

MOONRAIL LIMITED BV

Anti-Money Laundering, Counter Financing of Terrorism, and Know Your Customer Policy

Version Control

Version	Date	Author	Notes
2.0	2020-06-24	MLRO	Document created, replacing old AML policy
2.1	2020-08-02	MLRO	Updated AML policy to expand on the Risks chapter.
2.2	2020-09-15	MLRO	Updated to emphasise that the policy applies to the entire company and related changed.
2.3	2021-01-26	MLRO	Expanded on procedures around due diligence and high risk countries.
2.3.1	2022-02-01	MLRO	Annual review, minor adjustments
2.3.2	2023-03-01	MLRO	Annual review, minor adjustments
2.4	2024-03-14	MLRO	Annual review, minor adjustments
2.5	2025-05-19	MLRO	Annual review, adjustments in accordance with regulatory requirements

Table of Contents

Version Control.....	1
1. Abbreviations.....	4
2. Policy Statement.....	4
3. Applicable Laws and Regulations	5
4. Money Laundering (ML) Terrorist Financing (TF) Proliferation Financing (FP)	6
5. Responsibilities.....	7
5.1 Board of Directors	7
5.2 Money Laundering Reporting Officer (MLRO)	7
6 Business Risk Assessment	7
• Customer Risk.....	8
• Delivery Channel Risk.....	8
• Payment Risk.....	9
• Country and Geographic Risk.....	9
• Product Risk.....	9
• Employee Risk.....	10
7 Know Your Customer (Customer Due Diligence)	10
7.1 Basic CDD.....	11
7.2 EDD	12
7.3 Ongoing Due Diligence	12
8 Other Due Diligence	13
8.1 B2B.....	13
8.2 Third-Party Providers.....	13
8.3 Retrospective	13
9 Ongoing Monitoring and Reliance on Third-Party Tools.....	13
10 Training	14
11 Record Keeping and Data Retention.....	14
12 Reporting Suspicious Activities	15
12.1 Suspicious Activity Report (SAR)	15
12.2 Tipping Off.....	15

13	<i>High Risk Factors.....</i>	<i>15</i>
13.1	PEP	15
13.2	PEP Log.....	16
13.3	Sanctions.....	16
13.4	Beneficial Ownership	16
13.5	Anonymous Accounts	16
13.6	Duplicate/Multiple/Shared Accounts.....	17
13.7	High Risk Countries.....	17
14	<i>Cooperation with Regulators and Law Enforcement.....</i>	<i>17</i>
15	<i>Regular Review and Internal Audit.....</i>	<i>17</i>
16	<i>Non-Compliance</i>	<i>17</i>
17	<i>Contact Information</i>	<i>17</i>
18	<i>Board Approval</i>	<i>18</i>

1. Abbreviations

- **AML:** Anti Money Laundering
- **CDD:** Customer Due Diligence
- **CFT:** Counter Financing of Terrorism
- **CFP:** Counter Financing of Proliferation
- **CGA:** Curaçao Gaming Authority
- **EDD:** Enhanced Due Diligence
- **FIU:** Financial Intelligence Unit of Curaçao
- **KYC:** Know Your Customer
- **PEP:** Politically Exposed Person¹
- **POI:** Proof of Identity
- **POA:** Proof of Address
- **SAR:** Suspicious Activity Report
- **SOF:** Source of Funds
- **SOW:** Source of Wealth
- **VIP:** Very Important Player

2. Policy Statement

Moonrail Limited B.V. (the “Company” or “Moonrail”) is a licensed and regulated igaming operator offering gambling services to end customers. The Company recognizes the money laundering and terrorist financing risks that are inherent to igaming and has therefore enacted this policy.

This policy applies to Moonrail and all its related companies in prohibiting and actively working to prevent money laundering, financing of terrorism and proliferation, or other criminal activities.

Moonrail’s AML/CFT/CFP policies, procedures, and control mechanisms function together to ensure compliance with applicable laws and regulations.

The policy applies to all Moonrail operations, group companies, and for all player accounts. If there is a discrepancy in scope or efficiency in applicable laws and regulatory guidelines, the most stringent shall be applied across the entire company and all who work for Moonrail.

The policy has been approved by the Board of Directors.

¹ As defined in FATF Guidance Politically Exposed Persons (Recommendations 12 and 22)

3. Applicable Laws and Regulations

Moonrail is supervised by the Curaçao Gaming Authority (CGA) in accordance with the National Ordinance on Games of Chance (N.G. 2024,157). Additionally, the Company's AML/CFT/CFP Policies and Procedures were created and are subject to:

- a. The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- b. The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- c. Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- d. Sanctions National Ordinance (N.G. 2014, no. 55);
- e. Kingdom Sanction Act (N.G. 2016, no. 54);
- f. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- g. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- h. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- i. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- j. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- k. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- l. CGA, *Regulations for combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction*, January 2025.

Moonrail understands that the above listed laws and regulations along with any future updates constitute the legal basis for the Curaçao's gambling sector in its efforts to combat money laundering, financing of terrorism and the financing of the proliferation of weapons and as such is fully committed to complying with these laws and regulations.

Additionally, Moonrail is committed applying the strictest regulation and ensures to stay updated to regulatory changes and alerts and recommendations issued by FATF-GAFI (Financial Action Task Force), CFATF-GAFIC (Caribbean Financial Action Task Force), and Moneyval (Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism). The Company, furthermore, upholds compliance with the six European Union Anti-Money Laundering Directives.

4. Money Laundering (ML) Terrorist Financing (TF) Proliferation Financing (FP)

Money laundering is the process by which criminals attempt to conceal and disguise the true origin and ownership of the proceeds or any other benefits of their criminal activities. This allows them to avoid prosecution, conviction, and confiscation of their criminal funds. The process consists of three stages:

1. Placement: Illicitly obtained money first enters the financial system at the placement stage, where the cash generated from criminal activities is converted into monetary instruments.
2. Layering: The connection between the funds and the criminal is obscured.
3. Integration: The funds are invested or recovered in a way that appears legitimate.

Terrorist financing involves the solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organisations. These funds may originate from both legal and illicit sources.

Proliferation financing is generally described as the provision of funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons, their means of delivery, and related materials.²

² CGA, *Regulations for combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction*, January 2025 p.7.

5. Responsibilities

5.1 Board of Directors

The Board of Directors is responsible for the development and implementation of Moonrail's compliance framework. The Board of Directors reviews Moonrail's annual risk assessment and compliance report and approves this policy in writing annually.

5.2 Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for developing, implementing, and overseeing all AML, CFT and KYC procedures, controls, and systems for Moonrail's licensed operations.

The MLRO's duties are to:

- Development and supervision of all internal AML policies and procedures as well as the risk assessment.
- Liaise with third party suppliers.
- Conduct staff AML training.
- Receive and evaluate any suspicious activity reports.
- Liaise with the FIU Curaçao and the gambling license supervisor.
- Perform an annual review of Moonrail's AML/CFT policy, its effectiveness, and internal SARs, which shall be delivered to the board of directors.
- Inform relevant changes to AML/CFT laws as applicable to the business and communicate changes to this AML Policy to all relevant employees.
- Respond to AML-related incidents and provide reports during the incident and a report thereof to the board of directors. This response and report may be included in the suspicious activity report.

The MLRO reports directly to the Board of Directors, which in turn has the ultimate responsibility for AML/CFT compliance. The MLRO has access to all Moonrail's data and systems to enable uninterrupted ability to fulfil his or her duties.

Moonrail has appointed a Compliance Officer who shall, for the time being, fulfil the role of MLRO.

6 Business Risk Assessment

An annual risk assessment is performed to assess the risks related to money laundering and terrorist financing or proliferation financing as well as the effectiveness of Moonrail's AML controls and

systems. The MLRO is responsible for ensuring that the assessment is carried out on an annual basis.

The assessment shall be in written form and prepared by the MLRO carefully studying each aspect of the business, interviewing senior management, and performing spot checks. It shall also detail measures taken to effectively manage and mitigate identified risks, changes in risks since the previous assessment, and assess the severity, implications, and possible mitigations of remaining risks.

The purpose of the risk assessment is to:

- Identify gaps or opportunities for improvement in the AML policies, procedures, processes, and systems.
- Assess and make informed decisions about Moonrail's risk appetite and implementation of adequate controls.
- Assess allocation of resources and technology for AML/CFT purposes.
- Develop risk mitigation strategies.
- Ensure the Board of Directors and senior management are aware of risks, gaps, and remediation efforts.
- Assist the Board of Directors and senior management with strategic decisions in relation to AML/CFT.
- Assist the Board of Director with ensuring that resources and priorities are aligned with their risks.
- Ensure that the regulator is made aware of the risks, gaps, and remediation efforts.

When assessing the risks related to money laundering and terrorist financing in Moonrail's activities, we consider the following risks and indicators:

- Customer Risk
 - Assess the risk a customer poses to Moonrail.
 - Who is the customer?
 - What type of customer? B2B, B2C, VIP, PEP?
 - Geographical location of customer's country of origin and residence.
 - Customer's occupation.
 - SOW and SOF checks.
 - Changes to the customer's normal, expected pattern of behaviour.
- Delivery Channel Risk
 - Identify the risks associated with serving customers entirely via the internet.

- Consider the impacts to this risk of using a third-party KYC vendor to perform video-based verification of comparing a valid identity document with a selfie of the person.
- Payment Risk
 - Identify the payment methods used and to what degree the payment methods may be attractive for money laundering or financing of terrorism.
 - Determine if the player is using multiple payment accounts to move money from one to another.
 - Assess changes in payment method usage and identify how these changes affect Moonrail's risks. Are players using payment methods of higher or lower payment risk? Does the Company fully understand the risk posed by different payment methods?
- Country and Geographic Risk
 - Identify and assess the geographic locations which may pose a higher risk of money laundering or financing of terrorism. Moonrail evaluates the specific risks associated with doing business in, accepting customers from, or facilitating transactions involving certain geographic locations. Moonrail will not accept customers from:
 - Countries subject to sanctions.
 - Countries identified as supporting terrorism.
 - Jurisdictions and countries monitored for deficiencies in the effectiveness of their AML/CFT laws and their enforcement.
 - Jurisdictions and countries identified as non-cooperative by FATF-GAFI, CFATF-GAFIC, Moneyval, or the government of Curaçao.
 - The MLRO shall inform the board of directors and senior management of jurisdictions and countries from which the Company shall not accept players or work with any type of supplier or other business counterpart.
- Product Risk
 - Consider the type of product used by the customer.
 - Consider the risks associated with different products and include this risk assessment when developing new products.
 - Games of chances: casino-style games, coin flip.
 - Games of mixed chance and skill: match betting.
 - Trading: person-to-person trades of virtual goods.

- Supply Chain Risk

- Ensure we only work with reputable service providers, vendors, and suppliers which, where applicable, are duly licensed, regulated, and supervised.
- Perform due diligence on business counterparts under a risk-based approach which may include:
 - Collect evidence (through documents, register searches, public databases) to ensure that such counterparts are duly incorporated.
 - Where the counterparty is licensed, obtain evidence of license.
- We will only work with business counterparts which are subject to adequate AML legislations comparable to that of the EU.
- We execute and record appropriate documentation of procurement, such as contracts, proof of delivery, invoices, receipts, and written communications.

- Employee Risk

- The risks posed by the employees and independent contractors of Moonrail or associated companies. We restrict access to sensitive financial, payments, and customer data information systems. The Company also provides AML training on an annual basis to all employees with relevant duties such as customer service, finance, risk/fraud management, and senior management.

7 Know Your Customer (Customer Due Diligence)

Customer Due Diligence (CDD) is a crucial tool for effectively managing Moonrail's risks and protecting the Company from potential financial crimes and related activities. By adopting a risk-based approach, Moonrail ensures that measures to prevent and mitigate money laundering and financing of terrorism are commensurate with the identified risks. This enables Moonrail to allocate resources efficiently.

For this purpose, and as part of the customer acceptance policy of the Company, an initial customer risk assessment is performed, taking into account factors such as the type of customer, geographic location, products and services used, betting and spending behaviour (gambling and transactional behaviour), Fraud and AML red flags triggered, payment method, and any other relevant risk indicators identified throughout the duration of the business relationship. This assessment helps determine the level of customer due diligence required and identifies which customers require enhanced monitoring based on their risk classification (Low, Medium, High).

Furthermore, Moonrail only allows customers to open accounts that are personal, individual, in their own name and controlled by the customer. Only customers who have registered an account and provided personal information are permitted to deposit money into their account.

CDD is divided into two levels:

1. Basic Customer Due Diligence
2. Enhanced Due Diligence

7.1 Basic CDD

Basic Customer Due Diligence (Basic CDD) is applicable to all customers. Basic CDD measures applied by the Company entails the identification and verification of identity of customers, address verification and requesting information regarding the Source of Funds.

During registration and prior to making their first deposit (payment), customers are required to provide personal information such as full name, email address, date of birth, and address and country of residence.

These details are verified on a risk-based approach using third-party databases and systems and/or manual verification, by manually or automatically verifying documents submitted by the customer, such as POI, POA.

The third-party system performs PEP and Sanctions checks automatically against lists issued by OFAC (*Office of Foreign Assets Control, USA*), FATF (*Financial Action Task Force, intergovernmental*), HMT (*HM Treasury's Office for Financial Sanctions Implementation, United Kingdom*) and the EU Consolidated Financial Sanctions List.

These checks are performed before establishing a business relationship with the customer and before allowing them to make an initial deposit. By conducting PEP and specifically Sanction Checks, Moonrail is able to identify individuals who may appear on sanctions lists prior to establishing a business relationship. Through ongoing monitoring and periodic reviews, such individuals may also be detected during the course of the business relationship. Upon identification of a sanctioned individual, Moonrail, complies with its legal obligations by submitting an Unusual Transaction Report to the FIU. Additionally, the account of the customer undergoes increase monitoring until further instructions from relevant authorities to block or freeze the account in question in accordance with applicable local laws and regulations.

7.2 EDD

Enhanced Due Diligence (EDD) is required when a customer and product/service combination is considered to be higher in risk and in relation to any transaction that amounts to 2,000 EUR or more (currency equivalent), whether the transaction is executed in a single operation or in several transactions which appear to be linked.

In any case, EDD shall be carried out if any of the following indicators are manually or automatically detected:

- We suspect the customer may be a minor.
- We identify suspicious information provided by the player, such as customer details which are not commensurate with the normal, expected customer profile.
- A customer's total lifetime deposits or withdrawals reach 2,000 EUR.
- A customer is using multiple payment methods.
- A customer has a suspicious deposit pattern, such as name on cards not matching customer's account, high deposit amounts, or high deposit velocity.
- A customer is identified as a PEP.
- A customer qualifies as VIP.
- A customer is from, is resident, or logs in from an IP address in a high-risk country.
- A customer shows any High-Risk Factors(see below).
- We have any suspicion that Moonrail is being used for money laundering or funding of terrorism by the customer or players linked by IP address or other customer data parameters.

In performing EDD, we shall:

- Perform additional identification checks via further documents, data, and information, for example requesting POI, POA, SOF, SOW.
- Take additional measures to verify or certify documents, for example requesting certified, notarized, or apostille copies.
- Ensure that deposits and withdrawals are from and to the same person and account.
- Search public sources for adverse information and negative information about the customer.

7.3 Ongoing Due Diligence

Customers are continuously evaluated through the Ongoing Monitoring system as well as manual controls. If a customer is, through automatic or manual controls, found to act in a manner that is

suspicious, they may be required to undergo Basic CDD or EDD even if they have already done so.

8 Other Due Diligence

8.1 B2B

B2B partners are generally licensed in reputable jurisdictions to provide gambling products, payment processing and/or financial services and are therefore expected to have similar AML/CFT procedures in place to those of Moonrail. Moonrail will not work with shell banks or shell companies that do not have a substance in the EU or their country of incorporation.

8.2 Third-Party Providers

When appropriate, Moonrail will carry out corporate due diligence on third party companies that it intends to contract with. CDD may include use of a third-party database to verify CDD information.

8.3 Retrospective

Moonrail may by using a risk-based approach decide to do retrospective remediation on existing accounts, where deficiencies are identified or when the Company deems it necessary.

9 Ongoing Monitoring and Reliance on Third-Party Tools

Moonrail performs ongoing monitoring on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, their spending patterns, gambling preferences, and risk profile, including, where necessary, the source of funds and source of wealth.

Every payment transaction is subject to monitoring by an external tool (SEON) and every player which is subject to due diligence is checked by an external tool (Shufti Pro) to ensure validity and authenticity of identity documents and subject to PEP and sanctions screening. Additionally, transactions and players are subject to spot checks.

Virtual currency transactions are monitored and screened using Chainalysis.

If any unusual or suspicious behaviour is identified, further investigation is performed in order to determine whether to keep the relationship, request further documentation, terminate the relationship and/or report it to the authorities accordingly.

The Company performs repeated due diligence on customers every two years, if the customer is still using the services. Specifically, high- risk customers are reviewed annually for due diligence purposes, or sooner if a risk event occurs that requires an earlier assessment such as significant changes in their individual status, or gambling and transactional behavior. In any case, repeat due diligence is applied as and when risks/indicators are detected.

10 Training

Moonrail provides training to all new employees and refresher training for all current employees annually to ensure all employees are aware of relevant subjects:

- Anti-Money Laundering and Counter Financing of Terrorism and the Counter Financing of Proliferation
- Fraud Prevention
- Information Security
- Identification and reporting of suspicious transactions
- Responsible Gambling

All training is managed, administered and reported upon by the MLRO.

The Payments and Customer Services team receives specific training on monitoring reports regarding customer registration, payment patterns, gambling activities, and personal information for indications of money laundering and how to respond to alerts or suspicions of money laundering or terrorist financing activities.

11 Record Keeping and Data Retention

As required by AML/CFT requirements, Moonrail keeps records of the procedures applied to establish the identity of our customers and their transactions history, for at least 5 years after the relationship ends or longer as required by applicable laws.³ The Company also keeps records of the data collected.

The records are stored electronically.

³ Article 11a, National Ordinance on the Reporting of Unusual Transactions (N.G.2017, no.99).

12 Reporting Suspicious Activities

12.1 Suspicious Activity Report (SAR)

Moonrail has a clear process in place for the submission of internal SARs. The process as well as the Internal SAR forms are available on the intranet and accessible by all employees.

Employees are aware of, and reminded by internal communications, who the MLRO is. The MLRO is accessible by all employees.

For every written SAR received, the MLRO will provide the employee with an acknowledgement.

The MLRO will assess all internal SARs and, after thorough investigation, decide whether or not to file an SAR (*Unusual Transactions Report*) with the FIU Curaçao through the Curaçao On-line Reporting System (GoAML).

The MLRO will also consider whether a report should be made to other supervisory or law enforcement authorities.

Regardless of whether the SAR is reported to the FIU Curaçao or other supervisory or law enforcement, a copy of the original SAR shall be stored for a period of at least ten years.

12.2 Tipping Off

When an employee submits an internal SAR, the MLRO provides an acknowledgement to serve as:

- Evidence that and safeguard for the employee who submitted the SAR that they have fulfilled their legal obligation of reporting any suspicious activity.
- A reminder that tipping off (directly or indirectly informing the customer that a SAR has been filed) is an offence.
- A reminder that if in doubt they should only contact the MLRO with their concerns.

13 High Risk Factors

13.1 PEP

Under a risk-based approach, if a customer is identified to be a PEP, the account must be blocked from making payments or placing bets until the MLRO has approved the account.

EDD must be performed.

The MLRO must be satisfied that the identified PEP does not pose any risk to the Company. In assessing the risk, an important factor is the location of the PEP and whether the PEP is from a high-risk jurisdiction. To assist in the assessment and ultimate decision on whether to continue with the relationship, Moonrail uses available third-party databases that allow it to compare the registration details of the customer with information contained on this database.

13.2 PEP Log

Any identified PEP is recorded within the PEP Log, to enable the MLRO to set up regular reviews and monitoring of these customers. This way, the Company can identify any relevant changes which might increase the risk of the relationship and change the decision to accept the account.

13.3 Sanctions

Moonrail will not knowingly engage in any form of business with any person who is on a relevant international sanctions list.

Sanction checks are performed as part of basic due diligence.

The sanctions lists used are:

- Consolidated list of persons, groups and entities subject to EU financial sanctions: [Consolidated list of persons, groups and entities subject to EU financial sanctions - European Union Open Data Portal](#)
- US OFAC: [OFAC Sanctions List Search](#)
- Additional lists may be used by third-party sanctions checks vendors.

If a customer is on a sanction list a report will be sent to the FIU immediately. Moonrail will support the FIU if it becomes necessary to freeze, seize, or surrender funds under the control of a person or institution on the sanctions list.

13.4 Beneficial Ownership

Moonrail does not allow corporate customers or third-party, proxy, or beneficial ownership of accounts.

13.5 Anonymous Accounts

Moonrail does not allow anonymous accounts.

13.6 Duplicate/Multiple/Shared Accounts

Moonrail does not allow multiple, joint, or shared accounts. Accounts are personal and may only be used by one person. Accounts may not be shared or traded.

13.7 High Risk Countries

Customers with a connection to a high- risk country is subject to EDD. A list of high- risk countries is maintained by the MLRO and is available to all employees.

14 Cooperation with Regulators and Law Enforcement

Moonrail is fully committed to working with and cooperating fully with the relevant competent authorities and any law enforcement agency as required.

15 Regular Review and Internal Audit

This policy is reviewed annually or earlier if there is a change to our business, legislation or regulation that might impact its content.

The policy shall be reviewed by an internal auditor or other independent third party on an annual basis.

16 Non-Compliance

It is the responsibility of all employees to comply with this policy. Failure to do so, will be considered gross misconduct and can result in employee dismissal. Additionally, the Company understands that there are legal implications and regulatory repercussions for non-compliance with its AML/CFT/CFP obligations, and thus with this policy. The Company may face administrative fines, penalties, and regulatory actions, such as the revocation of its gambling license, for failing to comply with applicable AML/CFT/CFP laws and regulations.

Furthermore, the Company is aware of the reputational damages and financial losses that can result from such non-compliance.

17 Contact Information

For any questions regarding this policy, please contact:

Name: Pearl Reiph

Email: preiph@xcm.cw

Phone: +5999 843-0013

18 Board Approval

As of the latest date set out in the versions table above, the board of directors of the Company have reviewed and agreed to this policy.

Analissa Heiland/Lorenza Godett
Directors obo Xecutive Corporate Management B.V.

INTERNAL SUSPICIOUS ACTIVITY REPORT

INSTRUCTIONS:

1. Complete all fields in Parts 1 through 3 of this form.
2. In Part 1, you can create additional tables if you want to report multiple parties at the same time.
3. If details are not known, please state so.
4. Submit the form to the MLRO (**PEARL REIPH**) via email: [**PREIPH@XCM.CW**]
5. The subject of the email should be:
Suspicious Activity Report (SAR)
6. If the case requires urgent attention or if you need help, please speak to the MLRO right away.

Do not disclose to any of the involved parties that you have submitted a SAR. Doing so is called *tipping off* and is an unlawful act.

WHEN SHOULD YOU SUBMIT A SUSPICIOUS ACTIVITY REPORT (“SAR”):

You should submit a SAR if:

- You suspect that a customer, partner, vendor, supplier, or other business counterparty of the company is, was, or will be involved in money laundering, funding of terrorism, located in a forbidden country or territory, or involved in any kind of activity that you believe is unlawful.
- You should also file a SAR if you suspect an employee of any of the above mentioned.
- You should submit even if the SAR does not involve **MOONRAIL LIMITED BV** and instead applies to another group company, such as **JHOLT LTD**.

IMPORTANT: You do not need the approval of your manager or anyone else to submit a SAR. If someone attempts to stop you from submitting a SAR, immediately notify the MLRO.

PART 1: INVOLVED PARTIES

Create as many tables as required for your case.

INDIVIDUAL <i>Use this table when an involved party is an individual</i>	
Customer reference number <i>If applicable</i>	
Name <i>If known and if applicable, include known spelling variants or different alphabets</i>	
Date of Birth <i>yyyy-mm-dd format</i>	
Passport/ID number	
Nationality <i>Add multiple if applicable</i>	
Address	
Contact details <i>Insert any phone number, email address, user ID, Discord username, and so on</i>	
IP address <i>Insert any known IP addresses</i>	
Additional details <i>Any other details that be known about the individual</i>	
Involvement <i>This should indicate the involvement as you understand it of this party in the activity you are reporting, eg client of the firm</i>	

NON-INDIVIDUAL <i>Use this table when an involved party is an entity</i>	
Reference number <i>If applicable</i>	
Name <i>If known and if applicable, include known spelling variants or different alphabets</i>	
Registration number	
Jurisdiction	
Address	
Contact details <i>Insert any phone number, email address, Discord username, and similar</i>	
Additional details <i>Any other details that be known about the individual</i>	
Involvement <i>This should indicate the involvement as you understand it of this party in the activity you are reporting, eg client of the firm</i>	

PART 2: REASON FOR SUSPICION

Guidance:

Begin with a summary to explain your suspicion.

Next, provide a chronological sequence of events. Keep it clear and simple, so that someone who doesn't know what you know can easily understand what has happened and why you believe it is suspicious.

For example, explain how you became aware of the suspicious activity, the order of events, and how and why you find them suspicious.

- **Who?** Who are the involved parties?
- **What?** What did the parties do.
- **Where?** Where did this take place? In person, online, in chat, in voice conversation, via emails?
- **When?** Times and dates of events.
- **Why?** If you know the reasons for the activities, please provide.
- **How?** How were the suspicious activities performed?

Remember to include details about products and services used.

PART 3: SUPPORTING DOCUMENTS

Attach any supporting documentation that is relevant for the case. For example, this may include copies of correspondence, customer files or information that you have obtained on the matter.

For each file attached, ensure that an explanation is provided of what it is, as this will help the third party when reviewing the case.

Attach the files separately. List the files here. Describe why you believe the file is relevant to the suspicious activity.

PART 4: YOUR DETAILS

Name	
Contact details	
Date of report <i>The date when you submit the report; not the date when the suspicious activities took place</i>	

Note that you are allowed to submit anonymously. However, it may be helpful if the MLRO is able to contact you for further information.

FOR MLRO'S USE

Date received	
Internal report reference number	
MLRO's assessment, decision, and reason for specific decision	
Date reported to the FIU <i>If applicable</i>	
External report reference number <i>If applicable</i>	