

Anti Money Laundering Policy
Carletta N.V.
Registration number 142346

1. Introduction

1.1 Money Laundering

Money Laundering (ML) is the process of creating the appearance of funds obtained from criminal activity, such as drug trafficking or terrorist activity, being originated from a legitimate source. Criminals attempt to launder money by disguising the source and/or changing the form of the funds, or moving them to a place where they are less likely to attract attention.

1.2 Anti-Money Laundering

Anti-money laundering (AML) is a financial/legal term used to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report ML activities.

An effective AML program requires a jurisdiction:

- To have criminalized Money Laundering
- To have given the relevant regulators and police the powers and tools to investigate it
- To have its financial institutions identify their customers, establish risk-based controls, keep records and report suspicious activities
- To be able to share information with other jurisdictions as appropriate

2. Regulation

Employees working in the remote gaming industry are required to make a report in respect of information that comes to them in the course of their business:

- When they know
- When they suspect
- When they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend.

These obligations are collectively referred to as grounds for knowledge or suspicion. What the authorities are looking for is that we are able to demonstrate, with supporting evidence, that a risk assessment is and has been undertaken prior to entering into business relationships with customers and that adequate customer due diligence is conducted in order to ensure that customers' transactions are consistent with the level of risk presented.

The Merchant must be able to demonstrate that the extent of the ongoing monitoring undertaken is conducted on a risk-sensitive basis and that all the records are retained by us to reflect this, with risk profiles being properly maintained. In this document, we have identified additional measures that are being applied in order to carry out risk monitoring

and the need of where we would require a Declaration of the source of funds from customers in situations which present a high risk and potentially money laundering.

2.1 Specific Regulations

The Merchant is committed to ensuring that compliance is embedded in all aspects of our business and licensed Curacao Gaming License that allow the operations of Games of Chance on the International market via service lines.

3. Crime & Disorder and AML policy

AML policy is based on principles and practises:

- We develop systems and controls that are appropriate for our businesses and comply with legal and regulatory requirements
- We assess the AML risks inherent in our current business at least annually; we then adopt a risk-based approach that is flexible, effective, proportionate and cost effective
- We have full commitment for this from, and responsibility resting with, senior management
- We regularly assess the adequacy of our systems and controls
- We maintain, where necessary, records of transactions that meet the needs of law enforcement investigations tackling money laundering and terrorist financing
- We provide initial and ongoing training for all relevant employees
- We support the nominated officer with resources and authority to operate objectively and independently

4. Risk Management

We have a policy and procedures in relation to risk assessment and management, as required under the Money Laundering Regulations 2007 (the Regulations). This risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks we face:

- Identify the money laundering and terrorist financing risks that are relevant to us
- Design and implement policies and procedures to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls
- Record what has been done, and why

This risk-based approach focuses the effort where it is most needed and will have most impact. It has the full commitment and support of our senior management, and the active co-operation of all employees. We have conducted an assessment of our business risk exposure to money laundering, which considers the threat, and its impact.

5. Suspicious Activity

Suspicious Activity in this case is being referred to as suspicious transactions, extreme player profiles, when deposits are not matching up amongst other elements. Other concrete examples of how we identify players who require our team to undertake a risk monitoring approach of our customers and when to specifically carry out enhanced due diligence checks on the Player Profiles can be further required:

1. Passport or ID card.
2. Utility bill.
3. Bank statement.
4. Other proof of identity.

The Enhanced Due Diligence Checks are subject to players' profile and the amount of Risk they pose to us. Only when we determine some of the above points or a combination of a few will we flag the customer/customers in question and conduct risk monitoring. This will include checks of where the customer works, value of house, where the customer lives and checks to see whether the value of the house is logical compared to the customers spending.

5.1 Suspicious Activity Reports SARs

Within that framework, Suspicious Activity Reports (SARs) are an imposed requirement. The Merchant ensures that any employee reports to the Risk Team where they have grounds for knowledge or suspicion that a person or customer is engaged in ML or terrorist financing. Any employee failing to do so is open to criminal prosecution.

Escalations of SARs should be done in a confidential, discreet manner, in a handwritten form and not via email so as to ensure maximum anonymity.

An employee must not, under any circumstances, disclose or discuss any AML concern with the person or persons subject to an investigation, or any other person for that matter. Disclosure (also known as "tipping off") is strictly prohibited and carries with it very serious legal penalties.

Furthermore, and in order to keep ourselves protected as much as possible, no remark should ever be left on an account that would give any indication that ML is suspected, a player being entitled, at any point in time, to request the full notes/remarks on their account.

5.2 Working Procedure

Merchant reviews players spend and game play to check for suspicious activity. Before any withdrawal is processed the following procedures are carried out:

1. The customers deposit history is reviewed to confirm that no suspicious payments have been made to the customer's account. The frequency of deposits and the sum of deposits are reviewed to ensure they are within normal range for the customer based on his depositing history and the general depositing range throughout our network.
2. The customer's turnover is reviewed to ensure that they have played in the casino and are not using Merchant as a method to move money.
3. When possible, funds must always be refunded back to the original payment method used by the player to make a deposit.

5.3 Withdrawal Procedure

When reviewing a customer's account prior to withdrawal the agent must answer the following questions in the AML segment in the Risk Entry:

1. Did the player wager?
2. Does the payment Method belong to the player and has the player used it to deposit?
3. Are the customer's transactions and bets in line with expectations for the player?

5.4 Escalation Process

Following the AML policies in place and escalating any suspicious activity, as previously described, are crucial to the company as they protect it from financial losses and ensure that it remains compliant within the different jurisdictions which govern it.

Any activity which appears suspicious, even only slightly, has to be escalated. Not escalating a suspicion of money laundering can lead to criminal prosecution.

6. Employees

6.1 Senior Management

Senior management is fully committed to and responsible for the implementation of this policy. Senior management is made aware of their individual personal liability for consenting to, or conniving in, the commission of offences under the Regulations, or where such offence is attributable to any neglect on his part.

6.2 MLRO

A designated Money Laundering Reporting Officer takes responsibility for SARs in respect of the prevention and detection of money laundering, counter terrorism financing and our obligations under article 11 of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99).

The nominated MLRO has responsibility for making reports and reporting of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

6.3 Staff training

All staff will receive training on their obligations in respect of money laundering reporting and are aware of the procedures in place for escalation of any suspected incidents to the MLRO. As part of this process, staff are made aware that personal disregard for the legal requirements, for example, turning a blind eye to a customer spending criminal proceeds, may result in criminal or regulatory action.

Relevant employees receive training on how to follow house policies and procedures for:

- Client due diligence (CDD), including enhanced requirements for high risk clients, which includes PEPs;
- reporting suspicious activity to the nominated officer where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions

7. 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 so identified by the Gambling Commission. Client registered in High Risk Countries are always subject to EDD.

Countries currently on the FATF list are:

- Afghanistan
- Algeria
- Angola
- Bosnia & Herzegovina
- Ecuador
- Guyana
- Iraq
- Lao PDR
- Myanmar
- Panama
- Papua New Guinea
- Syria
- Uganda
- Yemen
- Iran
- Democratic People's Republic of North Korea

Players from the FATF list of jurisdictions seen to threaten the international financial system from on-going and substantial money-laundering or terrorist financing activities, as identified on FATF publications, will be refused.

8. Record keeping

We ensure that there is an audit trail to assist in any financial investigation by a law enforcement body. Our record keeping policy and procedure covers records in the following areas:

- Details of how compliance has been monitored by the nominated officer
- Delegation of AML/CTF tasks by the nominated officer
- Nominated officer reports to senior management
- Information not acted upon by the nominated officer, with reasoning why no further action was taken
- Customer identification and verification information
- Supporting records in respect of business relationships or occasional transactions
- Employee training records
- Internal and external SARs
- Contact between the nominated officer and law enforcement or the NCA, including records connected to appropriate consent

9. Offences

All employees are made aware of their risk of committing the following related offences:

- POCA and the Terrorism Act create offences of failing to report suspicious activity
- Where an employee fails to comply with the obligations to make disclosures to a nominated officer, or the nominated officer to NCA*, as soon as practicable after the

information giving rise to the knowledge or suspicion comes to that person, they are open to criminal prosecution

- They may also commit an offence under POCA or the Terrorism Act if they disclose information that an SAR has been submitted that is likely to prejudice any investigation, or disclose information that an investigation into allegations that an offence under POCA or the Terrorism Act has been committed, that is likely to prejudice the investigation
- They also commit an offence if they know or suspect that an appropriate officer is acting (or proposing to act) in connection with a relevant investigation which is being or is about to be conducted, and they falsify, conceal, destroy or dispose of documents which are relevant to the investigation

10. Vetting procedures for new employees

The company undertakes a number of vetting procedures when staff are employed. We will ensure the employee is not a minor through proper identification checks and we will verify the identification and credentials of the employee through at least two independent references. We will also look to verify any further personal information or background information.

11. Protecting our equipment from internal crime and criminal misuse

The company is very aware that a key way to combat fraud is to first identify where the company's most valuable assets are. Processes and controls have been built into the routine business of the company to minimize the chances of any of the key assets being misused.

Our server equipment are located at Unicept Malta who have in place necessary policies around protection of equipment, for example, a visitors management procedure, fire alarms, shredding of confidential documents, locked cabinets, testing, a security team etc. Merchant also implements such policies at our offices.

12. Compliance and Risk Committee

We intend to establish this to review executive risk. Both the MLRO and Compliance Officer will be members as will another non-executive director. These will meet no less than quarterly or as required.

13. Ensuring the companies we deal with are trustworthy and reputable

Merchant promotes strong principles of business and professional ethics at every level. When selecting suppliers, there are a number of criteria we consider:

- Financial strength (for long term sustainability);
- Legal and regulatory compliance;
- Commitment to a wider corporate responsibility program; and
- Desire and ability to deliver quality and value.

All new suppliers must go through a rigorous approvals process where all information put forward by them is verified.

This information is then assessed internally to consider the risks associated with the supplier; taking into account all of the above criteria. If rejected, the supplier will be

informed. Merchant ensures that all organisations we contract with understand the compliance obligations under the relevant player jurisdictions.

14. Our responsibilities under the Proceeds of Crime Act (POCA)

Merchant is fully aware of the procedures and policies required by the Proceeds of Crime Act 2002 and have policies and procedures in place related to this Act (as detailed below).

15. Internal record keeping

The below key principles: know your customer, internal record keeping and reporting, ensure our compliance with laws and regulations.

- Records on all customer transactions - regardless of their relation to payments or plays - will be kept for at least 6 years after the transaction.
- Records on customer details - regardless of their value state or open/blocked status - will be kept for at least 6 years after the relationship with the customer was terminated.
- Records on money laundering investigations and suspicious activity reports will be kept for 6 years after the investigation was completed.

16. Prevention of collusion and data protection compliance

The Merchant Terms and Conditions make clear that cheating will not be tolerated and that customer accounts will be closed if cheating occurs.

In terms of data protection, all data related to user payment accounts is stored, encrypted, and managed by Payment IQ, and Merchant employees have no access to user payment information. All Customer Information in the organization will be protected through a strict Information Security policy that all employees and suppliers will adhere to, that will include System Access and Authentication Control, Password Policy, Malware Protection measures, Intrusion Prevention policy, Encryption Policy, and strict Network Control and Management.

Know Your Customer (KYC)

Introduction

By agreeing to the Terms you authorize us to undertake any verification checks we may require or that may be required by the third parties (including, regulatory bodies) to confirm your identity and contact details (the "Checks").

During this Checks we may restrict you from withdrawing funds from Your Account.

If any information that you have provided is untrue, inaccurate, misleading, does not match your ID or otherwise incomplete we reserve the right to terminate your account immediately and/or prevent you from using the services, in addition to any other action that we may choose to take.

If we are unable to confirm that you are at the Legal Age then we may suspend Your Account. If a fact that you were under the Legal age at the time you made any gambling or gaming transactions, then:

- Your Account will be closed;
 - all transactions made during that time will become void, and all related funds deposited by you will be returned in amount;
 - any winnings which you have accrued during that time will be forfeited from you and you will be required to return to us all funds that were withdrawn from Your Account.
- In the event of any change in your personal details You are required to inform us by contacting Support.

Objective of the Policy

The Company shall request verification of the user of its Services at the following situations:

1. Suspicion of fraud, money-laundering, criminal activity etc.;
2. Doubts about the authenticity of the provided documents;
3. Violation of conditions for using the services of the Company;
4. Any other situation the Company shall deem appropriate.

By means of that request the Company may demand a standard set of identification data and documents, as well as additional documents.

The minimum set of identification data includes:

- full name;
- date of birth;
- citizenship;
- address of permanent residence;
- an identification number;

The required documents are:

- actual passport of the client / ID card;
- document confirming the address of the client's permanent residence at the given time (utility bill, statement of the status of the bank account, etc.)

Additional documents are:

- additional national identity card (driver's license, military ID, etc.);
- photos of a user with an open passport against the background of his face (the document should be readable)
- photo of the bank card on the front side (5 first and 4 last digits, owner's name and date of expiry shall be readable).

Also the Company may ask the User to provide source of funds documentation which is important to make sure that user provides evidence that identifies the actual source(s) of funds that he uses to bet or play with.

This information may be in the form of:

- proof of earnings: Payslip/Director remuneration/Dividends/Pension;
- a bank statement/savings account that clearly shows consistent incoming values from an identifiable source;
- a Trust deed clearly showing a consistent entitlement to funds;

- dated proof of an award/payment made to the user;

The documents that the user provided shall be not approved because:

- address/Name on documents don't match with account name/address;
 - illegible documents or copies;
 - document Not Acceptable (for example user sends a copy of a document that is not on the accepted documents for ID verification or a copy of mail envelope instead of an actual utility bill);
 - any other reasons employees or contractors of the Company shall deem appropriate.
- Upon the results of the analysis of the documents provided the Company shall make a solution according to the Terms Conditions, Privacy policy, License agreement of the Website and legislation requirements.

Obligations

Due diligence (DD): Company's customers should be subject to a DD process and record keeping.

Anonymous Accounts: Anonymous or nominal' account records are not permitted. Any existing anonymous accounts or accounts believed to be nom de plume' or that have inconsistent identification should be subject to appropriate due diligence to establish the identity and bona fides of the account holder at an early opportunity. In case it is impossible to determine identity of the account holder, the account shall be closed, winnings cancelled and deposits paid out to the the account from where they have been received or withhold in case return of the deposits turn out to be impossible or costly.

Duplicate/Multiple Accounts: Many customers wish to operate parallel accounts in order to segregate their gambling spend. Notwithstanding this activity, Company shall identify and associate linked' accounts that may belong or be under the control of the same person. Company shall be entitled to cancel additional accounts or accounts of the player in question, cancel winnings thus gained and return deposits to the owner of the account.

Politically Exposed Persons (PEP). Company have to respond to any attempt to gamble by any person qualifying as Politically Exposed Person, i.e. any person holding significant public office (or who has held it at any time in the preceding year), having access to public funds or in a position of influence. PEPs include the readily identifiable family and associates of such persons. A risk based approach should be applied based on the value and scale of gambling and the location of such customer. The questionnaires shall include questions identifying PEPs.

The Company reserves the exclusive right to unilaterally decline any clients' application and/or terminate further provision of services without any statements or explanations to the client in case of breach of KYC policy.

Managing Director
Represented by: Vivian V. Ersilia
For and of behalf of Carletta N.V.

02.01.2024