

POLICY

UmiiUmii

Anti-Money Laundering and Counter-Terrorist Financing Policy

UmiiUmii - Anti-Money Laundering & Counter-Terrorist Financing Policy

Version	1.1
Effective Date	20 th of July 2025
Sign Off Date	20 th of July 2025
Document Owner	MLRO

VERSION CONTROL

Next Review Date	20 th of July 2026
------------------	-------------------------------

The policy will be reviewed on the following basis:
No less than once annually, with such review to be initiated by the Policy owner approximately one month prior to the date following 12 months from which the procedure was last approved.

- in response to any changes in relevant regulation and/ or legislation.
- in response to general guidance notes or best practice guidance issued by any relevant regulator.
- in response to any regulatory action taken against any operator by any relevant regulator.
- in response to findings of a relevant internal or external audit; or
- upon request of the management.

NAME	ROLE
Mark Taylor	Money Laundering Reporting Officer

Contents

1. Introduction.....	Error! Bookmark not defined.
2. Regulatory Framework.....	Error! Bookmark not defined.
3. Purpose and Scope	3
4. Understanding Financial Crime.....	4
5. What are the vulnerabilities of the Online Gambling Industry	7
6. How can online gambling be used by criminals for ML/FT?	8
7. ML/FT Indicators or Red Flags	10
8. Understanding Risks	10
9. Risk Management.....	11
10. The Risk-Based Approach.....	12
11. The Customer Acceptance Policy	13
12. Customer Due Diligence	13
13. Enhanced Due Diligence	15
14. Politically Exposed Person.....	15
15. Sanctions	16
16. Obtaining Information on the Purpose and Intended Nature of the Business Relationship	16
17. Reporting Procedures and Obligations	17
18. High Risk Jurisdictions	18
19. Internal Controls.....	18
20. Due Diligence for third parties/Clients.....	19
21. Record Keeping	19
22. Training	19
23. Employee Vetting	20
24. Independent Audit.....	20
25. Policy Distribution.....	20
26. Due Diligence for Third Parties	20
27. Policy URL.....	21
28. Compliance and Consequences of Non-Compliance	21
Appendix 1 – Internal Suspicious Money Laundering Transaction Report.....	21
Appendix 2 – Form to be completed by the Money Laundering Reporting Officer upon receiving the above report from an employee.....	22

1. Introduction

The Anti-Money Laundering and Counter-Terrorist Financing (AML) Policy applies to UmiiUmii who will abide by the gambling licence provided by the Curacao regulations.

This Anti-Money Laundering (AML) policy applies to the Company and all of its staff who provide services that might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.

UmiiUmii are required to have adequate policies, procedures, and controls that identify, assess, and mitigate the risk of Money Laundering/Terrorist Financing. This is fulfilled by implementing the following procedures and controls:

- Policies and procedures which are compliant to the regulatory requirements
- Customer Due Diligence (CDD) is performed upon first withdrawal or at a point a customer reaches total deposits or withdrawals of 2,000 USD, further Enhanced due diligence (EDD) is only performed if considered appropriate based on the risk grading of the customer.
- An Internal and External Suspicious Transaction Reporting (STR) system.
- Document retention procedures.
- Face to Face training as well as online AML Training is provided to all relevant staff at least annually

Further, a robust ML/TF Risk management framework is implemented across markets in order to prevent, detect, and report on suspicious transactions.

2. Regulatory Framework

Below is a list of all the relevant AML legislation and regulations pertaining:

- Curacao Gaming Board Regulations for AML/CFT
- National Ordinance on Identification when rendering services (N.G 2017, no 92)
- NORUT – National Ordinance on the Reporting of Unusual Transactions (N,G 2017, no 99)
- Sanctions National Ordinance (N,G 2014, no 55)
- Kingdom Sanction Act (N,G 2016, no 54)
- National Decree entering into force of Kingdom Sanction Law (N.G 2017, no 2)
- The Code of Criminal Law (Penal Code) N.G 2011, no 48)
- Financial Action Task Force (FATF) and Caribbean Financial Action Task Force (CFATF)
- National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) (NOOGH).
- National Ordinance for Games of Chance (LOK)

3. Purpose and Scope

The company is mandated by the AML directives, as well as National Legislation and Regulations, to identify persons potentially carrying higher risk in order to prevent any misuse of its sites for criminal purposes. This procedure applies to all clients falling under the Curacao licence.

This Policy applies to all employees (and persons of a comparable position) of UmiiUmii, all of whom must understand how money laundering may be conducted so that they can be as alert as possible to

any signs of suspicious behaviour and be able to protect UmiiUmii from breaching its obligations in this area. Any updates made to this Policy are to be duly communicated to all employees.

4. Understanding Financial Crime

Financial crime refers to all crimes committed by an individual or a group of individuals to provide monetary benefits through illegal methods. It ranges from basic theft or fraud committed by ill-intentioned individuals to large-scale operations masterminded by organised criminals across the globe. Regardless of the scale of crime committed, such activities should not be underestimated. Financial crime is a worldwide issue that threatens the integrity of financial systems and the stability of economies and is often linked to violent crimes as well as terrorism.

Technological advancements are facilitating criminals to operate internationally and conduct transactions between banks and different countries more easily. As digital technology continues to evolve, financial crime becomes more sophisticated and harder to detect.

Types of Financial Crime

The most common financial crimes are fraud, tax evasion, money laundering and terrorist financing – all of which are detailed further below.

Identity Fraud

Identity fraud is used by fraudsters to create multiple accounts or to take over existing accounts. In the online gambling world, multiple accounts are usually created to facilitate schemes such as bonus abuse to benefit from new signup bonuses and other attractive promotional offers. Although these marketing promotions are an excellent approach to attracting new players, they can quickly cause revenue loss for the company if exploited drastically by bonus abusers.

Credit Card Fraud

Fraudsters can use stolen credit card information to top up their gaming account, in which case winnings are obtained from illegitimate funds. After the fraudster has used a stolen credit card on the gambling platform, the legitimate cardholder will likely realise what happened and request a chargeback from their banking or credit card provider. The funds will unfortunately get refunded at the gambling operator's expense along with any incurred processing charges and fines.

Chargeback Fraud

Chargeback Fraud, also known as friendly fraud, is when a legitimate customer files a chargeback under false pretences to get their money back. This scheme is often noticed in the online gambling industry whereby players who just lost substantial amounts of money can simply call up their bank, claim that their card was used without their permission, and get reimbursed for their gambling losses.

Tax Evasion

Tax evasion is the illegal non-payment or underpayment of taxes, usually committed by deliberately making a false declaration or no declaration to tax authorities. Some examples include:

- Not declaring or understating taxable income,
- Not paying taxes owed,
- Declaring less income or profits than the amounts earned,
- Overstating deductions, and

- Hiding taxable assets from the authorities.

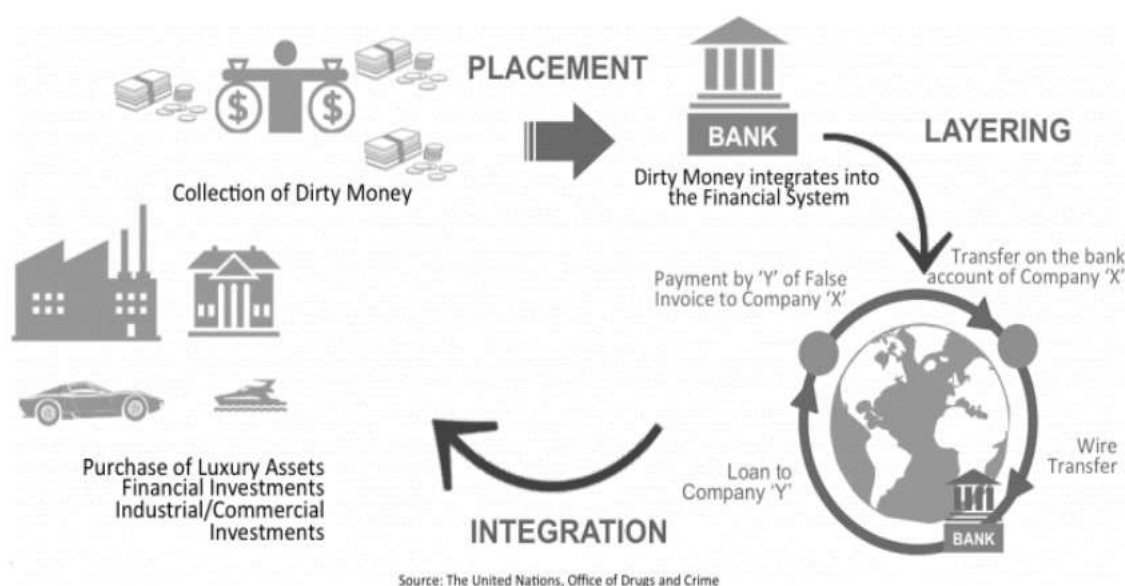
Tax evasion is illegal and those caught are generally subject to criminal charges and substantial penalties. Like fraud, tax evasion can also be a predicate offence for money laundering.

Money Laundering

Money Laundering (hereinafter “ML”) is generally understood to be the process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly derived property or funds to make them appear legitimate.

When a criminal activity generates substantial revenue, the involved individual and/or group would need to find a way to control the funds without attracting attention to the underlying activity and/or the persons involved. To achieve this, criminals disguise the sources, change the form, or move the funds to a place where they are less likely to attract attention. This process enables the criminals to make seemingly legitimate economic use of their criminal proceeds.

Conventionally, it is recognised that money laundering occurs in three key stages i.e., placement, layering, and integration. However, it is crucial to keep in mind that the three-stage model (illustrated below) is reflective of organised crime and does not reflect a large proportion of money laundering that impacts gambling.



Placement

Placement involves the physical disposal of cash or other assets derived from criminal activity. This process begins with the collection or generation of proceeds derived from criminal activity. This so-called “dirty money” is placed into the financial system usually by breaking up large amounts of cash into less conspicuous, smaller sums and placing these funds into circulation through formal financial institutions and other legitimate businesses, both domestic and international.

This is the most vulnerable stage in the laundering process as it is the stage at which the proceeds of crime are most apparent and hence, most easily detected.

Some examples of placement transactions include but are not limited to:

- Mixing illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned restaurants.
- Placing cash in small amounts and depositing it into numerous bank accounts in an attempt to evade reporting thresholds.
- Purchasing foreign exchange with illegal funds.
- Repayment of legitimate loans using cash derived from criminal activity.

Layering

Once the money has been placed in the financial system, layering (sometimes referred to as structuring) starts taking place as the launderer engages in a series of conversions or movements of the illicit funds to distance them from the source. The layering stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to conceal the source and ownership of the funds.

Some examples of layering transactions include but are not limited to:

- Transferring the proceeds from the bank account to a holding company.
- electronically moving funds from one country to another and dividing them into advanced financial options and/or markets.
- Moving funds from one financial institution to another or within accounts held with the same institution.
- Paying the proceeds to a company in order to pay a false invoice.
- Making a private loan to another company.
- Placing money in stocks, bonds, and life insurance products.

Integration

Integration constitutes the third stage of the ML Process whereby the launderer seeks to grant apparent legitimacy to illicit funds through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. It therefore provides launderers with the opportunity to increase their wealth with the proceeds of crime.

Some examples of integration transactions include but are not limited to:

- purchasing luxury assets, like real estate, artwork, jewellery, or high-end automobiles.
- the funds are used to purchase goods and services, invest in businesses or financial services, and are therefore made to look legitimate.
- Investments that can be made in business enterprises through financial arrangements or other ventures.

Integration is generally difficult to spot unless there are great discrepancies between an individual's or company's legitimate employment, business or investment ventures and an individual's wealth or a company's income or assets.

Funding of Terrorism (hereinafter "FT")

The Funding of Terrorism (also referred to as "Terrorist Financing") is the process of making funds or other assets available to support, directly or indirectly, terrorist activities. Such a process in fact comprises two separate types of financial activity:

- Money and other assets generated by acts of terrorism; and
- Money and other assets intended to fund acts of terrorism (including the promotion of terrorism and the radicalisation of individuals).

The funding of terrorist activity, terrorist organisations or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. In fact, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations. Although one may fairly assume that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the terrorist group and its legitimate funding sources. As a result, terrorists must similarly find ways to manage these funds in order to be able to use them without drawing the attention of authorities.

Another difference between terrorist financing and money laundering is the ultimate goal. While the money launderers move or conceal criminal proceeds to obscure the link between the crime and the generated funds and avail themselves of the profits of crime, the terrorists' ultimate goal is not to generate income from the fund-raising mechanisms, but to obtain resources to support terrorist operations.

Whilst there is a difference in goals between terrorism and other criminal activity, terrorists still require financial support to achieve their aims. Like any criminal organisation, a successful terrorist group is therefore one that is able to build and maintain an efficient financial setup. Terrorists and their organisations need funding for multiple purposes, including but not limited to recruitment, training, weapons, travel, material, and protection.

Like other criminal activity, a large proportion of the terrorist funding originates in cash which is then laundered. Terrorists often control funds from a variety of sources around the world and make use of increasingly sophisticated techniques to move these funds between jurisdictions. Therefore, identifying the transmission of money to finance terrorist activity as it moves through the finance and business sectors can be quite challenging. Nonetheless, disturbing the financial support for terrorism creates complications for their operations and places further importance on the significance of intelligence in protecting national and international security and upholding the integrity of national and international financial systems. Such intelligence can be obtained by gaining insight into their financial transactions and dealings and tracking the flow of funds to obtain information on links, profiles, and movements.

5. What are the vulnerabilities of the Online Gambling Industry

Although gambling is intended to be a leisure industry, its correlation with crime and money laundering is inevitable. The main vulnerabilities related to online gambling are detailed below

Non-face-to-face nature of online gambling

Because players are not physically present for verification of identity purposes, there is a heightened risk of identity fraud which consequently renders the CDD procedure more complex

The rapidity and cross-border nature of transactions

Inarguably, the rapidity and cross-border nature of transactions can be a very appealing factor for criminals to exploit. However, there are opposing views on the traceability of online gambling transactions. While some argue that tracing of such transactions may prove to be problematic in certain instances, others contend that ML/FT risks through online gambling are minimised as financial transactions are conducted electronically and are therefore easily traceable.

The risk of an ‘open loop’ system

Online gambling operators that credit winnings or unused funds to an account different from the account through which funds were originally deposited into the gambling account, may unknowingly launder illegally obtained funds. Such an operation is commonly referred to as the “open loop system.” Although licensed online gambling operators are not allowed to perform such operations, complications may arise when funds are initially deposited through, for instance, a MasterCard account which does not allow for inward transfers of funds.

Reliance on Financial Sector

There is a common assumption that because online gaming transactions are largely conducted through the financial sector, ML/TF risk is considerably reduced due to the additional layer of preventative measures in detecting ML/TF activities. However, such notion overlooks the fact that banks do not have access to certain information on the player (such as player’s gambling pattern) and are therefore not in a position to identify every possible ML/TF suspicion related to a player.

The shift to alternative payment services

Over the years, the online gambling industry has witnessed increasing numbers of financial institutions blocking credit card transactions related to online gambling which has consequently increased the demand for alternative payment methods such as prepaid cards and e-wallets. Because they are considered to be less traceable means of payments, UmiiUmii recognises its duty to ensure that the players funds are deposited through alternative payment services provided by regulated entities which are subject to adequate AML/CFT measures.

6. How can online gambling be used by criminals for ML/TF?

Criminals continuously seek to find ways of disguising their ill-gotten funds as an attempt to make any dealings of illegal activity appear to be clean and legitimate assets. Like any other service sector, online gambling operators are often targeted by criminals as a means to conceal the illicit funds through their platforms.

Several studies have identified a number of ML/TF typologies showing the various techniques, schemes, and instruments criminals use to launder illicit funds through the online gaming industry. Understanding these typologies is crucial for UmiiUmii to be able to look out for a set of indicators or red flags when carrying out its compliance obligations and hence, be effective in its fight against financial crime and ensure regulatory compliance.

UmiiUmii recognises that money laundering and terrorist financing typologies are always evolving and therefore acknowledges that its compliance team should always be looking to update and learn more typologies, focusing on those most relevant to its sector.

ML/FT Typologies

Below is a list of typologies that have been compiled from reports issued by international regulatory organisations:

‘Mule’ Accounts

‘Mule’ accounts are created via the misuse of personal details belonging to third-party individuals (referred to as ‘money mules’). Their personal data can be used to open online gambling accounts, bank accounts and/or e-wallet accounts with payment service providers. Studies show that the most targeted

individuals are students, unemployed individuals, newcomers to a country and people in economic distress, particularly young men under 35 years.

Match Fixing

Match fixing can be defined as the illegal influencing or alteration of the course or result of a sports event with the intention of achieving a predetermined result and is mainly committed for financial gain. It can involve asking a player to intentionally miss a shot, telling a referee to call more fouls against a certain team, or asking a coach to bench a specific player.

Match fixing in sports is being increasingly used by criminals as a means of laundering substantial amounts of illicit proceeds and is becoming a serious threat to the integrity of sports. According to Europol, "high illegal gains are secured through the execution of an extended series of manipulated matches for betting purposes." The most 'professional' method used by criminal groups is to buy a club (particularly one in the lower division which may be heavily affected by financial problems) or sponsor it to an extent of gaining effective control over the team, with the sole purpose of fixing matches and laundering money. Studies show that football is the most targeted and manipulated sport by international organised crime groups because of its worldwide popularity, financial dimension, and large turnover.

Fixed Odds Hedging

Hedging is a scheme commonly used in sports betting but is also possible in baccarat, roulette, and blackjack. It is a strategy in which a bet is placed on a second wager against the original bet when they are unsure that the outcome of a wager will be a win. The intention of a hedge is generally to guarantee a profit, or at the very least, reduce or eliminate the potential loss. Simply put, hedging is a form of "insurance" that reduces the odds in favour of losing and increases the chances of winning.

False Identity and Minimal Gambling Activity

Ill-gotten funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses, the funds are then transferred from the gambling account to a legitimate bank account.

Collusion

A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. Professional gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.

A money launderer, in collusion with an operator of an offshore gambling website, deposits illicit funds in the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.

Other Typologies

- Criminal ownership, infiltration, or coercion of an online gambling licensee to either launder on an ongoing basis or to launder a limited number of large transactions before simulating business failure and surrendering the licence.
- Use of an online gambling platform as an informal payroll, banking system or money/value transfer system for criminals or terrorists (including use by PEPs to transfer value across borders where currency controls exist).
- Introduction of criminal proceeds to an online gambling platform by gamblers who steal money to fund gambling.

- Use by hackers of stolen passwords to transfer value from hacked online accounts to other withdrawal methods or accomplices.
- Use of numerous funding methods with the intention of confusing audit trails.
- Attempts to use gaming accounts to disguise funds from sanctioned businesses.
- Use of e-wallets and prepaid cards to mask transactions.
- Proxy servers and use of Virtual Private Networks (VPNs) which disguise the user's physical location.

7. ML/TF Indicators or Red Flags

ML/ TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. They typically result from one or more factual characteristics, behaviours, patterns, or other contextual factors that identify irregularities or inconsistencies with what is expected of the customer based on what is known about them.

Indicators by themselves may not always lead to a reasonable suspicion of criminal activity but they can prompt a risk assessment through which one will be able to determine whether there are further facts, contextual elements or additional red flags that might assist in establishing reasonable grounds to suspect the commission or attempted commission of an ML/TF offence. These ML/TF indicators provide valuable information from a financial intelligence perspective and are usually used to explain the rationale for filing a Suspicious Transaction Report (hereinafter “STR”).

The following is a non-exhaustive list of possible red flags one must look out for:

- Customers display suspicious gambling behaviour, particularly on higher risk games.
- Customer does not cooperate in the carrying out of CDD.
- Customers attempt to register more than one account with the same licensee.
- Customers deposit considerable amounts during a single session by means of multiple prepaid cards.
- Customer deposits funds well in excess of what is required to sustain usual betting patterns.
- Customers make small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customers make frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to transactions carried out in the past.
- Customers carry out transactions which seem to be disproportionate when seen in the context of what is known about the customer’s wealth, income, or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.

8. Understanding Risks

Money Laundering and the Funding of Terrorism carry a wide array of risks, regardless of whether a business is seen to be complicit or negligent. UmiiUmii therefore recognises that in case of non-compliance or negligence of AML/CFT regulations, it may face regulatory, legal, financial, and reputational risks, all of which are interdependent:

- Regulatory risk comes from failure to meet regulatory rules which may result in loss of licence, increased regulatory visits, increased regulatory scrutiny, and/or sanctions against the organisation.
- Legal risk occurs if an organisation contravenes local laws in its conduct of business (e.g., sanctions breaches or allowing a customer to launder money through an account within the organisation) or faces a civil lawsuit from dissatisfied customers (e.g., customer's personal data has been stored securely). Its outcome could involve disqualification of directors, sanctions against the organisation, criminal charges against the organisation and/or staff.
- Non-compliance or negligence of AML/CFT regulations also results in financial risks which mainly come from the time and money it takes for the business to undergo a regulatory investigation, resolve a failed regulatory inspection, defend legal actions, replace money lost to criminals, or undergo a criminal prosecution. Consequences of financial risks could involve fines from the regulator, criminal convictions and fines, loss of position within the organisation due to gross misconduct or gross negligence, loss of business due to proceedings against the organisation and bad publicity, and/or being required to pay money back to innocent parties.
- Reputational risk comes when an institution is recognised as having weak controls and is therefore targeted by criminals. Such risk may result in negative comments on blogs and forums, damaged reputation throughout the industry, and/or loss of business and a decrease in customers due to reduced trust.

9. Risk Management

UmiiUmii recognises that consideration of both inherent and residual risk is one of the most important aspects of risk management.

Inherent Risk

Inherent Risk is the risk that UmiiUmii is exposed to before adopting and applying any measures, policies, controls, and procedures to mitigate the same. The level of inherent risk that UmiiUmii is exposed to is determined by likelihood (how likely it is for UmiiUmii to be exposed to such risk) and the impact (how big would the impact be on the business should UmiiUmii be exposed to such risk).

As a remote gambling operator, UmiiUmii is inherently exposed to the following risk factors:

- Customer Risk
- Geographical Risk
- Product, Service, and Transaction Risk
- Interface or Delivery Channel Risk

Mitigating Measures

Risk mitigating measures are applied on a risk-sensitive basis and involve the development and implementation of strategies, policies and procedures that are targeted at moderating the identified risks to which UmiiUmii is exposed too:

- Some of the risk mitigating measures that UmiiUmii implements include but are not limited to:
- Strengthening and implementing its internal controls and measures commensurate to the risk posed.
- conducting the correct level of Customer Due Diligence ("CDD") and ongoing monitoring in line with the customer's risk profile.
- Prohibiting customers that fall outside of UmiiUmii risk appetite.
- Training and awareness for UmiiUmii's employees and contractors.

- keeping abreast with any developments in AML/CFT legislation and internationally identified risks and typologies.
- Appointing a trained, skilled, and experienced MLRO as well as compliance officer(s).
- Implementing a culture of effective internal reporting and external reporting.
- Implementing an independent audit function to occasionally test UmiiUmii's internal measures, policies, controls, and procedures.

Residual Risk

Residual Risk is the risk that remains after the implementation of its controls. UmiiUmii's recognises that determining the residual risk is crucial in:

- Considering whether the remaining risk falls within the risk appetite of the company

UmiiUmii will ensure the Business Risk Assessment is documented and approved by the board of Directors. The assessment will cover:

Considering whether the remaining risk falls within the risk appetite of the company

- The Methodology adapted
- The reasons for considering a risk factor as presenting a low, medium, or high risk
- The outcome of the BRA
- Any information sources used.

10. The Risk-Based Approach

Pursuant to the PMLFTR, UmiiUmii's is obliged to adopt and implement a series of measures, policies, controls, and procedures on a risk-sensitive basis through the adoption of a risk-based approach. This means that UmiiUmii must identify, assess, and understand the ML/FT risks to which it is exposed to, and take the appropriate mitigation measures commensurate to the level of risk. In this way, resources are applied where most needed.

UmiiUmii recognises that a risk-based approach can be effectively adopted after it understands and assesses the risk that its business is generally exposed to as well as the specific risk that it exposes itself to when establishing individual business relationships with its customers.

The Customer Risk Assessment (hereinafter "CRA")

UmiiUmii recognises that the provisions of its CAP can only be applied once it has understood the risk inherent in a particular business relationship. For this reason, UmiiUmii has to carry out an assessment of the particular risks it will be exposed to in providing its services or products throughout a business relationship to specific customers linked to particular jurisdictions through one or more channels (i.e., the Customer Risk Assessment).

UmiiUmii understands that the level of detail of a CRA must reflect the complexity of the business relationship and the information collected to draw up the CRA formulates the customer's risk profile. Based on the CRA, UmiiUmii will apply the proper level of CDD depending on the risks identified.

UmiiUmii when conducting a customer risk assessment will assess these four risk areas:

- Product, service, and transaction Risk
- Geographical Risk.
- Customer Risk.

- Distribution channels Risk.

11. The Customer Acceptance Policy

UmiiUmii has a Customer Acceptance Policy in place that provides a description, with non-exhaustive examples, of:

- The type of customers that are likely to pose a higher-than-average risk of ML/FT.
- The risk indicators that will lead to a business relationship being considered as presenting a low, medium, or high risk of ML/FT.
- The level of CDD measures, including ongoing monitoring to be applied in their relation.
- The circumstances under which UmiiUmii will decline to service someone.

12. Customer Due Diligence

Customer due diligence refers to the processes used by different organisations to collect and evaluate relevant information about their customer(s) for the purpose of knowing who their customers are and being able to build customer profiles.

UmiiUmii acknowledges that the implementation of a robust CDD programme is key to safeguarding its services and products from being misused and ending up as conduits for proceeds of crime or being used for ML/FT purposes, as well as to assist the FIU and law enforcement authorities in carrying out their responsibilities of analysing and investigating cases of ML/FT effectively.

As part of its CDD process, UmiiUmii shall ensure that it has adequate mechanisms in place:

- Determine who the customer and, where applicable, any beneficial owner is,
- Verify whether that person is the person s/he purports to be,
- Establish the purpose and intended nature of the business relationship, and
- Monitor that relationship on an ongoing basis.

UmiiUmii recognises that the application of its CDD measures shall be done to an extent determined on a risk-sensitive basis.

Simplified Due Diligence

Identification takes place by obtaining the personal details and other relevant information in relation to that person upon registration. At registration, UmiiUmii requires the following information on each player (also known as simplified due diligence/SDD):

- Name and surname.
- Place and date of birth.
- Permanent residential address.
- Identity reference number.
- Nationality

UmiiUmii recognises that customers will sometimes open duplicate accounts and that the same can be used to avoid hitting various AML triggers. UmiiUmii has in place that ensures that a customer cannot sign up with the same details.

The company in high-risk scenarios will collect all personal details as necessary to mitigate the higher risk of ML/FT.

CDD Process

UmiiUmii is required to obtain documentation upon a customer reaching a total deposit or withdrawal of (4,000 NAF) 2K USD. The reasons for carrying out customer due diligence are outlined below:

- To be satisfied that the customer is who he says he is.
- To determine whether the customer is acting on behalf of others; and
- To guard UmiiUmii against being used for fraud, money laundering, or other criminal activity.

UmiiUmii may request documentation from the customer before reaching this threshold depending on the risk level of the customer.

By following a risk-based approach, the appropriate due diligence can be applied to such a customer. This means that the higher the ML/FT risk is, the greater the level of due diligence will be applied.

Once the (4,000 NAF) 2K USD threshold has been met UmiiUmii will restrict the customer from making further deposits and processing withdrawals from their gaming account.

UmiiUmii will terminate the business relationship within 30 days from the moment the CDD threshold has been met and report the transaction to the FIU.

Due Diligence documentation:

In order to verify the details on their player account, The company will request the customer to provide a copy of one document from each of the categories listed below:

Personal identification

- Valid Passport
- Valid Driving Licence
- Valid National Identification Document (Picture ID)

Where any such document does not allow verification of one's residential address, the following documents will be requested.

Address verification

- Utility Bill, which is less than 3 months old. Mobile phone bills are not sufficient. The bill provided must pertain to a service delivered to the address provided.
- Tax Bill, which is less than 3 months old
- Copy of Bank Statement, which is less than 3 months old

Source of Payment Verification

When we are unable to verify the ownership of the payment method, UmiiUmii requires the customer to provide:

- Registered credit/debit card (Front only) or e-wallet.
- Account statement of payment registered with the account

13. Enhanced Due Diligence

UmiiUmii will apply a risk-based approach and the business conducts more thorough checks for higher-risk customers and enhanced due diligence is requested when the customer's transactions or activities appear unusual. UmiiUmii will request documents from where the risks of ML/FT are higher, for example:

- Residents of higher-risk geographic areas
- Politically exposed persons
- Products or transactions that might favour anonymity
- Suspicions that the customer may be involved in money laundering/terrorist financing.

The company may initiate enhanced due diligence documentation as part of any account review.

In order to verify the customer's source of wealth/funds, UmiiUmii will request the customer to provide any of the categories listed below:

Acceptable Enhanced due diligence documentation

- Payslips.
- Bank statement showing salary being received.
- Tax Return.
- Company's financials.
- Savings.

UmiiUmii may request additional documents depending on the person's occupation and activity on the account.

14. Politically Exposed Person

A PEP is defined by the Financial Action Task Force ("FATF") as an individual who is or has been entrusted with a prominent public function. The definition of PEP applies to both foreign and domestic PEPs, international organisation PEPs, as well as to family members and close associates of the PEPs. Please see the below table for more details:

Foreign PEPs	individuals who are or have been entrusted with prominent public functions by a foreign country, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials.
Domestic PEPs	individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
International organisation PEPs	persons who are or have been entrusted with a prominent function by an international organisation, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors, and members of the board or equivalent functions.
Family members	individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of Partnership.

Close associates	individuals who are closely connected to a PEP, either socially or professionally.
------------------	--

Studies show that due to their position and influence, PEPs are in positions that can potentially be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing. In recognition of these risks, UmiiUmii has adopted a business-wide strategy of not accepting players who are identified as PEPs and/or PEPs by association at the registration stage.

UmiiUmii will conduct politically exposed person checks upon reaching total deposits of (4,000 NAF) 2K USD and rescreens customers through this list regularly as part of on-going monitoring.

15. Sanctions

UmiiUmii recognises that, besides its obligations under the Curacao regulations, it also has obligations relating to sanctions screening, freezing of assets, and reporting.

Sanction screening is key for an effective financial crime compliance programme as it assists with the identification of sanctioned individuals and/or entities, and illegal activity to which persons may be exposed to. As a subject person, UmiiUmii is obliged to have effective policies and procedures for sanctions screening in order to be able to detect, prevent, and manage sanctions risk. In recognition of this, UmiiUmii will screen customers against sanctions lists issued - amongst others - by the United Nations, European Union, and the United States Office of Foreign Assets Control ("OFAC") and shall ensure that:

- under no circumstance should business be conducted with sanctioned persons,
- employees are aware that tipping off is strictly prohibited, and
- in the event of a hit, an STR will be submitted to the Curacao FIAU.

Furthermore, UmiiUmii acknowledges the importance of keeping abreast of any sanctions that may be imposed from time to time along with any guidance, notices, decisions, recommendations

UmiiUmii will conduct a sanction check upon establishing a business relationship in line with regulatory requirements and rescreens customers through these lists regularly as part of on-going monitoring.

To comply with the United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. Upon notification of a sanctioned person playing on any of the sites across the group, any funds held on the gaming account with frozen and reported to the FIU immediately.

16. Obtaining Information on the Purpose and Intended Nature of the Business Relationship

UmiiUmii to develop a customer risk profile and collect sufficient information to allow the business to detect unusual activity in the course of the relationship, and when necessary, documentation to establish customer's source of wealth including the expected level of activity.

To this end, UmiiUmii will require the customer to complete a declaration from the customer to provide relevant information when information cannot be found via social media when the customer is not identified as high-risk.

In situations where the customer poses a high risk of ML/FT or has doubts over as to the veracity of the information collected, the information will be substantiated by independent and reliable information and documentation.

The purpose of developing a customer business and risk profile, allows UmiiUmii to scrutinise customer's activity as part of ongoing monitoring.

17. Reporting Procedures and Obligations

The Money Laundering Reporting Officer/Compliance Officer.

In accordance with regulations, UmiiUmii shall appoint (and ensure that such appointment remains at all times) an MLRO/Compliance Person to establish and review internal controls and procedures, to monitor compliance with the relevant legislation, regulations, policies, and procedures and to provide a central point of contact for reporting suspicious activity. The MLRO/Compliance Person's core functions are to:

- Receive reports on information or matters that may give rise to knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT,
- Consider these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT,
- Report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIAU, and
- Respond promptly to any request for information made by the FIU.

Due to the serious confidentiality obligations and the level of responsibility of the MLRO/Compliance person, the appointed person shall be a level of seniority who either sits on the Board of UmiiUmii or reports directly to the Board and shall be afforded every assistance and cooperation by all employees and senior management when performing their duties.

Internal Reporting

UmiiUmii shall put in place internal reporting procedures that clearly set out the steps to be followed when an employee of UmiiUmii becomes aware of any information or matter that in his/her opinion gives rise to knowledge or suspicion that a person or a transaction is connected to ML/FT

The procedures should clearly state that, when an employee becomes aware of any such information or matter, s/he shall treat the case with the utmost urgency and shall report the matter to the MLRO/Compliance officer without any delay. In light of this, UmiiUmii shall ensure that all employees are informed of the identity of the appointed MLRO/Compliance officer (and of the designated employee) to whom the report has to be made.

To ensure there is no tipping off, employees and senior management will not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU.

External Reporting

UmiiUmii acknowledges that, when the MLRO or the designated employee determines that UmiiUmii knows, suspects, or has reasonable grounds to suspect that:

- A transaction (including attempted transactions) may be related to ML/FT; or
- A person may have been, is, or may be connected with ML/FT; or
- ML/FT has been, is being, or may be committed or attempted.
- The customer is identified as a sanctioned person
- The customer fails to provide customer due diligence or documentation is identified as unusual.

UmiiUmii will consider filing a suspicious transaction report when:

- The customer is identified as a politically exposed person
- The customer is a resident from a high-risk jurisdiction
- The customer refuses to provide source of wealth documents

The MLRO/Compliance officer is under the obligation to file a suspicious transaction report ("STR") with the FIU. Any disclosures should be made to the FIU promptly, meaning that a suspicious transaction report should be submitted on the same day when knowledge or suspicion of ML/FT is considered to subsist by the MLRO/Compliance officer unless it relates to certain cases that prove to be more challenging due to the extensive volume and/or complexity of information/documentation that may be provided, in which case, the FIAU allows for the MLRO/Compliance officer to submit the STR within the shortest time possible (as long as the delay was not caused by lack of resources).

18. High Risk Jurisdictions

High-risk countries are those countries identified as such by publications issued from time to time by the Financial Action Task Force, or additionally those identified by the regulators. Players from the FATF list of jurisdictions are seen to threaten the international financial system from ongoing and substantial money-laundering or terrorist financing activities, as identified from FATF publications, will be refused.

Other countries may be considered to be high-risk but will not necessarily be refused. Players residing in such jurisdictions will be subject to monitoring. UmiiUmii relies on the following websites to determine the risk of a country

- FATF Jurisdictions under Increased Monitoring.
- FATF High-Risk Jurisdictions subject to a Call for Action.
- EU List identifying high-risk 3rd countries with strategic deficiencies.
- The US Department of State Money Laundering Assessment (INCSR).
- Basel AML Index.

To mitigate the risk, UmiiUmii will not accept customers that resides in high-risk countries or are in line with the risk appetite of the business.

19. Internal Controls

UmiiUmii carries out ongoing monitoring of the business relationships with players in order to ensure that:

- Documents, data, or information held on the player is kept up to date.
- Transactions are scrutinized.

Documents, data, or information is kept up to date.

To ensure that all documents, data, and information are kept up to date, all player accounts are subject to a review. Accounts are periodically reviewed throughout their lifetime and also upon withdrawal, where all documents are checked and if documents are expired, new valid documents will be requested. Upon discovery/recognition that verification documents are expired, withdrawals will not be processed until valid documentation is provided to UmiiUmii.

Scrutiny of Transactions.

Transactions are monitored and when certain trigger events occur, the employee will investigate the relationship with the player and determine whether documentation or any other action is needed. UmiiUmii generates the following reports and checks the players on such reports manually:

Behaviour/Transaction Monitoring thresholds

At UmiiUmii we have several technical features and rules that are set up to limit AML risks where transactions are involved along with Deposit and Withdrawal procedures. Below are a number of rules that apply to each customer account:

- Third party funding.
- Customers linked by the same residential address or IP Address.
- Large Deposit thresholds.
- Large Withdrawal requests.
- Accounts funded with multiple payment methods.
- Large Deposits with anonymous payment methods.
- Enforcement of closed loop.
- Failed Card deposits

UmiiUmii will terminate the business relationship with the customer when notified by the game provider when the person's gameplay is deemed suspicious.

20. Due Diligence for third parties/Clients

UmiiUmii has processes in place when applicable, to carry out due diligence upon establishing a business relationship in line with our regulatory requirements. To ensure that the company only works with reputable entities.

21. Record Keeping

UmiiUmii shall retain all relevant records in line with the legal requirements set out by each jurisdiction in which it is licensed and shall ensure that all decision-making is appropriately and centrally recorded so that internal checks and audits can be undertaken on AML/CFT to ensure compliance and identify risks and required improvements in the field of AML/CFT.

22. Training

UmiiUmii shall retain all relevant records in line with the legal requirements set out by each jurisdiction in which it is licensed and shall ensure that all decision-making is appropriately and

centrally recorded so that internal checks and audits can be undertaken on AML/CFT to ensure compliance and identify risks and required improvements in the field of AML/CFT.

UmiiUmii acknowledges that AML/CFT training is an essential component to raising awareness on ML/FT risks and observing methods potentially related to ML/FT in the gambling industry. It is therefore fundamental that UmiiUmii provides training to all employees at the outset of employment, with regular refresher courses to support and enhance their learning. Such training should be reviewed periodically to ensure that it remains:

- relevant to UmiiUmii AML/CFT Policy and associated Procedures, and
- up to date with the latest legislative and regulatory developments

Furthermore, UmiiUmii shall ensure that all employees are suitably trained in AML/CFT as relevant to their role. Examples of such relevant training could include:

- Assisting those responsible for onboarding external partners
- Training customer facing employees (customer service, VIP managers) in identifying data or customer behaviours which exhibit money laundering.
- All new employees who handle customers or their transactions, irrespective of their level of seniority.

UmiiUmii also encourages employees to share learning in a non-formal manner by sharing experiences where internal lessons have been learned regarding AML/CFT practices.

23. Employee Vetting

UmiiUmii follows high ethical standards in the recruitment of all its staff. This includes taking prospective employee's professional backgrounds into account, performing background checks, obtaining a certificate of good conduct from the local police authority, and verifying references provided, as per HR processes.

24. Independent Audit

UmiiUmii in line with regulatory requirements will conduct an internal audit through either an internal audit department or an outside independent party.

25. Policy Distribution

All employees receive a copy of the AML policy and other associated policies upon induction, and each year, once a review is completed and signed, the new AML documents is circulated to all staff, including subcontractors and Third-party suppliers when applicable by email, including a summary of any material changes.

26. Due Diligence for Third Parties

The company has processes in place, when applicable, to carry out due diligence upon establishing a business relationship in line with our regulatory requirements and to ensure that the company only works with reputable entities.

27. Policy URL

This policy cannot be accessed online through the company website.

28. Compliance and Consequences of Non-Compliance

The company is obligated to apply to all regulations covered under section 2 of the regulatory framework within this policy. Should Trent Tech Group violate these regulations, the company can be subject to disciplinary actions, legal implications, or business risks.

In situations of non-compliance, the following actions could be taken:

- The company will be subject to regulatory fines
- Regulatory enforcement.
- Respective action on particular regulations and processes.
- License revoked.
- Assess adequately the risk of money laundering or terrorist financing

Contact Information

Any questions regarding this policy, please contact:

Name – Mark Taylor
E-mail Address – markt@diligenzagroup.com
Contact Number - +356 99911164

Appendix 1 – Internal Suspicious Money Laundering Transaction Report

To: The Money Laundering Reporting Officer
Date of the report: [Insert date]
Prepared by: [Insert name and position]
Name & Player ID of individual(s) suspected: [Insert name of all individuals suspected]

Name & Player ID of client (if different): [Insert client name or confirm that no difference from the list above]
Reason for suspicion: [Give a detailed description of the reasons for your knowledge or suspicions. Please include supporting documentation if applicable]
Date suspicion first aroused: [insert date]
Names of all other colleagues who have been involved with this client’s affairs: [Insert name of all individuals informed – each of whom should sign the declaration below]

Declaration

I am aware of the risks and penalties regarding “tipping off”, or investigation of the above or related matters by the authorities.

Name:	Signed:	Dated:

Date received _____
Consideration of Disclosure:

Appendix 2 – Form to be completed by the Money Laundering Reporting Officer upon receiving the above report from an employee.

Are there reasonable Grounds for suspicion?

Is consent required from the Financial Intelligence Unit (FIU) to any ongoing or imminent transactions which would otherwise be prohibited acts? • YES • NO
--

If YES, please record authorisation and “way forward” details received from the Financial Intelligence Analysis Unit

If there are reasonable grounds to suspect Money Laundering, but you do not intend to report the matter to the FIU, please set out below your reasons for non-disclosure

Signed _____ Dated _____

THIS REPORT SHALL BE RETAINED FOR A MINIMUM OF FIVE (5) YEARS

