent payment operational risks
 - 2.1.6** Inherent payment operational risk board
 - 2.1.7** Inherent game product operational risk
 - 2.1.8** Inherent game product operational risk board
 - 2.1.9** Inherent product risk summary
 - 2.2.0** Inherent customer risk
 - 2.2.1** Inherent customer operational risk
 - 2.2.2** Inherent customer operational risk board
 - 2.2.3** Inherent customer risk summary
 - 3.0** Risk Controls
 - 3.1** Interface risk controls
 - 3.2** Interface risk control board

- 3.3** Interface risk control summary
- 3.4** Geographical risk controls
- 3.5** Geographical risk control board
- 3.6** Geographical risk control summary
- 3.7** Product risk controls
- 3.8** Product risk control board
- 3.9** Product risk control summary
- 3.1.0** Customer risk controls
- 3.1.1** Customer risk control board
- 3.1.2** Customer risk control summary
- 3.1.3** Overall risk control board
- 4.0** Residual risk description
- 4.1** Residual interface risk
- 4.2** Residual interface risk board
- 4.3** Residual interface risk summary
- 4.4** Residual country risk
- 4.5** Residual country risk board
- 4.6** Residual geographical operation risks
- 4.7** Residual geographical operational risk board
- 4.8** Residual geographical risk summary
- 4.9** Residual payment product risk
- 4.1.0** Residual payment product risk board
- 4.1.1** Residual game product risk
- 4.1.2** Residual game product risk board
- 4.1.3** Residual payment product operational risks
- 4.1.4** Residual payment product operational risks board
- 4.1.5** Residual game product operational risk
- 4.1.6** Residual game product operational risk board
- 4.1.7** Residual product risk summary
- 4.1.8** Residual customer operational risk
- 4.1.9** Residual customer operational risk board
- 4.2.0** Residual customer risk summary
- 5.1** Overall residual risk description
- 5.2** Overall residual risk board
- 5.3** Overall residual category risk definitions
- 5.4** Overall residual risk summary

1.0 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. Licensed and regulated under Curacao eGaming's licence no. OGL/2024/361/0119.

1.1 Objective of the Business risk assessment

- To list and analyze all the risks business is encountering when providing online gambling to various regions under the Curacao gambling license.
- Review current established risk controls in detail. Analyzing the reason for establishing them and their effectiveness when it comes to mitigating the inherent risk.
- Provide a summary of the residual risk remaining for the business and highlight if further controls need to be introduced further to align with businesses' current risk appetite.

1.2 Business risk assessment regulatory compliance

The BRA is designed to be compliant with the Curacao Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction and to take account the following list of recommendations, assessments, and laws when they are deemed applicable to online gambling services.

- Article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92)
- 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
- Sanctions National Ordinance (N.G. 2014, no. 55);
- FATF Recommendations and risk evaluations
- Fight against crime is one of the operational goals in Finanstilsynet's strategy for 2019–2022.
- New Zealand National Risk Assessment of money laundering and terrorist financing

1.3 Definition of money laundering

Money laundering is defined and understood by the business as:

- The conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions.
- The acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein.
- The concealment or disguise of true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.
- Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission in any money laundering activities
- Money laundering is regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.
- Money laundering is regarded as such also where the details of a criminal activity which generated the property to be laundered have not been identified.

1.4 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.

1.5 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.

1.6 Risk based approach

A risk-based approach means controls applied to each area are measured to the degree of the existing risk. This is to ensure all controls that are in place evaluate each customer differently depending on the risk they impose on the business and effectively categorize them to a risk bracket intended by the business. The risks business encounter are measured by its probability of it being encountered and by its impact to the business if materialized within the business. This is to ensure that businesses have adequate controls in place for inherent risks that have a low probability of appearing but can cause significant damage to the business if not mitigated properly.

1.7 Abbreviations used in business risk assessment

- | | |
|---|--|
| ● BRA: Business Risk Assessment | ● EU: European Union |
| ● NRA: National Risk Assessment | ● FATF: Financial Action Task Force |
| ● CRA: Customer Risk Assessment | ● PEP: Politically Exposed Person |
| ● AML: Anti Money Laundering | ● FTD: First Time Deposit |
| ● CFT: Countering the Financing of Terrorism | ● CDD: Customer Due Diligence |
| ● ML: Money Laundering | ● SDD: Standard Due Diligence |
| ● TF: Terrorist financing | ● EDD: Enhanced Due Diligence |
| ● FP: Financing of proliferation | ● KYC: Know Your Customer |
| ● RBA: Risk Based Approach | ● SOW: Source Of Wealth |
| | ● SOF: Source Of Funds |

- **P2P:** Peer To Peer
- **MLRO:** Money Laundering Reporting Officer
- **FIU:** Finance Intelligence Unit

2.0 Inherent risk description

Inherent risk is the risk that resides in the essential nature of the business. Which are categorized to: Interface, Geographical, Product and Customer risk

2.1 Inherent interface operational risks

Non face to face business model

Organization is establishing business relationship in a non-face to face model, on which makes it difficult to authenticate customers, or partners effectively upon registration.

Customer providing false details upon registration

Customers' information is not verified upon registration which means there is a risk that they can provide false personal information. The risk of providing false information allows potential ML/TF/FP to conduct transactions with false or 3rd party details which can be used to prevent the business of verifying the origin of funds and whether they originate from legitimate sources.

Duplicate accounts

Customers are able to create multiple online gambling accounts which increases risk of collusion, where customers can manipulate the interface to their benefit. Either by manipulating the odds in different games or split large sums of money into smaller amounts to avoid detection(smurfing)

2.2 Interface operational risk board

| Risk indicator | | | |
|---|-------------|--------|------|
| Non face to face registration | | | |
| Customer provides false details upon registration | | | |
| Duplicate accounts | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.3 Interface risk summary

Overall, the main interface risks are related to money launderers providing false details or opening multiple accounts which can then be used to deposit funds that originate from illegitimate sources. The risk of this is increasingly higher when business relationship is established on non-face to face basis.

2.4 Inherent geographical risk

The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. Geographical/country risk is closely linked to customer risk, which includes factors such as receiving transactions from area with high level of organized crime, corruption, country has a vulnerable financial system or insufficient AML/CFT/CFP framework.

Norway

Geographical risk assessment

- No is not on the FATF List of Countries that have been identified as having strategic AML deficiencies and was deemed Compliant for 19 and Largely Compliant for 18 of the FATF 40 Recommendations. It was deemed Highly Effective for 0 and Substantially Effective for 5 of the 11 areas of Effectiveness of its AML/CFT/CFP Regime.
- Norway is not currently under any international sanctions.
- Norway overall AML Basel index is 3.76 which is deemed a low risk
- Norway Transparency International Corruption Index is 84 (0=bad 100=good)

- Norway World Bank: Control of Corruption Percentile Rank is 91 (0=bad 100=good)
- Based on Norway National risk assessment, the deficiencies that need to be considered by online gambling service providers are Virtual currency service providers.

NRA specific deficiencies

- Finanstilsynet consistently finds that the firms fail to fully understand the AML legislation and the risk that they may be used for money laundering purposes. In Finanstilsynet's opinion, the firms are ill-prepared to recognise suspicious circumstances and to implement relevant customer due diligence measures. In cooperation with the police, they have identified and followed up several unregistered market players, thus seeking to prevent illegal activities.
- At all inspections, Finanstilsynet checks audit firms' and external accounting firms' compliance with the AML legislation. In 2020, They have collected documents from 62 entities and carried out AML inspections at 22 of these. The inspections had not been completed at year-end 2020, but several of them revealed deficiencies in the business-specific risk assessments and procedures of external accountants and audit firms. There were shortcomings in their compliance with requirements for the risk classification of customers, internal training and their ability to identify circumstances indicating that funds could be used for AML/CFT/CFP

Summary

Norway NRA clarifies that major of concerns arise from organizations failing to provide a sufficient risk rating when it comes to allocating a sufficient risk rating for virtual currencies. Additionally, the failure to properly amend organizations business-specific risks related to customers, and procedures when it comes to external audits were also highlighted. Norway is considered a low-risk jurisdiction by the business.

New Zealand

Geographical risk assessment

- New Zealand is not on the FATF List of Countries that have been identified as having strategic AML deficiencies and was deemed Compliant for 9 and Largely Compliant for 25 of the FATF 40 Recommendations. It remains Highly Effective for 2 and Substantially Effective for 4 of the Effectiveness & Technical Compliance ratings

- New Zealand is not currently under any international sanctions.
- New Zealand overall AML basel index is 3.68 which is deemed a low risk'
- New Zealand Transparency International Corruption Index is 85 (0=bad 100=good)
- New Zealand World Bank: Control of Corruption Percentile Rank is 99 (0=bad 100=good)
- Based on New Zealand's national risk assessment, the deficiencies that need to be taken into account by online gambling service providers are Weaknesses in customer due diligence (CDD), Inadequate transaction monitoring, Risks from virtual currencies, Limited enforcement and sanctions for AML/CFT/CFP breaches and Cross-border risks.

NRA specific deficiencies

- Cash remains the dominant means of transacting for domestic drug crimes. Dealers in high value goods remain vulnerable to abuse to place cash proceeds as does casino gambling. The detection rates for illicit cash in the high value goods sector are expected to improve now that the AML/CFT/CFP regime has been expanded to include high value dealers.
- Previous estimates and cases analysed as part of this risk assessment have identified three main domestic predicate offence types in New Zealand; drug offending, and to a lesser extent, fraud offending and tax offending. The analysis drew on crime statistics and reported cases from New Zealand Police Asset Recovery Units (ARU) involving restraint of assets worth more than NZD 1 million, to generate understanding of the risk associated with each of these crime types. Analysis identified seventy-two cases. Of these, the ARUs held sufficient information for analysis on 57 cases involving assets worth NZD 165 million (half of the total value of assets restrained at that time).

Summary

Despite successive studies, reliable information relating to the scale of international money laundering is limited. The most commonly cited estimate of global money laundering is the estimate by the IMF of 2-5% of global GDP. The confidence of this estimate is very low, but it does serve to provide an indication of the scale of international money laundering and the global illicit economy that New Zealand is exposed to. Based on this estimate, approximately USD 2 trillion, or around ten times New Zealand's GDP, could be expected to

be generated for laundering globally per annum. Main money laundering concerns highlighted by the New Zealand are cash heavy transfers and drug dealing and tax evasion are most common offences tied to money laundering. New Zealand is considered a Low-risk jurisdiction by the business.

Rest of the world

While business does not expect registrations from other jurisdictions and does not allow registration from countries that are deemed high risk from ML/TF/FP perspective. If the customer registers an account from a country that does not fall into the category where business concentrates their activity or are deemed high risk jurisdictions, a general risk-based approach will be taken that evaluates customers' registration country on ad hoc basis. Risk presented by rest of world countries are deemed medium risk by business.

2.6 Geographical country risk board

| Risk indicator | | | |
|-------------------|-------------|--------|------|
| Norway | | | |
| New Zealand | | | |
| Rest of the World | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.7 Inherent geographical operational risk

Customer registers from a high-risk country

Customer completes a registration from a high risk country or jurisdiction. This significantly increases the risk of the customer since they are trying to conduct transactions from a country that has anti money laundering and counter terrorist financing deficiencies. Risk is deemed a high risk.

Customer logs in or registers using a VPN or a proxy service

Customer registering using a VPN or a proxy service is a risk that they are trying to hide their country of origins, which raises the risk from both fraud and AML perspective, however VPN

is still a common product used by individuals so using it does not systematically categorize customers as high risk. Risk is deemed as medium risk.

Customer is logging in or registering with an IP that already exists in the database

Customer registers or completes a login with an IP that previously another customer has used to log in. This is a risk of collusion which, if not deemed a false positive significantly increases the customers risk. There exists duplicate dynamic IPs that are used by ISPs in the same region, meaning multiple customers logging in from the same IP does not systematically categorize customers as high risk. Risk is deemed as medium risk.

Customer completes a log in from a different country they have a residence

Customers completing a log in from a different country raises the risk that accounts actual owner has had their account compromised or customer has provided false details upon registration. Risk is deemed high risk since activity has a significant chance that organized crime can group target customer accounts considered low risk

2.8 Inherent geographical operational risk board

| Risk indicator | | | |
|------------------------------|-------------|--------|------|
| High risk country | | | |
| VPN registration | | | |
| Country IP mismatch | | | |
| Residential country mismatch | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.9 Inherent geographical risk summary

Inherent country risk

Majority of concerns that the country's NRA's rise are regarding organizations having ineffective controls regarding identifying suspicious activity, and having consistent transactional monitoring. These are more of a subjective finding as they lean more on organizations within the country that do not have adequate internal risk controls in place rather than countries themselves having deficiencies in their governmental finances. Based on countries not having any significant AML deficiencies, and after applying a risk based approach, countries the business is currently operating in are not considered a high risk for the business

Inherent operational risk

Main risks business encounters lean on customers attempting to register and deposit from countries outside of business risk appetite and collusion from residential areas. While the risks encountered are not high risk of ML/TF/FP automatically the risk increases if the activity originates from a high risk country.

2.1.0 Inherent Product risk description

Product risks are risks that businesses encounter when providing their product and services to the customers. Some products are considered lower risk of ML as the source of funds can be verified to originate from a licensed financial facility and have a smaller chance of the customer being able to manipulate the product to illegitimate means such as money laundering and terrorist financing. While some products are considered a higher risk due to the opposite effect.

2.1.1 Inherent payment product risk

Bank transfers

Deposits through bank accounts verify funds originate from a regulated financial institution and account owner details are received with the transactions. Bank transfers are considered a Low risk

Card transfers

Deposits through bank cards verify funds originate from a regulated financial institution and account owner details are received with the transactions. Card transfers are considered a Low risk

E-wallets

Deposits through E-wallets are considered higher risk from bank transfers, as the same regulations that are applicable to bank facilities cannot be applied to E-wallets. While account details are collected, they are not necessarily verified upon registration. E-wallets are also more lenient regarding funding of the account, which means there are less restrictions when it comes to 3rd party funding and peer to peer transfer monitoring. E-wallets are considered a Medium risk from a money laundering perspective.

Anonymous payment methods

Payment methods that permit customers to create an account without collecting any personal information or allows customers to deposit funds while having the ability to remain anonymous, are more commonly used by organized crime groups. This is due to the accessibility the methods provide when it comes to disguising illegitimate funds as the beneficial owner of funds is not established during transactions. Anonymous payment methods are considered a high risk.

2.1.2 Inherent payment product risk board

| Risk indicator | | | |
|----------------|-------------|--------|------|
| Bank transfers | | | |
| Card transfers | | | |
| E-wallets | | | |
| Anonymous PM | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.1.3 Inherent game product risk assessment

Slots

Slots are considered a low-risk product as they are purely RNG based, there is no risk of collusion or hedging.

Table games

Table games are considered a medium risk product. While they cannot be fixed as the event organizer is a licensed game provider, they do have a risk of collusion. Customers can collude together to effect the outcome and mitigate the loss of funds by making sure the winning amount is received by the colluding party. Customers can also practice safe betting to minimize their losses while completing the turnover requirement. This can be used to build a false winning trail to make the wagered amount seem more legitimate.

Sportsbetting

Sports betting is considered a medium risk product as they have a risk of hedging collusion

and a risk that the organizer has rigged the event. Customers can then use insider knowledge to influence their chance of winning and minimize the loss of revenue when making their winning appear legitimate.

P2P games

P2P games are considered a high risk since customers can choose their opponents which have a high risk of collusion and chip dumping, such as online Poker. Colluding players can use chip dumping to transfer funds between each other, while also receiving a false narrative for the source of funds.

2.1.4 Inherent game product risk board

| Risk indicator | | | |
|----------------|-------------|--------|------|
| Sportsbook | | | |
| Table games | | | |
| Slots | | | |
| P2P games | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.1.5 Inherent payment operational risks

Customer operates under open loop

Customers operate under open loop either by using anonymous payment methods where verifying closed loop is not applicable or conducted deposits and withdrawal proceedings are processed through different payment methods. This raises a risk regarding players attempting to conceal the trail of funds either from the business or the financial institution.

Customer makes a deposit using a method belonging to a 3rd party

Customer is using a payment method belonging to a 3rd party to deposit. This is considered a higher risk, since customers might be using funds not belonging to them and try to cut out the audit trail by operating on an open loop.

Customer is using multiple accounts under the same payment method

Customer uses the same payment method, however, uses multiple sub accounts under it.

This increases the risk of customers having multiple income sources and based on their withdrawal pattern can increase the risk of ML.

Customer is stacking deposits

Customer is doing multiple deposits without any wagering in between. This is unusual behavior since the customer is not using the product as intended and which raises concerns from an ML perspective.

Customer becomes inactive after deposit

Customer becoming inactive after deposit is deemed as usual behavior, since they are using the product in a way it was not intended. Gambling sites are not meant to be used as a banking institution, which means this behavior raises the risk of money laundering since customers may hide funds from financial authorities.

Customer initiates a chargeback request without cause

Chargeback is a practice put together by credit/debit card providers to protect customers in case an unauthorized deduction is done from their card either due to banking error or their card being compromised. This system can be exploited by the customers where after normally depositing to a gambling site they falsely claim the deposits were initiated by an unauthorized 3rd party. Depending on the dispute, the customer can successfully receive the wagered funds back, and in most chargeback cases the customer receives the chargeback funds to a new card which then can be used to create a questionable audit trail. Chargebacks are a greater risk of fraud but can also be a risk of money laundering

2.1.6 Inherent payment operational risk board

| Risk indicator | | | |
|-------------------------------------|-----|--------|------|
| Open loop | | | |
| 3 rd party deposit | | | |
| Multiple accounts under same method | | | |
| Customer is stacking deposits | | | |
| Inactive after deposit | | | |
| Chargeback | | | |
| Risk level | Low | Medium | High |

| | |
|--------------|-------------|
| Overall risk | Medium Risk |
|--------------|-------------|

2.1.7 Inherent game product operational risk

Customer makes a withdrawal without wagering their deposits

Customer initiates a withdrawal before wagering the deposited amount. This is considered unusual behavior, as customer had no intention of using the deposited amount for the purpose the product was intended to which raises concerns from ML perspective.

Customer is opposite betting

Customer is colluding with other customers in a table game e.g. baccarat or roulette where they match on each other's bets while betting on the opposite sides of the bet. Exercising this behavior minimizes the loss of deposits as it verifies either of the colluding players receive the winnings of the round. Opposite betting can be used to transfer funds between customers, which means players exercising it are deemed an AML concern.

Customer is counting cards

When a customer is counting cards they are calculating all the cards that have been played after the shuffle to calculate the possible outcomes for the dealer's card, customers own card or other possible colluding players. This combined with the option of placing insurance bets or doubling down rules can be used to manipulate the RTP in customers favor, which significantly mitigates the loss of deposit or eliminates it completely. Customers exercising counting cards are at risk of both Fraud and ML.

Customer is safe betting

Customers are exercising safe betting when they are betting in table games in a way where there is no chance of winning, however loss of funds is also minimal or low chance. This is commonly practiced in table games such as baccarat or roulette. Where placing an equal bet on both sides of the event. Normal winning ratio in table games is 1:2 which means customers returning from the bet will return the betted amount. Since there is no chance of winning, this is deemed unusual behavior and raises the money laundering risk.

Customer is chip dumping

Customers use P2P products to collude with other parties by intentionally losing to each other as a means of transferring funds between each other.

Money launderers can easily use chip dumping to layer funds to online gambling sites and disguise them as winnings that appear legitimate. Chip dumping is considered a high risk from a money laundering perspective.

Customer is hedge betting

Hedge betting is when a customer is betting on multiple sides of an event. This minimizes the losses as there is a high chance, customers either one of the bets in the Event will be the outcome. Hedge betting is not deemed a risk of ML automatically as hedge betting is commonly used by sport betters to reduce the loss in high odd games, however if hedge betting is exercised in a way where there is no chance of winning any funds and is only exercised to mitigate the risk of loss entirely, this is deemed a risk of ML.

2.1.8 Inherent game product operational risk board

| Risk indicator | | | |
|-----------------------------|-------------|--------|------|
| Withdrawal without wagering | | | |
| Opposite betting | | | |
| Counting cards | | | |
| Safe betting | | | |
| Hedge betting | | | |
| Betting on minimum odds | | | |
| Chip dumping | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.1.9 Inherent product risk summary

When it comes to product risks mainly lean on customer showing behavior that is not

expected from a normal customer that uses online gambling services. Above risks all can be an indicator that a money launderer is using the product to create false audit trails with minimal losses or try to completely disguise the source of illegitimate funds as gambling wins.

2.2.0 Inherent customer risk

Customer risk is the risk customer risk imposes to the business upon establishing the relationship. Based on their existing information, activity and behavior some customers impose a higher risk that they are using illicit sources to fund their gambling.

2.2.1 Inherent customer operational risk

Politically exposed person and relatives and close associates (PEP)/(RCA)

Customers identified as a political person pose a high risk to the business as the person has been assigned a public function which means they have access to funds that are meant to be used in upkeeping government procedures and functions. There then exists a risk a customer identified as a PEP is using governmental funds to gamble or attempt to launder governmental funds through the site. Persons that are associated with PEPs are equally considered as high risk, as they can be used to facilitate funds received from PEPs. This includes close relatives tied to a PEP and persons currently in a business relationship with a PEP.

Customer, or the organizations are under financial sanction, or the country they are currently resident in is under financial sanction

Customers identified as being under sanctions are an extreme risk since governmental entities have sanctioned the customers due to unlawful activities such as being part of terrorist organizations, human rights violations and being a threat to overall global peace. Purpose of assigning financial sanctions is to make sure customers cannot use any services that provide any type of financial benefit. That means businesses are prohibited from having business relationships with persons or organizations that are under financial sanctions.

Customer is showing unusual behavior

Customer unusual behavior can come in many forms, however the main one's business can encounter is with the interactions with the customers. If a customer shows obsessive behavior when interacting with the customer support department, they try to pressure

business to rush proceedings either through solicitation or intimidation. Customers attempting to circumvent policies set by the business raise concerns from a money laundering perspective.

Bribery

Customers may try to attempt to bribe a member of the business either directly or indirectly. This means providing funds of favor with monetary value in exchange for the business to not follow the established policies that were set in place to comply with a regulatory requirement or manage the risk customers impose. Attempts at bribery are extreme risk for the business as they compromise the entire customer risk infrastructure, which means risk controls in place aren't followed.

Customer tipping off/Illegal notification of the customer

Customers are "tipped off" when they are provided information regarding internal anti money laundering proceedings and policies or are provided information regarding any anti money laundering investigations business is conducting. Tipping of a customer is an extreme risk from money laundering perspective as it's a breach of regulatory requirements and compromises future investigation of a potential money laundering subject, as they can use the tipped of information to create preparations to hinder or counter the investigation.

Adverse media

Customer business relationships established with a customer with adverse media impose a higher risk as the customer has previously been involved in activities that can have an adverse impact on their source of funds, which makes customers with adverse media a money laundering risk.

2.2.2 Inherent customer operational risk board

| Risk indicator | | | |
|----------------------------|--|--|--|
| Politically exposed person | | | |
| Sanction list match | | | |
| Unusual behaviour | | | |
| Tipping off | | | |
| Bribery | | | |
| Adverse media | | | |

| | | | |
|--------------|-------------|--------|------|
| Risk level | Low | Medium | High |
| Overall risk | Medium Risk | | |

2.2.3 Inherent customer risk summary

Customers pose a high risk to the business as business relationships are established by the customers without businesses manual approval. So there are no initial restrictions for customers registering an account. Inherent customer risk is rated as high risk.

3.0 Risk Controls

Risk controls are policies and procedures established to mitigate the risk encountered by the business. Controls are assessed based on their functionality when it comes to remaining compliant with the regulatory requirements and their effectiveness when it comes to eliminating the probability and the impact of the risk. Risk controls are met to be dynamic when it comes to treating the inherent risks, and BRA is evaluated annually or whenever there is a significant change which exposes the business to new risk areas. Risk Controls are evaluated in ineffective -> satisfactory -> Effective category based on their efficiency in mitigating the risk and being compliant with the regulatory recruitments

3.1 Interface risk controls

Standard due diligence

When a customer registers an account, they are required to provide standard due diligence where they provide their personal information which includes their identity, residence and contact information. Customers can still write misleading details but aren't able to bypass the step. Control is deemed effective since it cannot be circumvented or exploited.

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. Overall risk profile upon registration cannot always be accurately rated due to the lack of information and activity the customer has at this time, registration report aids in highlighting customers who raise initial red flags, which the Payment and Risk department can then review and allocate a risk rating. Control is deemed satisfactory, while it does not provide full vision of the customer risk upon registration, it fulfills its function when it comes to highlighting high risk customers upon their first deposit.

Duplicate account alarm

If a customer registers with a matching first name, last name and date of birth system will trigger an alarm that will be reviewed by a member of staff. Depending on the review account will be suspended as a duplicate or discounted as a false positive. Customers can circumvent the alarm by changing the personal information on the duplicate accounts slightly, but the alarm still functions as intended when highlighting accounts with duplicate details. Control is deemed satisfactory due to customer being able to circumvent the alarm, however alarm still functions as intended when it comes to highlighting players with duplicate account details

3.2 Interface risk control board

| | | | |
|--------------------------------|---------------------|---------------------|--------------------|
| Established control | | | |
| Standard due diligence | | | |
| Registration report | | | |
| Duplicate account alarm | | | |
| Risk level | Effective | Satisfactory | Ineffective |
| Overall risk | Satisfactory | | |

3.3 Interface risk control summary

The overall difficulty of allocating a detailed risk rating from ML/TF/FP perspective upon establishing customer business relationship, limits the length of assessment that can be produced upon this stage. However, controls in place ensure customers that raise high ML/TF/FP concerns are suspended or are put under a more robust customer due diligence process before significant amounts of deposits are conducted by the customer.

3.4 Geographical risk controls

Geographical location details that are collected upon login and registration

Customer IP and their country location are collected on every sign in. There is no action that can be taken from customers end to prevent the following details from being received by the business. Customers can still disguise their IP and their residential country by using VPN and proxy servers, however other policies and procedures are in place to prevent this behavior, so overall efficiency of the control is not adversely impacted. Control is deemed as effective since customers aren't able to circumvent it in a way that would not lead to additional controls being triggered. Additionally, the business also enforces blocks on countries where online gaming is outright prohibited or where a local license is required to operate. This ensures compliance with applicable regulations and prevents customers from restricted jurisdictions from accessing the platform. Geo and reg block is deemed an effective control as it can't be circumvented by the customer.

VPN and proxy servers review

A customer using a VPN while logging in does not automatically translate to risk of ML/TF/FP. To take this to consideration, business does not systematically consider use of VPN as a higher risk, and does not have automated alerts identifying use of VPN. However customer IPs are monitored and depending on the applied risk based approach use of VPN is assessed proportionately, and usage limited, if it can be used to mitigate the existing customer risk. Control is deemed satisfactory as it does not prevent risks related to VPN usage, however it does give the necessary visibility to review customer VPN usage during customer risk assessments.

Duplicate IP alert

Business has an alert in place that highlights customers that log in using an IP that was used to log in, and has been used by another customer. Alert only highlights the customer, for being reviewed by the assigned employee who can discount it as a false positive or apply further controls if deemed a risk of collusion. Control is deemed effective as the alert identifies the possible risk, which leads to further manual assessment and evaluation.

Geo and reg block from unwanted countries and jurisdictions

Business has a geographical block in place that will automatically prevent a customer from registering an account from countries and jurisdictions that business has deemed high risk. Customers are unable to circumvent the geo block and aren't able to conduct transactions

from the blocked country as business has payment methods in place for selected countries that are geographically deemed low risk. Geo and reg block is deemed an effective control as it can't be circumvented by the customer.

IP/Country mismatch alerts

Businesses have alerts in place that highlight customers that login from a different country that differs from their residential country. Once the alert has been triggered, the payments and risk department will review it from ML/TF/FP perspective. Customer is unable to circumvent the alert which will lead to business relationship termination if alarm triggered and raises concerns from ML/TF/FP perspective. Control is deemed effective as alarm cannot be avoided from triggering and will lead to a manual review and possible business relationship termination.

3.5 Geographical risk control board

| Established control | | | |
|---------------------------|--------------|--------------|-------------|
| Geo info collection | | | |
| VPN/proxy review | | | |
| Duplicate IP alert | | | |
| IP country mismatch alert | | | |
| Risk level | Effective | Satisfactory | Ineffective |
| Overall risk | Satisfactory | | |

3.6 Geographical risk control summary

Geographical risk controls in place mitigate the risk significantly due to their ability to prevent the risk from appearing, and while some of them have a likelihood of appearing they

are mitigated by manual reviews by the employees and high risk cases lead to business relationship termination.

3.7 Product risk controls

Applying closed loop

Whenever applicable, business will enforce customers to operate on a closed loop. This means withdrawals are sent back to the account where deposits used to generate the gambling funds originated from. This is to verify the product is not used as a way to move funds originating from a different source to another method. While closed loop cannot always be applied due to some methods being anonymous and some methods only providing depositing as a service, there exist other controls that are applied to ensure funds are only sent to methods that belong to the owner of the depositing customer. Control is considered as satisfactory since closed loop is applied to majority of transactions, but due to lack of KYC visibility or the products or technical deficiencies closed loop cannot be applied on every transaction.

3rd party transactions monitoring

Business does not allow third party usage and we have rules in place to detect this. Any direct funding of gambling accounts with foreign payment methods will be detected in monitoring rules and procedures and in most cases many of these will be automatically rejected in real time. Control is considered satisfactory, as non PNP 3rd party deposits can still be conducted by the customer, they aren't able to make withdrawals or deposit significant amounts while remaining undetected by transaction monitoring procedures.

High value transactions alerts

We have real time risk alerts in place to detect substantial amounts deposited or withdrawn, these rules are based on various timeframes to catch players who might transfer high value transactions over a longer period of time. All of these players are reviewed carefully where a full risk assessment is carried out. Control is deemed effective while players can possibly bypass transaction alerts by depositing below them, there exist other controls to monitor this behavior, which would still lead customers to be reviewed and risk rated by an employee from ML/TF/FP perspective.

Deposit stacking alerts

Business has alerts in place to highlight players that have conducted a deposit before fully wagering their previous deposit. Control is deemed satisfactory, while the alert does not prevent customers from stacking deposits, it highlights the customer as a possible risk which leads to additional controls to be applied.

Anonymous transaction monitoring

All crypto transactions are monitored separately, and we have procedures in place to manage this risk adequately by automated risk assessment of each transaction on blockchain. Other funding with anonymous payment methods are monitored through reports and are risk assessed. Accounts with only this type of funding always must complete standard due diligence before any withdrawal approval. Control is deemed satisfactory. While the source of funds is not established on every transaction, customers using anonymous payment methods are highlighted and risk assessed either when a significant amount of deposits have been deposited or upon first withdrawal. This ensures sufficient risk controls are applied to the customer based on their allocated risk level.

Procedures in place to verify players wagering

According to business policy, customers aren't allowed to make a withdrawal until deposits linked to it have been wagered at least once. On PNP transactions customers are automatically prevented from making withdrawals without wagering. Non PNP their first and high volume withdrawals are reviewed by a member of staff to ensure necessary wagering requirements are met. If customer activity does not present significant amount of risk after the assessment their upcoming payouts can be assigned to be automatically processed by the internal system. If customers risk rating increases, their automatic payouts will be disabled, and they are placed back into manual review. Control is considered satisfactory as customers are restricted from conducting withdrawals without wagering their deposits at least once, as they are continuously monitored by automated systems and members of staff.

Reports raised by game provider

Game providers have full visibility when it comes to monitoring gameplay on their products. If a suspicious activity such as card counting, opposite betting, hedge betting and safe betting are being conducted, the game provider will report the customers to the business, which enables the business to apply the necessary RBA and terminate the business

relationship when required. Control is deemed satisfactory, while it does prevent customers suspicious activity, it assures customers that gameplay raises concerns from ML/TF/FP reported and treated with additional controls based on their allocated risk.

Business is not providing a P2P products

Currently the business is not offering P2P gambling services. This is considered an effective control as it makes risks that come with P2P products irrelevant.

3.8 Product risk control board

| Established control | | | |
|--|--------------|--------------|-------------|
| 3rd party transactions monitoring | | | |
| High value transactions alerts | | | |
| Deposit stacking alerts | | | |
| Anonymous transaction monitoring | | | |
| Procedures in place to verify players wagering | | | |
| Business is not offering a P2P product | | | |
| Game provider reports | | | |
| Risk level | Effective | Satisfactory | Ineffective |
| Overall risk | Satisfactory | | |

3.9 Product risk control summary

Product risk controls in place provide sufficient means to ensure business is not exposed to

risks that can significantly adversely affect it such as remain compliant with regulatory requirements and significant loss of revenue. While the controls in place do not preemptively eliminate all product risks that the business is exposed to, they effectively identify them, which allows designated employees to assess and evaluate the product risk proportionately based on the situation.

3.9 Customer risk controls

Customer risk assessment

When sufficient information is received during customer business relationships, or their risk rating is increased from geographical, interface, product or activity perspective. A customer risk assessment is conducted by an employee in the organization, who will identify the reason why customers fell under our risk review policy, assess their activity from the start of the business relationship and allocate a risk rating for them. Depending on the assessment result, the customer is either placed back into ongoing monitoring or apply further controls to de-risk the customer to the lower risk category. During the assessment if a customer raises concerns from an ML/TF/FP perspective, the customer is raised to MLRO for further review who then will make a decision if the customer needs to be raised to the Financial Intelligence Unit for suspicion of ML/TF/FP. Control is deemed satisfactory, while robust customer risk assessment cannot be conducted immediately upon establishing a business relationship, due to lack of information available at the time, it is still conducted whenever there's a possible change from low risk to higher one. Currently business has controls in place to highlight possible scenarios when there might be a change in customer risk, and with the combination of customer risk assessment, it is assured customers risk rating is constantly reviewed.

Customer due diligence

Business applies customer due diligence measures upon customers, when they reach an accumulative transaction sum of 4000 Naf. This applies to both deposits and withdrawals done by the customer during the business relationship, however both thresholds are counted independently and not combined. Meaning if a customer deposits 2000 Naf and makes a withdrawal of 2000 Naf threshold is not met. Business might also request customer due diligence earlier if it's required to de-risk the customer. Customer due diligence is understood by the business as verifying the personal details that customer has submitted upon establishment of business relationship by physical documents sent by the customer. The current approach is compliant with the regulatory requirements. Since the

original source of the documents is the registered customer who can adversely influence the quality or legitimacy of the documents current control is rated as satisfactory.

On-going monitoring

Every customer that the business establishes a relationship with are placed into on-going monitoring. Ongoing monitoring is based on customers behavior where their activity and transactions are continuously measured proportionately based on the severity the risk imposes, or if have they conducted transactions over 5,000 NAf. and quantity of the risks occurrence. This ensures all risks are monitored, however treated differently based on the situation. Customers who are considered a high risk but later mitigated to a lower risk category are placed into a timely monitoring to ensure regardless of the behavior, they are periodically reviewed. Control is considered effective as customer activity is continuously measured, which will eventually expose them to follow-up control that will assess and mitigate the customer risk.

Enhanced due diligence

Business applies enhanced due diligence upon customers that have been allocated a high-risk rating. High risk customers are persons who are raising concerns from an ML/TF/FP perspective or there are enough reasons to suspect a politically exposed person. Enhanced due diligence is understood by the business as a collection of documents that identify what funds customers have used to fund their gambling and assess whether the funds originate from legitimate sources. Control is deemed effective as business has controls in place to verify customers that pose a high risk are identified, and to complete an enhanced due diligence process customer has to verify they are funding their gambling with legitimate sources, or their business relationship is terminated.

Politically exposed person and sanction check monitoring

During establishing a business relationship, customers are screened against recognized PEP and Sanction lists. Any customer identified as a PEP will have their account closed as soon as flagged and reviewed by our internal rules. If any successful transaction has been carried out on account before being reviewed, then an Enhanced due diligence check is carried out before repayment of outstanding balance in account. Currently the business does not have any active PEP customers, and the database is continuously monitored in real time to keep that number at Zero. Any customer identified and verified as a potential

PEP should also be reported to MLRO for further investigation. Controls are considered satisfactory, while a customer can become a PEP or be listed under sanctions during a business relationship and not immediately identified. Continuous screening ensures they will be identified and business relationships terminated.

Suspension of customer withdrawals

If customers activities are deemed unusual and their risk is increased, business will refrain from processing further withdrawals until necessary controls have been applied to mitigate the customer risk and stay compliant with the regulatory requirements. Once customer withdrawals are suspended risk of ML/TF/FP are sufficiently mitigated as withdrawals are only process once business has conducted sufficient due diligence that mitigates the customer to a low enough risk to allow processing of withdrawals or they have raised significant number of concerns from ML/TF/FP perspective, which would lead to business relationship termination and customer to be reported to FIU. Control is deemed effective as customers cannot bypass it once set in place and prevents customers from transferring funds without business applying the necessary risk based approach.

Customer business relationship termination

Business will terminate any customer business relationships that do not fall under its current risk appetite and are unable to mitigate the risks with the existing controls. When a customer business relationship is terminated, their access to the account is permanently removed and they are unable to conduct any transactions to/from the account. Remaining funds on high-risk customers' accounts, are either sent to the customer via closed loop or to a verified bank account, that customer has beneficial ownership of. If monetary value of remaining balance is substantial or the customer raises concerns from an ML/TF/FP perspective, funds remain on the customer's game account, until customer risk has been mitigated, or a jurisdictional law enforcement agency has provided authorization to process remaining funds. Customers who raise concerns from ML/TF/FP perspective are also raised to MLRO for further evaluation whether the customer needs to be reported to the Financial Intelligence Unit. Control is deemed effective, as once a business relationship has been terminated, the customer's behavior that was deemed too much of a risk by the business is de-risked entirely.

Limited disclosure of ML/TF/FP investigations

Information regarding investigations related to ML/TF/FP are only shared and communicated between AML departments. When necessary, information can be shared to

senior management or relevant employees at sole discretion of the MLRO. Control is deemed effective as it significantly reduces the risk of tipping of the customer, since the AML department does not directly communicate with the customer and information regarding investigation is only being shared internally between them.

Reporting of suspicious activity

Customers that are considered high risk and raise concerns from ML/TF/FP perspective are raised to companies MLRO for review through internal suspicious transactions reports or reviewed directly by MLRO if the customer has been identified as ML/TF/FP by AML policies and procedures. Then a decision is made whether there are enough concerns raised by the customer that they need to be reported to the Financial Intelligence Unit for investigation. Control is deemed effective as all cases that raise concerns from ML/TF/FP perspective are reviewed by companies MLRO and are compliant with current regulatory requirements.

Reporting unusual transactions

Automated reports are run daily that highlight transactions that exceed 5000 Naf as they are deemed unusual by National Ordinance. Transactions identified on the report will then be raised externally to FIU for further review. Control is deemed effective as its compliance with the regulatory requirements and customers cannot directly affect the control.

Business employee training

Every employee in the business that has duties and obligations regarding establishing business relationships or the making of transactions are provided with training that will keep them informed regarding shared obligations when it comes to being compliant with regulatory requirements. Training also educates employees on how to identify ML/TF/FP concerns that they can encounter during their daily operations and how to report suspicious activity to the senior management. Control is deemed effective since it verifies employees who are aware of the ML/TF/FP concerns they can encounter during their day-to-day operations and are aware that they are held accountable for any intentional breaches of AML policies and procedures. Control is aligned with the regulatory requirements and is deemed effective.

Internal auditing

MLRO periodically reviews existing procedures and controls for their effectiveness when it comes to mitigating risk of ML/TF/FP. This includes assessing the procedures in place and

evaluating their previous effectiveness and whether it has changed. Internal auditing also includes interviewing staff members who are responsible for maintaining the controls on a regular basis, and evaluating does the performance aligns the results given for the policy. MLRO will also regularly review existing customer databases by dip sampling to ensure established controls are applied. Control is deemed effective.

External auditing

An external audit is performed by people who are not involved with the organization's AML compliance staff. They assess and evaluate the existing AML policies and procedures for their effectiveness in prevention of ML/TF/FP and do their adequately meet the regulatory requirements. Control is deemed effective as it meets the regulatory requirement.

3.1.1 Customer risk control board

| Established control | | | |
|-----------------------------------|-----------|--------------|-------------|
| Customer risk assessment | | | |
| On-going monitoring | | | |
| Customer due diligence | | | |
| Enhanced due diligence | | | |
| PEP and SAC list monitoring | | | |
| Suspension of withdrawals | | | |
| Business relationship termination | | | |
| Reporting of suspicious activity | | | |
| Reporting of unusual activity | | | |
| Business employee training | | | |
| Game provider reports | | | |
| Internal auditing | | | |
| External auditing | | | |
| Risk level | Effective | Satisfactory | Ineffective |

| | |
|--------------|--------------|
| Overall risk | Satisfactory |
|--------------|--------------|

3.1.2 Customer risk control summary

The current customer risk controls in place are compliant with regulatory requirements and effectively manage risk. Once sufficient information has been gathered, customers are assigned to a risk category, and based on the assessed risk, proportional mitigating controls are applied. These controls either verify that the individual falls within the business risk appetite or terminate the business relationship if the customer poses a risk that is not aligned with regulatory requirements.

3.1.3 Overall risk control board

| | | | |
|----------------------------|--------------|--------------|-------------|
| Established control | | | |
| Interface risk controls | | | |
| Geographical risk controls | | | |
| Product risk control | | | |
| Customer risk | | | |
| Risk level | Effective | Satisfactory | Ineffective |
| Overall risk | Satisfactory | | |

4.0 Residual risk description

The residual risk is the outcome of established risk controls applied to the inherent risks that business encounters. The main objective of the section is to outline the remaining risk and does it align with the current risk appetite.

4.1 Residual interface risk

Non face to face business model change and applied controls

- Information collected upon registration
- Registration report (Today & Yesterday)
- Customer due diligence
- Enhanced due diligence

While non face to face registration risks cannot be fully mitigated, applied controls ensure customers' identity is collected upon registration and verified after there's enough data to establish a customer risk profile or when they raise red flags that allocates customers to a higher risk. Risk is mitigated from a high risk to a low risk.

Duplicate account risk change and applied controls

- Duplicate account alarm
- Registration report (Today & Yesterday)

Customers can still register a duplicate account, however a duplicate account alarm in place highlights accounts with the same customer details, which allows the employee to review the alarm and apply a sufficient risk-based approach. Risk is mitigated from a medium risk to low risk.

Customer providing false details upon registration risk change and applied controls

- Customer due diligence
- Enhanced due diligence
- Registration report (Today & Yesterday)

Customers can still register an account with false details; however, controls monitor customer details on registration and due diligence applied automatically allocates customers to a higher risk if provided documents do not align with the details provided upon registration. Risk is mitigated from a high risk to a low risk

4.2 Residual interface risk board

| Risk level | | | |
|---|--------|--------|------|
| Non face to face registration | | | |
| Customer provides false details upon registration | | | |
| Duplicate accounts | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.3 Residual interface risk summary

Risks business encounters during establishment of customer business relationships are substantially mitigated by the controls to ensure no significant number of deposits can be conducted. In addition, withdrawals aren't being conducted until customer details are deemed genuine, and surface risk level has been established. While risks aren't de-risked entirely since customers can still establish a business relationship with the intention to abuse it, the controls identify this behavior in retrospect. Once an identified, business relationship is terminated, if confirmed business relationship was established in ill faith from the customers end.

4.4 Residual country risk

- Reporting of suspicious activity
- Customer risk assessment

Business is currently only focusing providing services to countries and jurisdictions that are inherently deemed as low risk, as they are not deemed to have significant deficiencies when it comes to AML/CTF/CFP by FATF. Business is currently reporting suspicious activity to the Curacao FIU to remain compliant with the jurisdiction's regulatory requirements. Risk remains a low risk, and established controls take account of the findings highlighted by countries' NRA. Any customer who registers from rest of world that is not automatically blocked will be have controls applied based on their inherent risk.

4.5 Residual country risk board

| Risk level | | | |
|-------------------|--------|--------|------|
| Norway | | | |
| New Zealand | | | |
| Rest of the world | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.6 Residual geographical operation risks

Customer registers from a high-risk country remaining risk and applied controls

- Geographical location details collected on login
- Log in and deposit blocks from unwanted countries and jurisdictions

Business has applied preventive measures to high-risk countries that reject all registrations and logins from high-risk countries. Risk is mitigated from a high risk to a medium risk.

Customer is logins or registers using a VPN or a proxy service remaining risk and applied controls

- Geographical location details collected on login
- First time deposit report
- Customer risk assessment
- On going monitoring
- Customer due diligence
- Enhanced due diligence

Customers can still use VPN and proxy servers to login and register an account, however their activity is reviewed upon first deposits and ongoing basis during the business relationship. Usage of VPN is not considered a risk of ML/TF/FP; however it is considered a potential red flag. If a customer in combination with VPN usage raises other red flags, they

are subjected to due diligence measures to mitigate the established risk. Risk remains as medium risk.

Customer is logging in or registering with an IP that already exists in the database risk and applied controls

- On-going monitoring
- Geographical location details collected on login
- Customer risk assessment
- Duplicate IP alarm

IP alerts highlight all customers that have raised red flags based on their log in activity. Due to the duplicate amount of dynamic IPs that exist, alerts do not lead to automatic increase in risk, but they are proportionately evaluated by the assigned employee for any concerns of ML/TF/FP. Risk remains as medium risk as alerts do not take preventive action and further controls are applied retroactively after customers login.

Customer completes a log in from a different country they have a residence remaining risk and applied controls

- IP/Country mismatch alerts
- Customer risk assessment
- 3rd party transactions monitoring
- Suspension of customer withdrawals

Controls that business have in place does not prevent customers from logging in from a different residence, however ensure logins are highlighted and a proportional risk based approach applied whether alarm is deemed as normal behavior by the customer or risk of account being hijacked. Depending on the risk level further controls are applied when necessary, which prevents accounts being used by criminals in ML/TF/FP purposes. Risk mitigated from a high risk to medium risk.

4.7 Residual geographical operational risk board

| Risk level | | | |
|--|--------|--------|------|
| Customer registers from a high-risk country | | | |
| Customer is logins or registers using a VPN or a proxy service | | | |
| Customer is logging in or registering with an IP that already exists in the database | | | |
| Customer completes a log in from a different country they have a residence | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.8 Residual geographical risk summary

Countries' geographical risk remains low, as countries business is operating have not systematic ML/TF/FP deficiencies and customers resident in high risk countries aren't able to establish business relationships. While risks related to customers using tools and services that can disguise remain apparent, usage of the tools are assessed and any concerns from ML/TF/FP will be mitigated by application of due diligence measures.

4.9 Residual payment product risk

- Customer due diligence
- Enhanced due diligence
- Enforcing closed loop

- Customer risk assessment
- Anonymous transaction monitoring

Customers that use E-wallets have a higher risk than bank and service, so during the due diligence process proof of payment method details are collected to ensure closed loop and risk of 3rd party exposure or the account details are verified by the payment service provider. Deposits done with anonymous payment methods cannot be preemptively de-risked and are deemed as high-risk products. To mitigate the risk business will enforce winnings that originate from anonymous deposits such as vouchers to be paid off to a bank account that shares the same name as the registered customer. To further mitigate this business will conduct enhanced due diligence if customers deposit significant amounts with anonymous payment methods to verify funds used to deposit originate from legitimate sources. Risk of bank transfers and card transfers remains low risk, E-wallet transfers remain a medium risk, and anonymous payment methods are mitigated to a medium risk.

4.1.0 Residual payment product risk board

| Risk level | | | |
|----------------|--------|--------|------|
| Bank transfers | | | |
| Card transfers | | | |
| E-wallets | | | |
| Anonymous PM | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.1.1 Residual game product risk and applied controls

- Business is not providing P2P products
- Risks reported by game provider
- Customer risk assessment

Business is currently not providing P2P products to the customers, which derisks them entirely. Customers' gameplay is monitored continuously through customer risk assessments, which if raises concerns from ML/TF/FP perspective are subjected to additional controls. Game Providers are also internally monitoring customers for suspicious activity and will report them to the business if detected. P2P product risk is mitigated from

high risk to low risk, Sportsbook products risk remains at medium risk, table games remain as medium risk, and slots remain a low-risk product

4.1.2 Residual game product risk board

| Risk level | | | |
|--------------|--------|--------|------|
| Sportsbook | | | |
| Table games | | | |
| Slots | | | |
| P2P games | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.1.3 Residual payment product operational risks

Customer operates under open loop risk changes and applied controls

- Customer due diligence
- Enforcing closed loop
- Anonymous transaction monitoring
- Suspension of customer withdrawals
- Customer risk assessment

While the risk of customers operating under open loop is not completely de-risked, applied controls enforce it whenever possible, and customers that use payment methods that lack full KYC visibility or technical ability to process both deposits and withdrawals, are continuously monitored to ensure they are withdrawing funds to bank account that belongs to gaming accounts owner. Risk is mitigated from high risk to medium risk.

Customer makes a deposit using a method belonging to a 3rd party risk changes and applied controls

- Customer risk assessment
- Customer due diligence
- 3rd party transactions monitoring
- Suspension of customer withdrawals
- Enhanced due diligence
- Customer business relationship termination

While 3rd party deposit risk cannot be fully de-risked, since they aren't preemptively identified and blocked, business will deem all 3rd party deposits as high risk, and further

controls are applied until risk of ML/TF/FP are eliminated or business relationship is terminated. Risk is mitigated from high risk to medium risk

Customer is using multiple accounts under the same payment method risk changes and applied controls

- Customer risk assessment
- Customer due diligence
- Suspension of customer withdrawals
- Enforcing closed loop

Customers can deposit using sub accounts on the same payment method, however this activity is monitored through customer risk assessments and customer falls under manual withdrawal processing to ensure closed loop is applied. Using multiple accounts on the same payment method is not systematically considered a risk from ML/TF/FP. However, during a risk assessment the customer is raising red flags, they are subjected to further controls to mitigate the risk. Risk is mitigated from medium risk to low risk.

Customer is stacking deposits

- Deposit stacking alerts
- Enforcing closed loop
- Customer risk assessment
- Customer due diligence

Customers can still enact deposit stacking, but it is monitored through internal procedures for possible risks of money laundering. Based on an applied risk-based approach, the customer is allocated back to a lower risk or subjected to further controls if they raise concerns from an ML/TF/FP perspective. Risk is mitigated from a medium risk to low risk.

Customer becomes inactive after deposit risk changes and applied controls

- Customer risk assessment
- Enhanced due diligence
- Registration report

There is no pre-emptive measure that highlights or prevents customers who become inactive after deposit. However, inactivity is still taken into account during a customer risk assessment or during a withdrawal review, especially if deposit amounts are significant and customer use of the product is deemed abnormal. Depending on the applied risk based approach, and customers' on going activity, they are either de-risked or subjected to further risk mitigating controls. Risk remains as medium risk.

Customer initiates a chargeback request without cause, risk changes and applied controls

- Customer risk assessment
- Customer due diligence
- Customer business relationship termination
- Reporting of suspicious activity

Chargeback risks cannot be fully mitigated as customers can initiate the process using their bank, who fall under their own policies and procedures. During a business relationship customers risk of chargeback is mitigated by risk assessment and due diligence by monitoring card activity and verifying card ownership, if the customer is deemed a high chargeback risk, business relationship is terminated to prevent further chargeback risks. Customers are also subjected to a retrospective risk assessment after confirmed chargeback where if the activity raises concerns from ML/TF/FP perspective, they are raised to MLRO that make a decision whether the customer is to be raised to FIU. Risk remains as medium risk.

4.1.4 Residual payment product operational risks board

| Risk level | | | |
|-------------------------------|--------|--------|------|
| Open loop | | | |
| 3 rd party deposit | | | |
| Multiple accounts on same PM | | | |
| Deposit stacking | | | |
| Inactive post deposit | | | |
| Chargeback | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.1.5 Residual game product operational risk

Customer makes a withdrawal without wagering their deposits, risk change and applied controls

- Customer risk assessment
- Suspension of customer withdrawals
- Procedures in place to verify players wagering
- Enhanced due diligence

Customers can still initiate a withdrawal without wagering their deposits, however their wagering is reviewed during a customer risk assessment or as part of the manual withdrawal process. Withdrawals done through the PNP system automatically detect if customers issued a withdrawal without necessary wagering, disables the automated withdrawal function, customer cannot continue making withdrawals until the situation has been manually reviewed. Non PNP solutions are equally exposed to the risk where it's possible for a customer to issue a withdrawal, without meeting the wagering requirements. Based on an applied risk-based approach, customers are de-risked or if they raise concerns from ML/TF/FP they are subjected to additional risk mitigating controls. Risk remains as medium risk.

Customer is opposite betting risk change and applied controls

- Customer risk assessment
- Game provider reports
- Reporting of suspicious activity
- Customer business relationship termination

There is no pre-emptive control in place that would prevent customers from exercising opposite betting, however once caught either by game provider or during internal risk assessment they are subjected to further risk mitigating controls. If a customer raises concerns from an ML/TF/FP perspective, they are raised to MLRO for further review, who will then decide whether to report the customer to FIU. Risk remains as medium risk.

Customers counting card risk change and applied controls

- Customer risk assessment
- Game provider reports
- Reporting of suspicious activity
- Customer business relationship termination

There is no pre-emptive control in place that would prevent customers from exercising card counting, however once caught either by game provider or during internal risk assessment they are subjected to further risk mitigating controls. If a customer raises concerns from an ML/TF/FP perspective, they are raised to MLRO for further review, who will then make a decision whether to report the customer to FIU. Risk remains as medium risk.

Customer is safe betting risk change and applied controls

- Customer risk assessment
- Game provider reports
- Reporting of suspicious activity
- Customer business relationship termination

There is no pre-emptive control in place that would prevent customers from exercising safe betting, however once caught either by game provider or during internal risk assessment they are subjected to further risk mitigating controls. If a customer raises concerns from an ML/TF/FP perspective, they are raised to MLRO or for further review, who will then decide whether to report the customer to FIU. Risk remains as medium risk.

Customer hedge betting risk change and applied controls

- Customer risk assessment
- Game provider reports
- Reporting of suspicious activity
- Customer business relationship termination

Business is currently cooperating with a sportsbook provider who monitors the issued bets for suspicious activity, which when identified is reported back to the business, so they can conduct their own risk assessment from ML/TF/FP perspective. If there's a risk that the reviewed activity is tied to ML/TF/FP the account will be raised to MLRO for further review who will then decide whether to report the customer to FIU. Risk remains as medium risk.

Customer bets on minimum odds risk change and applied controls

- Customer risk assessment
- Game provider reports
- Reporting of suspicious activity
- Customer business relationship termination

Business applies same controls to mitigate risk of betting at minimum odds than it does mitigating the risk of hedge betting. Risk remains as medium risk.

Customer is Chip dumping risk change and applied controls

- Business is not offering a P2P product

Business is not currently offering products where a customer could conduct chip dumping, which eliminates risks originating from this product entirely. Risk is mitigated from high risk to low risk.

4.1.6 Residual game product operational risk board

| Risk level | | | |
|------------------|--------|--------|------|
| No wagering | | | |
| Opposite betting | | | |
| Counting cards | | | |
| Safe betting | | | |
| Hedge betting | | | |
| Chip dumping | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.1.7 Residual product risk summary

While high risk game products and risks that come with them are de-risked entirely by the business not offering these products currently, business still encounters risks related to high-risk payment products. Due diligence procedures are used to mitigate the risks of allowing customers to conduct high value transactions anonymously, however the risk of open loop remains higher on crypto and other vouchers compared to other payment products as the beneficial owner of the wallet cannot be verified.

4.1.8 Residual customer operational risk

Politically exposed person (PEP) risk change and applied controls

- PEP monitoring
- Customer risk assessment
- Customer due diligence
- Enhanced due diligence

- Customer business relationship termination
- Reporting of suspicious activity

While a customer who is a PEP can still register an account they are regularly screened as a possible match. If a customer is identified as a possible match, they are either discounted as false positive, have further due diligence conducted for verification or confirmed as a match. PEPs do not fall under current business risk appetite, so all confirmed matches will lead to business relationship termination. Risk is mitigated from high risk to medium risk.

Customer under financial sanction risk change and applied controls

- Sanction screening
- Customer business relationship termination
- Customer risk assessment
- Reporting of suspicious activity
- Geo block

Countries and jurisdictions that are under financial sanctions or have sanctioned organizations are automatically deemed high risk by the business and have automated blocks in place that prevent logins and registrations from high-risk countries and jurisdictions. Customer details are also cross-checked with personal details currently in the sanction lists, which would lead to systematic business relationship termination for confirmed matches. Customers identified as a sanction list match are also reported to FIU. Risk is mitigated from high risk to medium risk.

Adverse media

- Customer risk assessment
- Customer due diligence
- Enhanced due diligence
- Customer business relationship termination
- Reporting of suspicious activity

While customers with adverse media can register an account, they are reviewed for any open-source findings during a customer risk assessment. If a customer has adverse information that is considered relevant and raises concerns from an ML/TF/FP perspective, the customer is subject to further risk mitigating controls. Risk is mitigated from high risk to medium risk.

Customer is showing unusual behavior risk change and applied controls

- Business employee training
- Customer risk assessment

- Customer business relationship termination
- Reporting of suspicious activity

Members of staff that interact with the customers directly or indirectly receive training, to ensure they are aware of the current ML/TF/FP risks business is currently facing and what to do in case they come across customers showing suspicious behavior. While customers with unusual behavior risk cannot be fully de-risked, they are subjected to mitigating controls if encountered. Risk is mitigated from medium risk to low risk.

Bribery

- Customer business relationship termination
- Reporting of suspicious activity

Bribery attempts by 3rd parties or customers who business currently has a business relationship with cannot be preemptively prevented since business has public chat communication service and email where anyone can establish communication with member or staff. Internal training provided for the employees verifies that staff members are aware of the accountability when it comes to penalties regarding bribery and attempts are to be reported to MLRO if ever encountered. Business relationship is terminated with the individuals linked to any attempts at bribery and reported to the FIU. Risk is mitigated from high risk to medium risk

Customer tipping off

- Business employee training
- Limited disclosure of ML/TF/FP investigations

Internal training provided for the employees verifies that staff members are aware of the accountability when it comes to penalties regarding bribery and attempts are to be reported to MLRO if ever encountered. Information regarding ML/TF/FP investigation is limited to MLRO, and when relevant to members of the board. Risk is mitigated from High risk to Low risk.

4.1.9 Residual customer operational risk board

| Risk level | | | |
|----------------------------|--|--|--|
| Politically exposed person | | | |

| | | | |
|------------------------|--------|--------|------|
| Person under sanctions | | | |
| Unusual behavior | | | |
| Bribery | | | |
| Tipping off | | | |
| Adverse media | | | |
| Risk level | Low | Medium | High |
| Overall risk | Medium | | |

4.2.0 Residual customer risk summary

After applying customer risk mitigating controls, business is still exposed to medium level of risks that cannot be pre-emptively eliminated upon customer registration. However, business has enough retrospective controls in place to identify the customers high risk activity, which leads to customer being de-risked to a level that aligns with the current risk appetite or customer business relationship is terminated. Overall customer risk is from high risk to medium risk.

5.1 Overall residual risk category description

Overall residual risk measures what general risks remain from each risk category for the business after established controls have been added to the acquisition. The section also provides a description of adverse impacts business can encounter in each risk category.

5.2 Overall residual risk board

| Risk level | | | |
|-------------------|--------------|--------|------|
| Interface risk | | | |
| Geographical risk | | | |
| Product risk | | | |
| Customer risk | | | |
| Risk level | Low | Medium | High |
| Overall risk | Satisfactory | | |

5.3 Overall residual category risk definitions

Low risk

- Risk of revenue loss deemed insignificant amount
- Small or no exposure for systematic money laundering and terrorist financing
- Low risk of regulatory findings

Medium risk

- Small risk of revenue loss deemed significant amount
- Moderate risk of revenue loss deemed insignificant amount
- Moderate exposure for systematic money laundering and terrorist financing
- Moderate risk of regulatory findings

- Low risk of regulatory fine

High risk

- High risk of significant loss of revenue
- High exposure for systematic money laundering and terrorist financing
- High risk of regulatory findings
- Risk of non-compliance
- Moderate chance of regulatory fines
- Reputational damage

5.4 Overall residual risk summary

With current controls in place, the business is not facing a risk of noncompliance that would lead to regulatory fines. However, there are multiple high-risk factors that customers may present, and while these are being assessed, there is an opportunity for the business to enhance the evaluation process further. Strengthening these measures would improve risk management when encountering inherent high risk customers

Full Name: Philip M.
Humme

Signature: *Philip M. Humme*

Date: February 7,
2025

Position: Managing Director obo Allyant Group B.V.

| | |
|-------------------------|--|
| Title | BRA Far Up entertainment |
| File name | Far_up_Entertainment_-_BRA_v1.0__1_.pdf |
| Document ID | 06d7a04ad09ef0a66a18e24dc1a4b5b430332c33 |
| Audit trail date format | MM / DD / YYYY |
| Status | ● Signed |

Document History



SENT

03 / 07 / 2025

21:04:42 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

21:07:56 UTC

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



SIGNED

03 / 07 / 2025

21:08:26 UTC

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



COMPLETED

03 / 07 / 2025

21:08:26 UTC

The document has been completed.