

GRACE BAY B.V.

AML-CFT POLICY AND PROCEDURES

TABLE OF CONTENTS

Date	3
Version.....	3
Name	3
1 Introduction	4
1.1 The Regulations	4
1.2 What is Money Laundering?	5
1.3 What is funding of Terrorism?	5
1.4 The Need to Combat Money Laundering and Financing of Terrorism	6
1.5 The AML requirements focus On the following areas:	6
1.6 Proceeds of Crime	6
2 Customer acceptance policy.....	7
2.1 Introduction	7
2.2 Age Verification	7
2.3 Politically Exposed Persons	8
2.4 Countries and territories excluded for registration	8
2.5 Accepted Payment methods	10
2.6 No cash policy	12
3 Business Risk assessment and customer risk assessment	13
3.1 Business risk assessment (BRA)	13
3.2 customer risk assessment	14
3.3 Risk Scoring Grid	15
3.4 Customer Due Diligence	17
3.5 Simplified Due Diligence (SDD)	17
3.6 regular Due Diligence	18
3.7 Enhanced Due Diligence (EDD)	22
3.8 Source of Wealth Questionnaire/Documentation	23
4 ONGOING MONITORING.....	26
5 RECORD KEEPING PROCEDURES	28
6 rePORTING PROCEDURES AND OBLIGATIONS.....	29
6.1 Internal Reporting Procedures	29
6.2 EXTERNAL REPORTING PROCEDURES	30
7 outsourcinG services	31
7 Outsourcing services	31

8 Awareness and Training.....	32
9 Sanctions	33
10 AML Department structure.....	33

DATE	VERSION	NAME
2019.10.10	1.0	Virae Management B.V.
2020.04.08	1.1	Virae Management B.V.
2023.09.14	1.2	Virae Management B.V.

1.1 THE REGULATIONS

This document describes the anti-money laundering policies used for Grace Bay B.V. hereinafter referred to as "the Company". The procedures adopted are based on the Curacao Remote Gaming Regulations, on the Implementing Procedures for Remote Gaming, on the Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations issued under it, and on the Implementing Procedures issued by FIAU on July 2019.

The respective laws & regulations can be obtained via de Financial Intelligence Unit of Curaçao (FIU) website (www.mot.cw) and the website of the Central Bank of Curacao St. Martin (www.centralbank.cw).

<http://mot.cw/Web/MOTWeb/MOTWeb.nsf/web/laws#LINKS>

[http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/3f138a325bb578a5042578200064a56a/\\$FILE/99. GT Landsverordening melding ongebruikelijke transacties%20 1 .pdf](http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/3f138a325bb578a5042578200064a56a/$FILE/99.%20Landsverordening%20melding%20ongebruikelijke%20transacties%201.pdf)

[http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/71f835ee862e77b3042578200064b538/\\$FILE/Landsverordening %20identificatie%20bij%20dienstverlening%20\(geconsolideerde%20tekst %20A.%20%202017%20no.%2092\).pdf](http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/71f835ee862e77b3042578200064b538/$FILE/Landsverordening%20identificatie%20bij%20dienstverlening%20(geconsolideerde%20tekst%20A.%20%202017%20no.%2092).pdf)

[http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/71f835ee862e77b3042578200064b538/\\$FILE/84.%20Lb%20houdende%20de%20inwerkingtreding%20Lv.%20tot%20wijz.%20Lv%20identificatie%20bij%20dienstverlening.def.pdf](http://mot.cw/web/motweb/motweb.nsf/a61721b0b7293b3204257685006d44ed/71f835ee862e77b3042578200064b538/$FILE/84.%20Lb%20houdende%20de%20inwerkingtreding%20Lv.%20tot%20wijz.%20Lv%20identificatie%20bij%20dienstverlening.def.pdf)

[http://mot.cw/web/motweb/motweb.nsf/29e3df05e1abce0804257682005b24be/e123edc5c7b30589042576da00757d7f/\\$FILE/FATF%20Recommendations%202012%20as%20updated%20november%202017.pdf](http://mot.cw/web/motweb/motweb.nsf/29e3df05e1abce0804257682005b24be/e123edc5c7b30589042576da00757d7f/$FILE/FATF%20Recommendations%202012%20as%20updated%20november%202017.pdf)

[http://mot.cw/web/motweb/motweb.nsf/29e3df05e1abce0804257682005b24be/e123edc5c7b30589042576da00757d7f/\\$FILE/FATF%20Methodology%202022%20Feb%202013%20as%20updated%20in%20november%202017.pdf](http://mot.cw/web/motweb/motweb.nsf/29e3df05e1abce0804257682005b24be/e123edc5c7b30589042576da00757d7f/$FILE/FATF%20Methodology%202022%20Feb%202013%20as%20updated%20in%20november%202017.pdf)

1.2 WHAT IS MONEY LAUNDERING?

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make legitimate economic use of the criminal proceeds. When a criminal activity generates substantial income, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or to the persons involved. Criminals do this by disguising the sources, changing the form or moving the funds to a place where they are less likely to attract attention.

Traditionally, three stages were identified for the process of money laundering – the placement stage, the layering stage and the integration stage.

- a) Placement: the first introduction of the cash proceeds of criminal conduct into the financial system, especially via deposit-taking institutions and, again, particularly in jurisdictions with extensive banking secrecy laws and little or no anti money laundering legislation.
- b) Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- c) Integration: the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into

1.3 WHAT IS FUNDING OF TERRORISM?

Funding of terrorism is the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism.

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. Indeed, funding from legal sources is a key difference between terrorist organisations and

traditional criminal organisations involved in money laundering operations. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

1.4 THE NEED TO COMBAT MONEY LAUNDERING AND FINANCING OF TERRORISM

The Company has three main concerns:

- 1 Reputational Risk;
- 2 Regulatory Risk; and
- 3 Litigation Risk.

1.5 THE AML REQUIREMENTS FOCUS ON THE FOLLOWING AREAS:

- a) Identification procedures;
- b) Record Keeping;
- c) Internal procedures;
- d) Staff Education, Training and Development;
- e) Internal controls and communication procedures that are appropriate for the purposes of forestalling and preventing money laundering and the financing of terrorism; and
- f) Procedures, controls and evaluation.

1.6 PROCEEDS OF CRIME

Irrelevant of how money is transferred to any of our casinos, there is always a risk that this money would have originated from illegal activities, such as credit/debit card fraud, theft from player's employer or even narcotics trafficking. Hence, by paying greater attention and increase monitoring of high spenders, the Company will be able to mitigate this risk.

2.1 INTRODUCTION

The Company's general policy is not accepting any players whose funds have emanated from ill-gotten means, and to comply with all applicable obligations in relation to anti-money laundering (AML) and know your customer (KYC). The Company identifies all players prior to establishing a business relationship, and proceeds to verify the data provided on certain activities being carried out, which may be first deposit, cumulative deposit thresholds being reached, cumulative transactions exceeding EUR 2,000 within 180 days or reaching other triggers. Players who are not registered will not be permitted to play for real money. One of the main drivers is to protect our operations from fraudulent transactions. The other key driver is preventing players from being able to launder money using our services; such money-laundering could take the form of either:

- (a) a customer gambling using funds which they have obtained through criminal conduct – proceeds of crime; or
- (b) a customer seeking to disguise the fact that they have obtained money from criminal conduct by passing it through our account in an attempt to 'clean' it.

It is important that the Company has a clear and concise understanding of all customer practices in order to avoid any possibility of money laundering and/or terrorist financing exposure.

To this end, the Company restricts or prohibits the commencement of business relationships with customers and/or entering into transactions that fall outside our established risk appetite.

2.2 AGE VERIFICATION

The Company will not accept any player unless of legal age, 18 years or older (Estonia 21 years or older). The registration process requires the date of birth to be over 18 years and will not permit a user to input a date which would contradict that.

2.3 POLITICALLY EXPOSED PERSONS

One of the most prominent risks of bribery and corruption is that posed by public officials, their associates and family members. PEPs are been defined as:

'individuals who have been entrusted with prominent public functions, including heads of state of government, senior politicians, senior government, judicial or military officials, and senior executives of publicly owned corporations and important political party officials.'

The danger posed to the Company accepting funds from PEPs is that such persons may be exposed to criminal property that has been generated by corrupt practices since there is always the possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. In addition to any legal or regulatory impact, if it becomes common knowledge, it may result in damage to reputation and loss of new businesses.

The Company carries out PEP checks when the client reaches the threshold of 2000,00 Euro.

There are several external sources that store lists of PEPs. These sources are automatically checked, and if a match of full name and birth year against our player database is found, PEPs suspicion is created. These suspicions are not shown in the main suspicion queue in the 4K interface, there is a separate tab for them, which can only be seen by users having right "Antifraud: access to PEPs list".

Once it has been ascertained that a customer is a PEP, the Company will refuse any business relationship with the person and if the person already has an account with the Company, this will be terminated.

2.4 COUNTRIES AND TERRITORIES EXCLUDED FOR REGISTRATION

1. Afghanistan
2. Belarus
3. Bosnia and Herzegovina
4. Burma/Myanmar
5. Burundi

6. Central African Republic
7. Crimea and Sevastopol
8. Cuba
9. Democratic Republic of the Congo
10. Egypt
11. Eritrea
12. Federal Republic of Yugoslavia & Serbia
13. Guinea Bissau
14. Haiti
15. Iran (human rights)
16. Iraq
17. ISIL and Al-Qaida
18. Ivory Coast
19. Lebanon
20. Libya
21. Maldives
22. Mali
23. Malta
24. Myanmar
25. Nicaragua
26. North Korea (Democratic People's Republic of Korea)
27. Pakistan
28. Republic of Guinea
29. Republic of Guinea-Bissau
30. Republic of Moldova
31. Russian Federation
32. Somalia
33. South Sudan
34. Sudan
35. Syria
36. Terrorism and terrorist financing
37. Tunisia
38. Ukraine
39. United Nations
40. Venezuela
41. Yemen
42. Zimbabwe

Countries and territories restricted as per Curacao Licensor requirement:

43. Aruba
44. Austria
45. Bonaire
46. Curaçao
47. France

48. The Netherlands
49. Australia
50. United Kingdom
51. Spain
52. Saba
53. Statia
54. St Martin
55. Unites States of America
56. Any other jurisdiction that the Central Government of Curaçao (formerly Netherlands Antilles) deems online gambling illegal or are blacklisted.

The following categories of players will not be accepted at registration/post registration checks:

- Players residing in non-reputable jurisdictions,
- IP login registered in a non-reputable jurisdiction,
- Sanctioned individuals, Players under the age of 18.

However, on a case by case basis, the Company has the right to refuse any applicant for business or terminate an existing business relationship if the required Customer Due Diligence requirements are not satisfied. A departure from the above, may be applicable, on a case to case basis, following the approval of Senior Management.

2.5 ACCEPTED PAYMENT METHODS

- 1 EFT
- 2 Bank Transfer
- 3 QR Code
- 4 Bitcoin
- 5 Jeton
- 6 Papara
- 7 Cardpay
- 8 Cashtocode
- 9 Ecopayz
- 10 Eps
- 11 Euteller
- 12 Ideal
- 13 Klarna
- 14 Muchbetter
- 15 Neteller
- 16 Nordea_Solo
- 17 Paysafecard
- 18 Poli
- 19 Przelewy24
- 20 Rapid_transfer

- 21 Siirto
- 22 Siru Mobile
- 23 Skrill
- 24 Sofort
- 25 Trustly
- 26 Trustly (pay and play)
- 27 Zimpler

Certain payment options must be treated as high risk factors, this includes cash and other payment methods that may not leave or disrupt the audit trail and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies.

Payment options used by the Company are Prepaid Card, Mobile Payments, Internet-based payment services, credit cards, and bank transfers. The Company does not accept cash payments or virtual currencies.

For Internet-based payment services and mobile payment services there is typically no face-to-face customer contact. This may increase the risk of identity fraud or customers providing inaccurate information potentially to disguise illegal activity if effective measures to address this risk are not employed. However, this lack of face-to-face contact is often counterbalanced through the adoption of alternative identification mechanisms, which can provide adequate risk mitigation measures.

Electronic wallets (e-wallets): Usually, electronic wallets which only accept money from financial institution accounts held in the player's name (for instance Skrill) will not pose any greater or lesser money laundering risk than funds received directly from the financial institution itself. Certain e-wallets do accept deposits via pre-paid vouchers (for instance Neteller) and hence these pose a higher risk as money launderers and/or terrorists may choose such payments methods to disguise the origin of their funds or to obstruct the audit trail. In order to mitigate this risk, the Company takes due care in choosing which e-wallets it will commit to provide to players, especially since not all e-wallets are licensed in reputable countries. Thus, due diligence checks are undertaken to ensure that the Company is only contracting with reputable companies

2.6 NO CASH POLICY

No cash deposits / withdrawals will be effected.

3.1 BUSINESS RISK ASSESSMENT (BRA)

A BRA is a process whereby the Company identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT risks. On the basis of this assessment, it will be able to determine which areas to prioritize in terms of AML/CFT and ensure that its AML/CFT measures, policies, controls and procedures are commensurate with the ML/FT risks it faces to mitigate the same. The BRA is therefore the foundation of the risk-based approach and through it the Company can identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business.

The BRA is based on 4 risk factors:

a) Customer Risk:

- the number of customers within each customer risk type;
- the volume of business.

(b) Geographical Risk:

- the number of customers from a given jurisdiction;
- the number of transactions to/from a given jurisdiction.

(c) Products, Services and Transaction Risk:

- the number and the type of products and services;
- the number of customers per each product and service;
- the volume per product and service.

(d) Delivery Channel:

- the number of relationships started on a non-face-to-face basis;

Furthermore, the Company follows a list of other risk factors to determine a client's risk profile in relation to ML/FT. The list includes the following:

- A list of countries which the FATF considers to apply deficient AML/CFT controls;
- A list of countries which in the Company's opinion represent heightened ML/FT risk (which may or may not be on the first list);

- A value which represents the upper value of a typical player's transactions;
- A list of payment channels which are considered higher risk;
- A list of any other indications which in the opinion of the Company's MLRO indicates higher risk;
- A list of the subjects of AML/CFT related warning notices; and
- Screening for politically exposed persons, sanctions and adverse information.
- Product risk (Casino, Live Casino, Bets)

The combination and assessment of these risk factors will allow the Company to identify the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes. Having done so, the Company has to determine the likelihood of any one scenario materialising, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk.

$\text{Likelihood} + \text{Impact} = \text{Inherent Risk}$.

Having determined the inherent risk, the Company has to consider what AML/CFT measures, policies, controls and procedures it already has in place or it plans to adopt and establish how effective these are in mitigating the inherent risk (Effectiveness of mitigation measures).

At the end the Company can calculate the residual risk:

$\text{Level of Inherent Risk} - \text{Mitigating Measures} = \text{Level of Residual Risk}$

Even though the Company set out the mitigation measures, there will remain a degree of ML/FT risk that cannot be addressed, avoided or controlled.

At this stage, the Company has to consider whether the residual risk falls within its risk appetite or to cease the business relationship. The BRA is regularly reviewed on an annual basis. However, the Company revises and updates the BRA:

- whenever new threats and vulnerabilities are identified;
- whenever there are changes to its business model/structures/activities;
- whenever there are changes to the external environment within which the Company is operating.

3.2 CUSTOMER RISK ASSESSMENT

Once the Company has understood the residual risk with regard to its clients, it will be able to carry out a Customer Risk Assessment (CRA).

The Company has set up the risk factors applicable to all its current participants (new and existing) in order to identify whose circumstances would indicate higher risk and flag them for enhanced due diligence, including enhanced ongoing monitoring, or refusal/termination.

On the basis of the CRA, the Company will be able to apply the proper level of CDD and will be able to identify a customer as presenting a higher risk of ML/FT.

In order to carry out the CRA, the Company should consider all risk factor referred under section 3.1. and other risk factors such as:

- a) The Reputation of the customer: the Company should consider whether a customer has been the subject of adverse reports linking him/her to crime (especially financial crimes) and/or terrorism.
- b) Nature and Behaviour:
 - (a) the customer is reluctant to provide any documentation and/or information requested by the Company without a legitimate reason for doing so;
 - (b) the documentation presented to meet the Company's request for information/ documentation gives rise to doubts as to its veracity or authenticity.

3.3 RISK SCORING GRID

SCORING	Type of customer	Product/Service	Delivery Channels	Geographical Risk
High 8 – 10	PEPs	N/A	Non face to face	Non-Reputable and High-Risk Jurisdiction
Medium 5 – 7	Individuals who reached the threshold	Fixed odds games where hedging is possible	Non face to face (using technological systems with embedded safeguards)	Reputable Jurisdiction

	of 2000,00 Euros			
Low 1 – 4	Individuals	Fixed odd games without hedging	N/A	EU Member State and Domestic

At the end the average shall provide the Company with the necessary risk score for each client.

High	Risk likely to happen and/or to have serious consequences. Response: Monitor transactions and customer behaviour +EDD measures.
Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
Low	Unlikely to happen and/or have minor or negligible consequences. Response: Fine to go ahead.

On the basis of the risk score, the Company shall apply the following measures:

1) Where the risk is low: default risk level – Standard Due Diligence and no additional measures.

2) Where the risk is medium (for example Paysafe depositors, after 500 EUR deposit, or non-closed loop withdrawal):

- Source of Wealth questionnaire;
- KYC including proof of ownership

3) Where the risk is high (for example withdrawal after Paysafe deposit, bin-country mismatch (excluding Revolut and similar), third party deposit, or Sanction, PEP, SIP (Not accepted as clients):

- Source of Wealth questionnaire;
- KYC including proof of ownership;
- Paysafe deposits over 1,000 EUR = SOWQ + Source of wealth documentation;
- Soft checks - Social networks, Ratsit, etc;
- Source of wealth documentation if needed;

- Validation of documents – we can request certified copies of documents to validate name, address, date of birth and source of funds; and/or
- Internal corroboration of user identity – this could emanate from a variety of sources from customer monitoring, other databases, gaming activity etc; and/or
- External corroboration – this can entail the use of a 3rd party solution to provide enhanced soft background checks on public records;
- Source of Funds checks consisting of the following:
 - Payslips
 - Employment Contracts
 - Proof of Deposits
 - Bank Statements
 - Inheritance Confirmations/Wills
 - Deed of Donation

The Company carries out the CRA within 30 days from when the pre-established threshold of Euro 2000,00 within 180 days is reached by the client.

3.4 CUSTOMER DUE DILIGENCE

There are three levels of customer due diligence that the company must carry out:

- Simplified due diligence
- Regular due diligence
- Enhanced due diligence

3.5 SIMPLIFIED DUE DILIGENCE (SDD)

A Simplified Due Diligence process will be the first stage of a risk-based process. Simplified Due Diligence is carried out between Registration and First Deposit on Customers that hail from low risk jurisdictions.

Simplified due diligence is performed by the customer providing identification details prior to registration. These details include:

- the date of birth;
- the player's identity;
- the player's place of residence;
- the player's valid e-mail address.
- The player's phone number confirmation

Every registering player must activate the account via the email, SMS or call activation procedure. Once a customer completes the registration form and verifies the email or SMS, then the account is opened and included within the back-office system.

It is company policy not to allow players to deposit or withdraw any funds whatsoever before the registration process is complete.

3.6 REGULAR DUE DILIGENCE

Stipulations as per FIU Curaçao

Objective and Subjective indicators for mandatory reporting regarding providers of internet gambling are as follows:

I. OBJECTIVE INDICATORS:

A. Transactions that are reported to the police or the judicial authorities:

Transactions that are reported in connection with money laundering or the financing of terrorism to the police or the judicial authorities must also be reported to FIU Curaçao.

B. An intended transaction performed by or on behalf of a natural person, legal person, group or entity that is included on a list established under the National Ordinance regarding Sanctions:

An intended transaction by or for the benefit of a person, legal entity, group or entity that appears on a list established under the Sanctions Ordinance.

C. A transaction worth NAf 5,000 (equivalent to USD 2800,-) or more, regardless of the form or platform used for such transaction. This includes at least:

1. A cashless transaction worth NAf 5000,- (equivalent to USD 2800,-) or more:

A cashless transaction is a transfer from a bank account of the service provider to a local or international bank account, at the request of a player.

2. Any deposit or withdrawal by a player for the amount equivalent to NAF 5000, - or more.

3. Sale of "gaming tokens" to players worth NAF 5000, - or more.

Gambling tokens include at least chips and credits (if applicable)

4. Payment of prize money worth NAF 5000, - or more.

Company Policy Applied

The Regular Due Diligence process is triggered on the occurrence of one of the following events:

- Single/Cumulative deposits/withdrawals/winnings exceeding €2,000 within 180 days
- Attempt to withdraw to a different payment method;
- Attempt to request a name change (clients cannot do so automatically)

The Euro two thousand (€2,000) deposit threshold can be calculated either:

a. On a daily basis taking into account all deposits effected by a customer since the establishment of the business relationship; or

b. On the basis of a rolling period of one hundred and eighty (180) days. In the latter case, the Company would have to consider whether a customer's overall deposits in the previous one hundred and eighty (180) days have met or exceeded the Euro two thousand (€2,000) threshold.

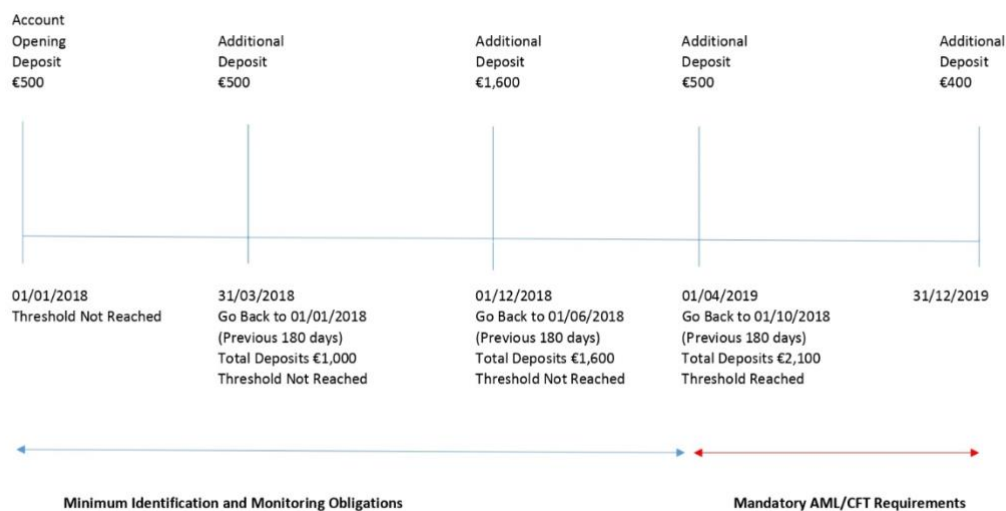


FIG. 2 Application of the Rolling Period

Page 20 of 37

In order to verify the details on their account, the customer is required to send customer care a photocopy or scan of one document from each of the categories listed below:

Personal Identification - one photo ID from the following list:

- 1) Current Signed passport
- 2) Current photo-card Driver's License (Provisional or Full)
- 3) Current Full Driver's License (old style paper version)
- 4) Current EU National Identify Card
- 5) Other recognized identity card such as an Armed Forces Identity Card
- 6) Norwegian credit cards with photo and ID number can be accepted as ID

Please note regarding some cards from Finland: It can be a debit card and credit card in one, number in the front is for Credit Card and number in the back for Debit Card usually.



Credit-numero etupuolella

Creditillä maksaessasi tarvitset allekirjoituspaneelin vieressä olevan kolminumeroisen tarkistelukoodin.



Debit-numero kääntöpuolella

Address Verification - one of the following:

- 1) Utility bill (within last 3 months)
- 2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
- 3) Current Full Driver's License (old style paper version)
- 4) ID card with address + Passport or additional ID
- 5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 3 months)
- 6) Council tax bill or payment book (within last 3 months)
- 7) Recent mortgage statement (within last 3 months)
- 8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 9) Home Insurance certificate or policy
- 10) Motor Insurance certificate or policy
- 11) Electoral roll
- 12) Credit reference agency
- 13) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

- 1) Company account registered Credit or Debit card
- 2) Copy of Credit or Debit card account statement of a card registered on with Company account (less than 3 months old)
- 3) Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)

When requesting such documentation, the customer must always be informed that:

- The card number must be blanked out leaving only the first 6 and the last 4 digits visible together with the expiry date.

- The documents must be clear and legible.
- The documents should show the residential address.

3.7 ENHANCED DUE DILIGENCE (EDD)

Following a risk-based approach for customer due diligence, customers which are flagged as high risk and/or certain triggers, or thresholds will require enhanced due diligence to take place. The triggers for the enhanced due diligence process to take place are as follows:

- Customer identified as politically exposed persons (PEPs);
- Lifetime customer deposits exceeding EUR 100,000;
- Customer identified as high risk when carrying out Risk Assessment;
- Regular Due Diligence identifies heightened risks;
- Significant anomalies in gaming or funding activity;
- Source of Wealth provided by customer cannot be verified following soft verifications and the customer is a High Spender or has Disproportionate Spending.

Enhanced due diligence is achieved by the following processes:

If we have	Ask for
a utility bill	a bank statement
a bank statement	a utility bill
a passport	driver's license
driver's license	a passport
national ID	a passport

In addition, the Company may carry out and/or request the following information/documents:

- Validation of documents – we can request certified copies of documents to validate name, address, date of birth and source of funds; and/or

- Internal corroboration of user identity – this could emanate from a variety of sources from customer monitoring, other databases, gaming activity etc; and/or
- External corroboration – this can entail the use of a 3rd party solution to provide enhanced soft background checks on public records;
- Source of Funds checks consisting of the following:
 - Payslips
 - Employment Contracts
 - Proof of Deposits
 - Bank Statements
 - Inheritance Confirmations/Wills
 - Deed of Donation

3.8 SOURCE OF WEALTH QUESTIONNAIRE/DOCUMENTATION

Customer due diligence is an ongoing process and as a result there are trigger events which warrant the collection of additional documentation. Upon classifying a player as High risk or upon the player reaching a lifetime deposit value as specified in the below table, the client will be requested to complete a Source of Wealth (SOW) and Source of Funds (SOF) questionnaire and if warranted the client will be asked to provide SOW/SOF documentation.

It is understood that the players may not have at hand the requested information thus the company has determined an acceptable timeframe by which documentation should be provided by the players without permanently impact the ability to utilize the services of the online casino.

The below mentioned table details the accepted wait time prior the player service is completely restricted:

Client Risk Classification	Value trigger	Calendar Days
Medium	2,000 EUR	14 days
High	2,000 EUR	7 days

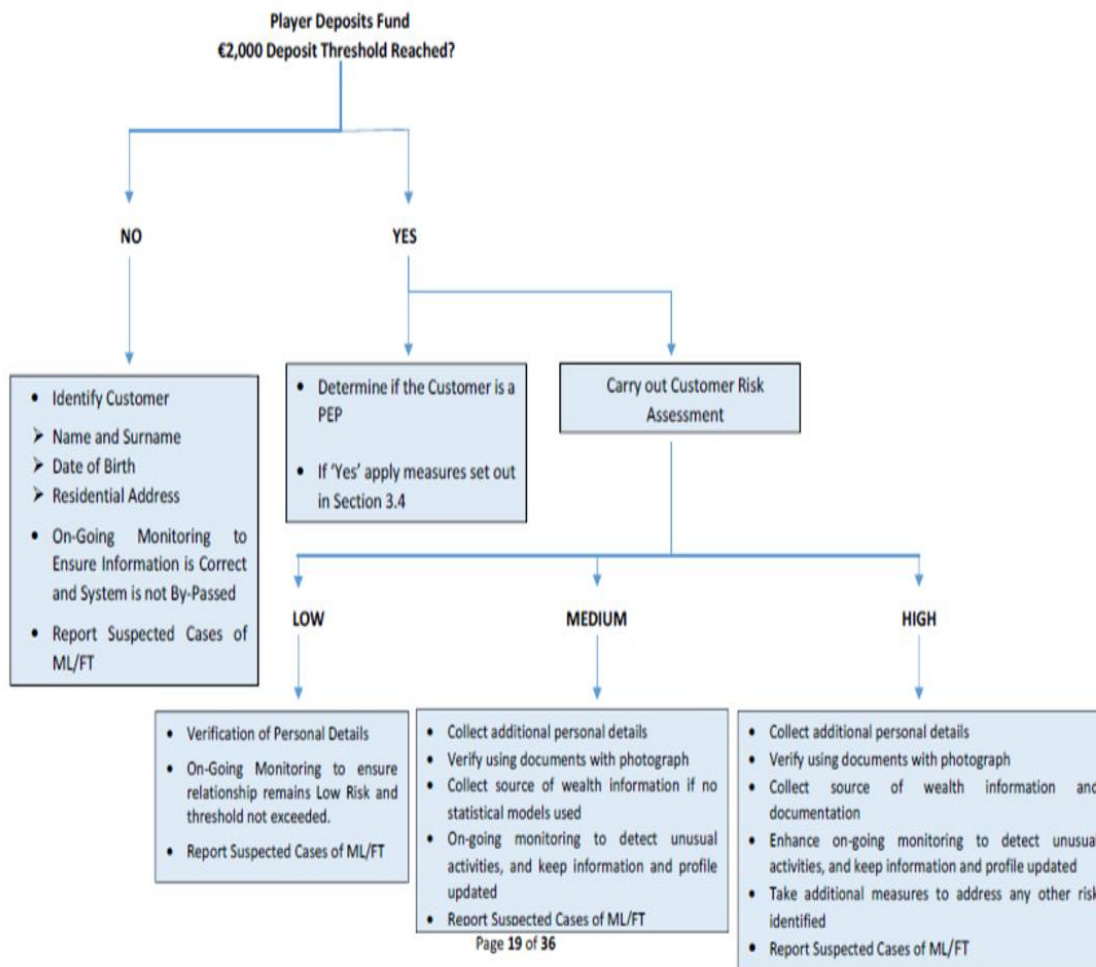
During this period, the players' account will remain operational however, no withdrawals will be processed.

A small variant to the above policy is applicable on game play offered to player profiles authorized under the Curacao license whereby the deposit threshold of EUR 2000 is applicable over a rolling period of the last 180 days. The description of this procedure and a flowchart highlight the process in details in the Country specific variations. Subsequently, additional KYC procedures take place when a customer reaches either one of the following thresholds first:

Value trigger
€10,000 within 7 days
€50,000 within 30 days
€100,000 over lifetime

A grace period will be applied according to the player risk rating as defined in the below table.

Client Risk Classification	Calendar Days
Low	30 days
Medium	14 days
High	7 days



Page 19 of 36

4 ONGOING MONITORING

Once a business relationship is formed, Regulation 7(1)(d) of the PMLFTR requires the Company to carry out ongoing monitoring. It comprises two key elements:

A) Scrutiny and monitoring of transaction:

The Company shall monitor the transactions throughout the course of that relationship to ensure that they are consistent and in line with the customer behavior and his risk profile.

The transactions are monitored by an automated monitoring system in real time (pre-transaction monitoring) and/or after the event (post-transaction monitoring).

Where the Company notices that a customer's account activity is not in keeping with what it knows or expects from the customer, the Company shall ask to the customer to provide the source of the funds and source of wealth used for the said activity. The aim is to understand what the reason for this divergence is and obtain sufficient information and documentation on the matter.

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- A client who is a Politically Exposed Persons (PEPs), their family members or close business associates ("persons linked thereto");
- SIPs, Watchlist
- A client residing or located in a country, the AML/CFT credentials about which the Company has doubts;
- A client subject to warnings issued by the Curacao Gaming Regulator and
- A client who has been the subject of a disclosure
- A client flagged on the sanctions list.
- A client depositing gambling/withdrawing big amounts.
- A client flagged as a fraudster (reported by PSP)

To minimise the risks, all payments and fraud agents are instructed to consider instances, where a customer uses a card belonging to a third party (i.e. the card holder name does not match the customer's registered

details), as high risk. (Account is blocked, explanation and documents requested from the client)

B) Updated the information and the documents of the clients:

The Company requests fresh identification documents when the expiry date of identification documents held on file is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events.

The below mentioned table depicts the manual trigger event based on KYC aging, warranting a player review (player interaction required) or desktop review (no player interaction review required).

Risk Rating	Frequency from date of last review or customer interaction.	Registered via Bank ID or equivalent	Registered through conventional channel
High	Yearly	*retrieve address using social security number	Check Identification document expiry date (automatic process), collect new one where warranted and assess if an updated SOW document needs to be collected
Medium	Every 2 years	*retrieve address using social security number	Check Identification document expiry date (automatic process), collect new one where warranted and assess if an updated SOW document needs to be collected
Low	As triggered through the transaction monitoring process	*retrieve address using social security number	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected

5 RECORD KEEPING PROCEDURES

In order to ensure compliance with the PMLFTR and Implementing Procedures the Company ensures that the following records are maintained:

1) Records of BRA, which is to include the following:

(i) a copy of the BRA, changes thereto, as well as a record of any decision taken with respect to that assessment;

(ii) a copy of the most recent controls, policies, measures and procedures.

2) Record of CRA which is to include the following:

(i) a copy of each CRA carried out by the Company.

3) Records of CDD information and documents;

4) Record of business relationship with the details of transactions;

5) Record of internal reports to the MLRO;

6) Record of any determinations made by the MLRO and the designated employee, where applicable;

7) Record of STRs;

8) Record of AML/FCT training;

9) Record of conduct certificates or other documentation obtained in carrying out employee screening; and

10) Record of any outsourcing agreements.

The Company maintains the records for a period of 5 years or for longer periods whether this extension is considered necessary for the purposes of the prevention of ML/FT. In any case the retention period will not exceed 10 years. The time period of five (5) years commences from the date on which the business relationship is terminated, or the occasional transaction carried out.

The Company maintains these records in electronic form and in its physical files.

6.1 INTERNAL REPORTING PROCEDURES

By employing the procedures as described in this policy and the Anti-Fraud and AML/CFT System (the System) fully investigating any transaction, we can identify suspicious transactions or activities that could be construed as money laundering or terrorist financing.

There is an obligation on all staff to report suspicions of money laundering or terrorist financing, and all suspicions should be reported immediately to the MLRO by completing the Internal Reporting Form.

These reports must be made by the Company's employees when they have a suspicion in relation to a customer's behavior or when they receive an alert from the System. In the latter case, before submitting a report to the MLRO, the employee must check whether the alert is simply a false positive.

Internal reports are to be submitted in writing using the standard template together with all relevant information and documentation available to the employee to assist the MLRO in making a determination as to how best to proceed.

The report must also include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

The MLRO must consider, without delay, every internal report he/she receives to determine whether or not the information contained in the report: (a) does give rise to a knowledge or suspicion of ML/FT; or (b) whether additional information is necessary to reach this determination.

Grace Bay B.V. is obliged to register with FIU Curaçao which will provide online access to a portal where reports will be submitted. The MLRO will have access to the online reporting portal of the FIU via:

<https://portal.mot.cw/portal.html>

6.2 EXTERNAL REPORTING PROCEDURES

After considering the internal report and all the necessary documentation, when the MLRO determines that there is:

- (a) knowledge;
- (b) suspicion; or
- (c) reasonable grounds to suspect that:
 - a transaction may be related to ML/FT (regardless of the amount involved); 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 MLRO must file an STR.

The MLRO will not disclose the name of the employee who made the internal report to the FIAU, and in completing this report the MLRO must provide as much detail as possible together with the relevant identification and other supporting documentation.

The decision to file or not to file an STR will always be at the discretion of the MLRO, and the MLRO will not be subject to the direction or approval of other parties within the Company, provided that in reaching a determination on whether to file an STR, the MLRO may seek assistance from other employees of the Company or external advisors.

STR Form available as ANNEX1 to this document.

7 OUTSOURCING SERVICES

Outsourcing involves transferring responsibility for carrying out an activity to a third-party provider ("**Outsourcing Provider**") for an agreed consideration. Outsourced services are usually provided on the basis of a mutually agreed service level as defined in a formal contract.

Despite the potential benefits of outsourcing, such as the reduction of costs of the company and access to specialized skills, information security incidents, such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to abide by agreed service levels, might occur and would reduce the benefits and jeopardize the security status of the organization.

This document (the "**Policy**") specifies procedures and controls in place at Grace Bay B.V. (the "**Organization**") to address and mitigate the risks associated with outsourcing and, in particular:

- Compliance/Regulatory/Legal risks;
- Country risks;
- Operational risks;
- Reputational risks.

And applies to any outsourcing providers including:

- Hardware and software support and maintenance staff;
- External consultants and contractors;
- IT or business process outsourcing firms;
- Temporary staff.

The policy addresses the following controls found under A.15.1 and A.15.2 of the ISO/IEC 27001 and 27002 standards:

- Identification of risks related to external parties;
- Addressing security when dealing with customers;
- Addressing security in third party agreements.

The Outsourcing Policy is available as a stand-alone document.

8 AWARENESS AND TRAINING

The Company shall adopt the appropriate and proportionate measures to:

- 1) ensure that the relevant employees are aware of relevant AML/FCT legislation and data protection requirements as well as of the Company's policy and procedures
- 2) provide training in relation to AML/FCT.

The training shall be provided to all employees involved in the relevant activity and business of the Company.

The training shall be relevant to the respective employees' specific responsibilities and function within the Company. Through the training the Company shall ensure that the relevant employees are aware of:

1. CDD measures
2. Record keeping procedures
3. Internal and external reporting procedures
4. Customer Acceptant Policy
5. CRA policy
6. BRA policy and the outcomes of the BRA

The Company shall provide the relevant employees with the following documents:

1. PMLA act
2. PMLFTR act
3. Criminal Code
4. FIAU Implementing Procedures
5. Curacao Gaming Regulator Implementing Procedures for Remote Gaming
6. Internal policies and procedures

The Company shall keep a record of training in which are included the following information:

1. Details of the training
2. Date on which the training was delivered
3. The nature of the training
4. The name of the employees who received the training
5. Copy of the training materials provided.

9 SANCTIONS

Upon reaching the Euro 2,000 within 180 days, customers are screened via the Dow Jones batch screening via API. This screening includes an extensive sanction list, adverse media content and PEP checks.

Any client which is flagged in these lists:

- Will have his account locked;
- the client will be allowed to continue once the MLRO approves the account; and
- the client may be asked for enhanced due diligence

10 AML DEPARTMENT STRUCTURE

The AML department structure in Grace Bay B.V. is presented in the following form:

- Junus Mursel – Money Laundering Reporting Officer (MLRO)

Other Supporting functions: Risk & Fraud, Payments and Verification departments

V. Demir

Virae Management B.V.

Managing Director

January 10, 2025

APPENDIX 1

STR FORM

INTERNAL SUSPICIOUS ACTIVITY REPORT	
1. Date of report:	
2. Person(s) making the report:	
3. Client name, Client ID and risk rating:	
4. Account status and account balance:	
5. Length of relationship/registration date of account:	
6. Client details (email, phone number, brand registration):	
a. Date of birth:	
b. Nationality/Country of registration:	
c. Address:	
d. Due diligence documents held:	
7. Person(s) suspected of criminal activity, if not client:	
a. Date of birth:	
b. Nationality/Country of registration:	
c. Address:	

d. Due diligence documents held:		
7. Crime/reason for suspicion (explain what activity or transaction gave rise to the suspicion i.e. the basis for suspicion) – if necessary, please use the additional information section:		
8. Date of suspected criminal activity/transaction:		
9. Provide details (e.g. dates and amounts) of any known transactions that are pending or due to occur in the future, if known:		
10. Name of individuals who know of this report (other than the signatories below):		
	Signature:	Date:
Upon completion, please forward the form to the MLRO or Deputy MLRO as soon as possible.		
11. Action taken by MLRO/Deputy MLRO:		

MLRO Confirmation: I confirm that I have received this STR from the person/s named above.	Signature:	Date:

ADDITIONAL INFORMATION RELEVANT TO THE REPORT

(this should be used for anything that you think may assist the MLRO e.g. background on the suspect, details on the activity of the related account, further explanation of the transaction, IP addresses, excel sheet of all deposits and withdrawals, methods of deposits/withdrawals. If/where applicable that third party intelligence databases were used in the search, these need to be included. **NB:** this page should not be attached where no additional information is provided)

Signature Certificate

Reference number: LK6WB-SHNQW-HLAHJ-DUMSU

Signer

Virae Management B.V.

Email: info@viraemanagement.com

Sent:

Signed:

Timestamp

10 Jan 2025 21:14:59 UTC

10 Jan 2025 21:14:59 UTC

Signature

V. Demir

IP address: 161.22.55.35

Document completed by all parties on:

10 Jan 2025 21:14:59 UTC

Page 1 of 1



Signed with PandaDoc

PandaDoc is a document workflow and certified eSignature solution trusted by 50,000+ companies worldwide.

