

LUCKYROO N.V.

AML/CFT Policy



Abraham de Veerstraat 1,
Willemstad, Curaçao

Approval Date	Next Review	Author	Approved by
28 May, 2025	May, 2026	Abdulrasaq Folorunsho (Compliance Officer) compliance@luckyroo.net	The Board of Directors
05 December, 2025	December, 2026	Abdulrasaq Folorunsho (Compliance Officer) compliance@luckyroo.net	The Board of Directors

A handwritten signature in black ink is placed over a circular official stamp. The stamp contains the text "MORGANITE CORPORATE SERVICES B.V." and "KONINKRIJK DER NEDERLANDEN" around the perimeter, with a small logo in the center.

Morganite Corporate Services B.V.
Managing Director

Contents

1. Purpose of the Policy	3
2. Money-Laundering.....	10
3. Terrorist- Financing.....	10
4. Proliferation Financing.....	11
5. National Risk Assessment (NRA) Integration.....	12
5.1. Risk Score Calculation	13
5.2. Ongoing Monitoring.....	15
6. Risk- Based Approach (ML/ TF risks' detection)	16
7. Client Due Diligence Guidelines (CDD, EDD) and Acceptance Policy (CAP)	22
7.1. The company applies CDD measures	23
7.2. To establish a player's identity, the following information will be collected:	24
7.3. Timing of Client Due Diligence Measures.....	24
7.4. Beneficial Ownership Identification and Control Structure Verification	28
8. Transaction Monitoring.....	29
8.1. Components of Luckyroo N.V.'s transaction monitoring system	30
9. Politically- Exposed Persons (PEPs)	31
10. Sanctions Management, FATF High-Risk List, License Restrictions	31
11. Suspicious Activity Reporting Guidelines	32
11.1. Identifying Unusual Transactions.....	33
12. Compliance Officer	34
13. Senior Management Responsibility	36
14. Employee Training and Screening Program.....	36
15. Record- Keeping.....	38
16. AML Compliance Audit.....	39
17. Regulatory Access and Cooperation.....	40
18. Internal Audit and Reporting.....	41
19. Appendixes.....	42

1. Purpose of the Policy

The purpose of the Anti-Money-Laundering Policy (the AML Policy) is to combat money laundering and terrorism financing, implement best AML/CFT industry standards, and promote company-wide compliance with the local and international Anti-Money Laundering/ Counter Terrorism Funding (AML/CFT) legislation. The AML Policy's uniform framework is based on robust AML/ CFT measures, including the identification and mitigation of the inherent risks associated with clients, products and services, payment methods, countries, and delivery channels.

The design, implementation, and monitoring of the AML policy's framework is approved by Luckyroo N.V.'s (hereinafter – the “Company”) Board of Directors (BoD) and is subject to an annual review. In addition to the annual review process, the AML Policy may be amended from time to time to reflect material changes in the AML/CFT legislation or operator practices. Furthermore, a nominated officer may put forward suggestions to implement urgent internal and third- party AML audit recommendations as regards risk probability and risk impact.

First and foremost, the AML Policy is a reflection of the main international objectives highlighted by the current AML/ CTF legislation in Curacao i.e. the upcoming National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, The National Ordinance on Offshore Games of Hazard (PB 1993, no.63) (NOOGH) as well as National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification of clients when Rendering Services (NOIS). The AML Policy also reflects the international legislation and policy initiatives such as Recommendations of the Financial Action Task Force (The FATF Recommendations), the European Anti-Money Laundering Directives (the 4th, 5th and the 6th AMLDs), and the Wolfsberg Principles as a best practice.

As of May 15, 2024, new regulations for combating money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction have become applicable to online casinos in Curaçao. New regulations came into force September 1, 2024. Non- compliance with these regulations can result in severe administrative and criminal sanctions, underscoring the seriousness with which Curaçao authorities are approaching AML/CFT enforcement

The AML/CFT/CPF Regulations are aligned with the FATF Recommendations, alongside the various AML/CFT/CPF legislations in Curacao.

To summarize, the AML Policy was drafted with the view of complying with the recommendations of the AML/CFT supervisor in Curacao, namely the Curacao Gaming Control Board. The Company's directors, officers, and personnel are committed to upholding the set of standards set in the Policy. The Policy applies to all people at all levels working for the Company and third-party consultants whose services are enlisted from time to time for audit purposes.

Online Gaming Industry Specifics

Luckyroo N.V. (hereinafter – the “Company”) is a Curacao-based legal entity which currently runs the following websites: www.betwinner.llc

Luckyroo N.V. (hereinafter – the “Company”) operates under the Curacao online gaming OGL/2024/1371/0694 issued by Curacao Gaming Control Board. It therefore complies with the licensing requirements as well as regional operational restrictions imposed on it by the Curacao

regulatory authorities which explicitly bans their remote gaming licenses from offering their services in the US, Australia, Dutch West Indies (Aruba, Bonaire), Curacao, France, Germany, the UK, Belize, and the Netherlands. The Company only operates in markets where it is permitted to operate and does not solicit clients from those jurisdictions where online gambling is explicitly banned i.e. Qatar or where it is imperative to have a locally obtained permit/ license.

Overall, gaming and betting operators are susceptible to the money laundering risks spanning identity theft and fraud, structuring, layering and collusion of the employees with the clients or the external payment providers to help them bypass internal safeguards.

Key Definitions

AML Policy- The Policy on Prevention of Money-Laundering Terrorist Financing.

Anti-Money Laundering and Counter -Financing of Terrorism Program- programs are established to fight against money laundering and terrorist financing and consist of written internal policies, procedures and controls, overseen by AML compliance team headed by Compliance Officer, who is also responsible for AML training as well as arranging an independent review to audit the program.

Alert - a notification that an analysis of red discrepancies is required based on defined red flags and underlying typologies.

AML/CFT Supervisor- the Curaçao Gaming Control Board (GCB) and a relevant local master license holder where applicable.

Automated Screening Tool (AST)- Software systems that automate the clients' screening process including against sanctions lists.

Beneficial Owner – a natural person who ultimately owns or controls an account through which a transaction is being conducted.

FATF high-risk list- An internal list of names (including places, persons, entities, and individuals) that are screened to identify any sanctions exposure, in addition to government and vendor-maintained sanctions lists.

Comprehensive Sanctions- Sanctions that prohibit all transactions and activity with a sanctioned country by the sanctioning country except in rare, specific instances.

Criminal Proceeds- Any property derived from or obtained, directly or indirectly, through the commission of a crime. **Client-** a person that opens an account and transacts with the Company.

Client Relationship- a client relationship encompasses all contact with a prospective client during onboarding and while using the Company's services and products.

Client Due Diligence- a set of internal controls that internet gambling operator establish a client's identity, predict with relative certainty the types of transactions in which the client is likely to engage, and assess the extent to which the client exposes it to a range of risks (i.e., money laundering and sanctions). Organizations also need to know their clients through CDD to guard against fraud and comply with the requirements of relevant legislation and regulation. "High-risk third country"- a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers and by FATF, and which has strategic deficiencies

in its national AML/CFT regime that pose significant threats to the financial system of the Union, and a third country which is classified by the Company as high risk, according to the risk assessment referred to in Article 58a of the Law.

Due Diligence- The investigation and examination of a company or group, conducted in the process of preparing for a business transaction. Due diligence should be completed before entering into any financial transaction or business relationship.

Economic Sanctions- The imposition of trade or financial restrictions and penalties by one or more countries against another country, entity, or individual with the purpose of changing a behavior. Economic sanctions can include actions such as tariffs, trade restrictions, and financial limitations.

Embargo- An official government action to ban trade or commercial activity with a specific country, sometimes involving a specific trade product (e.g., a grain embargo or an oil embargo). **Enhanced Due Diligence (EDD)-** In conjunction with Client Due Diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk clients. It requires developing a more thorough knowledge of the nature of the client, the client's business and understanding of the transactions in the account than a standard or lower risk client.

European Union (EU)- The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico-economic union of member states located primarily in Europe. **European Union Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing-** First adopted by the European Union in June 1991 and updated in 1997, 2005, 2015, 2018 and 2020 the directive requires EU member states to prohibit and manage the risks of money laundering and terrorist financing.

Exclusions List- A list of names that are excluded from the screening process. These are names that the compliance team has verified do not actually match a name on a sanctions list.

Financial Action Task Force (FATF)- FATF was created in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter- terrorist financing measures worldwide.

Financial Intelligence Unit (FIU)- A central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to appropriate authorities.

First Line of Defence- within the governance structure of a sanctions compliance program, the first line of defence (also referred to as the "front line") includes relationship managers and other client-facing employees who are closest to the clients and counterparties during the onboarding and contracting phase of relationships. The first-line defence is responsible for ensuring that adequate information is obtained so that effective screening of clients and their owners and controllers can be performed. In general, the first-line defence owns and manages the collection of SDD information.

Grey list- A grey list is a list of entities that are suspicious or higher-risk for causing a negative impact to a firm. Within the context of sanctions, the grey list includes the names of countries with strategic deficiencies in anti-money laundering and counterterrorism financing regimes. Moreover, these countries have also not made sufficient progress or otherwise committed to action plans to address deficiencies identified by FATF

Minor – is any person under 18.

Inherent Risk- The level of sanctions risks that exist before controls are applied to mitigate them. There are four main inherent risk categories: clients, products and services, countries, and delivery channels. Inherent risk is linked to the risk assessment process, which evaluates the effectiveness of an institution's risk controls. Inherent risk considers the likelihood and impact of noncompliance prior to considering any mitigating effects of risk management processes.

Investigation- The process of obtaining, evaluating, recording, and storing information about an individual or legal entity with whom one is conducting business, in response to an alert indicating a possible sanctions violation. Investigations often begin with simple checks before progressing to further investigation such as account review, client outreach, and possible escalation to the compliance function.

Know Your Client (KYC)- Anti-money laundering policies and procedures used to determine the true identity of a client and the type of activity that is "normal and expected," and to detect activity that is "unusual" for a particular client.

Know Your Employee (KYE)- Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

Layering- The second phase of the classic three-step money laundering process between placement and integration, layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.

Mandatory Sanctions Lists- Supranational sanctions lists, such as those including targets designated by the United Nations Security Council Resolutions (UNSCR), which must be screened against. Depending on the country in which a business is located and operates, local sanctions regimes may be required (i.e., mandatory) and would need to be included within a firm's sanctions compliance program.

Money Laundering - The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly- derived property or funds to make them appear legitimate. It usually involves a three-part system: placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds, and integration of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

Compliance Officer - A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The Compliance Officer is the key person in the implementation of anti-money laundering strategies and policies.

Monitoring- An element of an institution's anti-money laundering program in which client activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the client.

Office of Foreign Assets Control (OFAC)- the agency within the US Department of the Treasury responsible for administering and enforcing economic sanctions issued as part of US foreign policy and by international organizations like the United Nations against targeted foreign countries. It often works in consultation with other agencies, such as the Department of State, to oversee national security

goals. A core component of the agency's responsibilities is the creation and maintenance of the Specially Designated Nationals (SDN) list.

Politically Exposed Person (PEP) - According to FATF's revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle - ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

Red Flag (similar to alert)- A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

Regulatory Agency- A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction.

Risk Appetite- The amount of risk that a firm is willing to accept in pursuit of value or opportunity. A firm's risk appetite reflects its risk management philosophy and comfort level for undertaking business in situations in which there could be an elevated sanctions risk. In turn, risk appetite influences the firm's culture and operating style and guides resource allocation. An organization's risk appetite is determined through the risk-assessment process and formalized in a Risk Appetite Statement or Framework. A business should determine its risk appetite based on the resources it has to invest in controls, staffing, and measures to protect its reputation. Firms can have an overarching risk appetite (i.e., enterprise-wide) and/or have risk appetites defined on a more granular level (e.g., by department).

Risk Assessment- A tool that allows a business to identify and assess the extent to which it may be exposed to risks.

Risk-Based Approach- The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions to maximize the effectiveness of an anti-money laundering program.

Senior Management- an officer or employee of the Company with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the Board of Directors.

Structuring - small transfers or small deposit amounts from clients that are trying to avoid recordkeeping requirements or trigger AML flag alerts from any company (EMI).

Sanctions- Sanctions are punitive or restrictive actions taken by individual countries, regimes, or coalitions with the primary purpose of provoking a change in behavior or policy. Sanctions can restrict trade, financial transactions, diplomatic relations, and movement. They can be specific or general in their implementation and enforcement. Sanctions are also referred to as restrictive measures.

Sanctions Evasion- The deliberate attempt to remove or conceal the involvement of sanctioned places, entities, or individuals in a transaction or series of transactions. When sanctions evasion is successful, a business that would have been flagged, taxed, restricted, or prohibited is allowed to proceed unhindered. **Sanctions Due Diligence (SDD)** -A similar process to Know Your Client (KYC) / Client

Due Diligence (CDD) that focuses on the risks specific to sanctions, taking into account governance and risk assessment. SDD builds upon the KYC/CDD information an organization collects as part of its existing AML program. SDD is applied throughout the life cycle of a relationship at the start of a relationship (i.e., onboarding); when new products are introduced, in response to trigger events during a relationship, such as a "match" generated by a screening tool; during periodic reviews; and when a relationship ends.

Sanctions List- A document or database listing individuals, legal entities, and countries with whom it is illegal to do business.

Sanctions Regime - A set of sanctions that have a common nexus or theme. These are either referred to by the issuer of the set of sanctions or by the intended purpose of the set of sanctions. For example, the "OFAC sanctions regime" or the "North Korea sanctions regime." Depending on the context, a sanctions regime may be limited to unilateral sanctions or may include multilateral sanctions.

Sanctions Compliance- The act of adhering to the sanctions-related legislation, regulations, rules, and norms that make up the complex sanctions landscape.

Second Line of Defense - The sanctions compliance function, the larger compliance function, and the human resources and technology departments comprise the second line of defense within the governance structure of a sanction's compliance program. The sanctions Compliance officer ensures ongoing monitoring for sanctions compliance to enable the escalation of identified issues. In general, the second line exists to ensure that SDD procedures and processes applied by the first line are designed properly, firmly established, and applied as intended. The second-line defense reviews the effectiveness of controls used to mitigate sanctions risks; provides information to the first line; and investigates possible noncompliance with sanctions restrictions.

Simple Checks - One of the first steps in an investigation, simple checks are those initial actions taken to discount or confirm a sanctions link; an example of a simple check includes comparing data about a sanctions target with a firm's Know Your Client (KYC) data.

Specially Designated Nationals and Blocked Persons List (SDN List) - A list of individuals and companies, published by OFAC, that are owned, controlled by, or acting on behalf of a targeted country. The list also includes groups and people, such as terrorists or drug traffickers, who are associated with a specific crime as opposed to a country. The US Department of the Treasury maintains the list and may name a person or company as an SDN. When the government identifies a person or company as an SDN, it blocks their assets and forbids US persons to do business with them. The government may also impose fines and imprison lawbreakers.

Suspicious Activity - irregular or questionable client behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a client's known legitimate business, personal activities, or the normal level of activity for that kind of business or account.

Suspicious Transaction Report (STR) - A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

Terrorist Financing - The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves

financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

Third Line of Defence - The third-line defence within the governance structure of a sanctions compliance program is the internal audit, which involves independent reviews of the controls applied by the first two lines of defence. It independently evaluates the risk management and controls of the bank through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks. It also evaluates the effectiveness of the staff's execution of the controls, the effectiveness of the compliance oversight and quality controls, and the effectiveness of the training.

Third-Party Database- Third-party databases can be a good source of both primary and secondary information sources. Examples of third-party databases include rating agencies, stock exchanges, and legal databases.

Unilateral Sanctions - These are sanctions imposed by a single country against a targeted entity. These are generally considered less effective than multilateral sanctions. Still, they serve to target specific offensive practices on behalf of imposing nations.

United Nations (UN)- An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. Today, nearly every nation in the world belongs to the UN. See also Vienna Convention. The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money Laundering (GPML), the key instrument of the UN Office of Drug Control and Crime Prevention in this task. Through the GPML, the UN helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime.

Unusual Transaction - Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.

Abbreviations

AML – Anti-Money Laundering

Compliance Officer – Anti-Money Laundering Compliance Officer

BoD – Board of Directors of the Company

CDD - Client Due Diligence

EDD - Enhanced Due Diligence

CFT- Combating the Financing of Terrorism

EU – European Union

FATF – Financial Action Task Force

NOOGH- The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63)

PEP- Politically Exposed Person

UN- United Nations

CPF Counter-Proliferation Financing

2. Money-Laundering

Organized crime operations are based on money laundering, often on an international scale. The illegal origin of criminal proceeds from such crimes as financial fraud, tax evasion, violations of sanctions, bribery, illegal arms trade, drug trafficking, extortion, kidnapping etc. is disguised during its processing, including their identity, source and the destination and equals money-laundering. Therefore, the goal of money-laundering is to make the criminal proceeds appear legitimate from the time the money is placed into the financial system (placement stage), layered in order to hide the audit trail through the web of complex financial transactions at various financial institutions (the layering stage), to the time it is integrated back into the financial system through the purchase of luxury items or cash-intensive businesses (integration stage). Money-laundering has social, economic, legal and regulatory implications on the world economy and leads to increasing costs of monitoring businesses from a compliance standpoint.

The gambling and betting industry therefore is considered high risk since online platforms are vulnerable to money-launderers since online gambling transactions are cross-border and services are often anonymous in a non- face-to-face business. VIP accounts, money services businesses and multiple accounts are just a few challenges that the industry is known for.

Based on the results of the complex business risk assessments, Luckyroo N.V.'s main priority is to detect and deter money laundering threats as well as mitigate such risks in the following areas:

- Using the online platform as a player-to-player transfer route to funnel funds between sellers and buyers and cashing out when necessary.
- Depositing funds obtained from illicit operations and/or using the online platform as “parking”, rather than with the goal of engaging in online gambling or online sports betting.
- Verification fraud and identity theft (client due diligence covering documentation verification, age verification and location verification)
- Operation of multiple accounts and high transaction volumes

This list is not exhaustive and whereas additional risks may materialize from time to time, the Company implements robust KYC procedures to identify high-risk clients, utilizes advanced proprietary software to detect suspicious transaction patterns, offers regular AML trainings to the employees, and conducts regular audits of AML controls and systems.

3. Terrorist- Financing

Providing funds via different methods and sources for carrying out terrorist activities defines the term terrorism financing, including but not limited to direct funding for the planning and execution of terrorist acts or financial support enabling terrorism such as training, recruitment, and propaganda. Money laundering and terrorism financing are two separate crimes which, nevertheless, are often mentioned together. Countering the financing of terrorism is as important as combating money-laundering but its pattern is largely different and is known to comprise small donations from legitimate sources in the form of charitable donations, personal income or business revenue. Illegitimate sources of funds include fraud, criminal activities and money laundering whereas the methods of transfers differ from payment institutions and cryptocurrencies, inter alia. Overall, the FATF (The Financial

Action Task Force) Recommendations 2012-2023 identify client due-diligence, record-keeping, and reporting suspicious activity as main preventive measures that help businesses combat money-laundering. Furthermore, the FATF produced strategic guidance on the AML/ CFT risk-based approach for online casinos where it highlights the vulnerability of online casinos, and gaming sector as regards money laundering (ML) and terrorist financing (TF) risks (page 59, Vulnerabilities of Casinos and Gaming Sector- March 2009) due to the key industry threats associated with the ever evolving techniques of online gambling fraud within the context of limited AML/CFT controls or regulatory responses in many jurisdictions. From the payment methods standpoint, the volume of remote gambling transactions taking place over the online platforms with 24/7 accessibility is so large and the payment methods are so varied, that it is of paramount importance to develop efficient internal controls based on the periodic reviews of the results of the internal AML/CFT risk-assessments. Notably, the 2022 Supranational Risk Assessment Report by the European Commission identified the “gambling sector” and online gambling, as a “high risk” area of AML/CFT concern due to “the non-face-to face element, huge and complex volumes of transactions and financial flows” involving cryptocurrencies among other payment instruments. Prepaid cards have been identified as a highly popular method to acquire materials for the terrorist attacks and therefore it is important to conduct staff training based on newly available information.

The non-exhaustive list of conduct that may be indicative of terrorist financing risk include the following examples:

The parties to a transaction are based in a country or countries that are on a list of state sponsors of terrorism or a sanctions list.

Adverse media/ negative news screening reports indicative of links to the terrorist organizations.

- Small regular deposits that are structured to avoid detection.

4. Proliferation Financing

Proliferation Financing (PF) refers to the use of financial resources to support the development, manufacture, or distribution of weapons of mass destruction (WMD), including their delivery systems. Recognizing the severe global security risks posed by PF, Luckyroo N.V. is committed to preventing its platform from being used, even indirectly, to facilitate such activity.

The company takes a proactive approach by embedding PF-specific controls into its AML compliance framework. These include enhanced risk assessments focused on jurisdictions and client profiles associated with proliferation risk. Where elevated risk is identified, Enhanced Due Diligence is applied to verify the legitimacy of both the client and the financial activity in question.

Luckyroo N.V. strictly adheres to the sanctions regimes issued by the United Nations Security Council, the European Union, the Sanctions National Ordinance (SNO), and the Kingdom Sanction Act (Sanctiewet 1977). All transactions are screened against relevant sanctions lists to ensure no dealings occur with entities or individuals linked to WMD proliferation. By maintaining this level of diligence, the company supports international non-proliferation efforts and safeguards the integrity of its operations.

5. National Risk Assessment (NRA) Integration

Luckyroo N.V maintains a comprehensive AML/CFT/CPF framework designed to prevent its gaming products, services, and platforms from being misused for money laundering, terrorist financing, or proliferation financing. This framework is aligned with Curaçao's legal and regulatory requirements, the expectations of competent authorities, and FATF/CFATF international standards. All employees, management, partners, and service providers are required to follow this framework as part of their operational responsibilities.

The Board of Directors is ultimately responsible for establishing and overseeing an effective AML/CFT program. It ensures that sufficient resources, systems, and qualified personnel are in place to manage the risks associated with online gaming operations. Senior Management supports this oversight by implementing operational controls, ensuring compliance culture, and providing the Compliance Officer with full access to information and systems needed to carry out their duties.

The Compliance Officer is responsible for the day-to-day operation of the AML/CFT program. This includes managing client due diligence, enhanced due diligence, monitoring activities, filing unusual transaction reports, conducting internal investigations, and serving as the primary contact for FIU Curaçao and other supervisory bodies. The Compliance Officer also ensures that internal controls remain aligned with regulatory expectations and national risk developments.

The Company integrates Curaçao's National Risk Assessment (NRA) into its overall risk-management framework to ensure it remains aligned with nationally identified threats and vulnerabilities. The Compliance Officer reviews the latest NRA publications and assesses which risks are relevant to the Company's client base, products, payment channels, jurisdictions, and technological environment. The results of this review are incorporated into the Institutional Risk Assessment, which guides the risk-based approach applied across all AML/CFT processes.

Based on the NRA findings, the Company adjusts its internal controls to address high-risk areas identified for the gaming sector. These adjustments may include enhanced client verification, increased monitoring thresholds, additional transaction surveillance rules, and restrictions or prohibitions on specific jurisdictions or payment channels. When the NRA identifies new threats, the Company evaluates whether its existing controls are adequate or require strengthening.

Client due diligence is a core component of the Company's AML program. All players must be identified and verified according to the Company's KYC standards before withdrawals or after reaching specified thresholds. Verification includes identity checks, age confirmation, ownership of payment methods, and address verification where applicable. Additional checks are conducted when players trigger risk indicators or engage in high-value or unusual patterns.

Enhanced due diligence is applied to clients or activities that pose higher risks. This includes players from high-risk jurisdictions, politically exposed persons, high-value or VIP players, players involved in complex transaction patterns, and any client whose activity aligns with NRA-identified vulnerabilities. EDD may involve obtaining source of funds, source of wealth, adverse media reviews, and approval from Senior Management before continuing the relationship.

Luckyroo N.V conducts ongoing monitoring of client activity using automated tools and manual oversight. This includes monitoring deposit patterns, bet frequency, wagering behavior, streak patterns, device data, and potential misuse of bonuses or value-transfer schemes. Alerts generated through transaction monitoring systems are reviewed promptly, and suspicious activities are escalated to the Compliance Officer for investigation and reporting if necessary.

All unusual or suspicious transactions identified by the Company must be reported to FIU Curaçao in accordance with NORUT requirements. Internal procedures ensure that employees escalate concerns immediately and maintain confidentiality. Under no circumstances may any staff member inform a player that an internal or external report has been filed, as this constitutes tipping off and is prohibited by law.

Luckyroo N.V maintains detailed records of all client identification data, verification materials, transaction logs, monitoring results, internal reviews, NRA integration documentation, and FIU reports for a minimum of five years. Regular training ensures that all staff understand AML/CFT obligations, industry-specific risks, updated NRA findings, and their individual responsibilities. The AML framework is reviewed annually and updated as needed to remain aligned with regulatory expectations, national risk developments, and technological changes within the gaming industry.

5.1. Risk Score Calculation

Money laundering and terrorist financing risks are measured by using a number of factors listed above. Luckyroo N.V uses the application of risk categories to clients/situations to provide a strategy for managing potential risks and it enables the Company to subject clients to proportionate due diligence and ongoing monitoring. The weight given to these criteria in assessing the overall risk of the client and risk score assigned is as follows:

Category	Score	Level of Due Diligence	Approval Process
Low Risk	0-1.8	Standard Due Diligence	Client Service/Compliance Officer
Medium Risk	1.8.-2.5	Standard Due Diligence	Client Service/Compliance Officer
High Risk	2.5 or more	Enhanced Due Diligence	Annual and approval from Compliance Officer
Unacceptable	Any of the factors that are not accepted by the company	Automatically Reject	Automatically Reject

The Risk Score correlates with the level of due diligence imposed on the client and who is responsible for conducting due diligence. Regardless of the risk rating, Luckyroo N.V performs automatic PEP, sanctions and, adverse media screening on all clients as part of the client due diligence process and ongoing risk assessment, ensuring the Firm meets its regulatory requirements and obligations. Further, Luckyroo N.V uses risk score in order to determine the different treatments of identification, verification, additional client information, and monitoring for each client as follows:

Low – Standard Due Diligence applies. Clients in this category present an overall low risk to the Company, however, because of the high-risk nature of online gambling Company will not apply Simplified Due Diligence.

Medium – Standard Due Diligence applies. Clients in this category present an overall medium risk to the Company.

High – Enhanced Due Diligence applies. Clients in this category present an overall high risk to the Company. These clients will be reviewed by the Compliance Officer and approval or rejection, and final sign-off. Some of the high-risk clients include, but are not limited to:

- the business relationship is conducted in unusual circumstances
- the transaction is complex or unusually large compared to the profile of the client or to other clients of similar type/category
- clients that are resident in geographical areas of higher risk or sanctioned countries
- a client has been identified to be a Politically Exposed Person (“PEP”) or family member or close associate of a PEP. See section on PEPs below.
- clients receive a high-risk score at the onboarding stage. See Player Risk Scoring Assessment. **Appendix I.**
- clients that receive high-risk scores based on multiple factors described in this procedure (adverse media, a large deposit, and so forth)
- the client has provided false or stolen identification documents or other information on establishing the relationship
- transaction(s) have no apparent economic or legal purpose
- companies that offer financial services or offer services to underlying clients or have underlying clients in any capacity, excluding liquidity providers.
- in combination with other factors, clients with deposit amount over lifetime throughout the entire relationship with the client

Unacceptable Clients

- Person or entities subject to financial sanctions or have been engaged in money laundering activities
- Luckyroo N.V is required to adhere to the sanction’s regime, which is designed to deny services and gambling products to individuals who are deemed to be a high Money Laundering or Terrorist Financing risk. As a result, Luckyroo N.V is prohibited to enter in any business relationship with individuals or entities listed as targets for financial sanction.
- Individuals under the age of 18 years old. Luckyroo N.V requires an individual to be at least 18 years old to open an account with the Firm. All individuals under 18 years of age will be automatically rejected.
- Individuals with unknown or unverified wealth sources
- Gameplay matching knows fraudulent patterns

5.2. Ongoing Monitoring

Luckyroo N.V is obliged to conduct ongoing monitoring of business relationships with their clients. Compliance Team conducts ongoing monitoring of clients in the following ways in accordance with the Company's risk-based approach:

Screening of clients against PEP, Sanctions, and Adverse Media on a regular basis. Any alerts considered to be true matches may trigger an Event-Driven Review.

i. Event-Driven Reviews

Certain events will trigger an Event-Driven Review which may, depending on the type of changes flagged, require a full customer due to diligence refresh.

Luckyroo N.V, through the course of its daily activities, obtains the information that brings a question to the accuracy of the customer due diligence information collected, or if suspicion arises, then the customer will undergo an immediate review, irrespective of their risk status.

ii. Periodic Reviews

Luckyroo N.V. has an obligation to ensure that customer due diligence information is relevant and kept up to date via regular client reviews. The extent to which clients' reviews are undertaken will be determined by using a risk-based approach and applied in accordance with the risk rating applied to the customer during the customer risk assessment. The Company has a customer review process based on the High, Medium, and Low risk factors assigned to its customers

The periodic reviews are conducted in line with the client's risk score and profiles are as follows.

High Risk – Every year. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

Medium Risk – Every two years. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse media
- Complete review of transaction profile, including new products requested

The information obtained during the review will be assessed to determine if the medium risk rating still applies.

Low Risk – Every three years. However, reviews will be undertaken when trigger events occur such as:

- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious
- This review will entail establishing the following:
 - Re-confirmation of Address
 - Screening for adverse media
- The information obtained during the renewal will be assessed to determine if the low-risk rating still applies.

The company's procedures are reassessed whenever the National Risk Assessment (NRA) is updated, ensuring that internal controls, risk ratings, and related measures remain aligned with current national risk priorities and regulatory expectations. Confirm procedures are reassessed whenever the NRA is updated.

6. Risk- Based Approach (ML/ TF risks' detection)

Company applies a risk-based approach in combating exploitation of its online platform for the purposes of ML and TF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/ TF Risk Assessments and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location.

Luckyroo N.V. conducts a formal Business Risk Assessment (BRA) annually and upon any significant operational change. This BRA evaluates money laundering and terrorism financing risks associated with clients, products, delivery channels, geographical exposure, and technological developments. The assessment is documented, approved by the Board of Directors, and revised in accordance with the latest regulatory updates or business model changes

Specifically, AML/CFT risk assessment categories center around the risks associated with:

Risk Factors

Client risk pertains to the likelihood of exposure to money laundering (ML) and terrorism financing (TF) through interactions with particular individuals. As part of its risk-based compliance model, Luckyroo N.V. conducts thorough evaluations of client profiles, financial transactions, and sources of wealth to identify potential vulnerabilities.

Certain client types are considered to carry a higher risk of financial crime involvement. This includes individuals with multiple income streams, which can complicate the verification process of fund legitimacy. Clients with fluctuating or unpredictable financial behavior may also increase the risk due to the challenge in assessing their financial patterns. Politically Exposed Persons (PEPs) are subject to intensified scrutiny owing to their potential influence over public funds and associated corruption risks.

Additional high-risk categories include individuals with substantial and inconsistent spending, whose expenditures appear disproportionate to their declared income, and clients who maintain multiple gaming accounts, potentially to evade monitoring or obscure financial activity. To address these risks, Luckyroo N.V. has implemented transaction thresholds that reflect normal client behavior patterns.

Typically, low-risk individuals are characterized by having a single, verifiable source of income. In contrast, those with multiple income sources, inconsistent spending patterns, or irregular transactions are subject to elevated monitoring and Enhanced Due Diligence (EDD) measures.

Product, Service, and Transaction Risks

Certain gaming services, financial instruments, and transaction types inherently present greater risks of being exploited for money laundering and terrorism financing. Criminal actors often target weak points within gaming ecosystems to manipulate outcomes or obscure the origins of illicit proceeds.

Illicit funds derived from activities such as fraud, narcotics trade, or theft may be funneled through gambling platforms to disguise their origin. The use of anonymous payment tools such as prepaid cards and digital assets like cryptocurrencies or tokens presents heightened risks due to limited traceability.

The misuse of player accounts for non-gaming purposes, such as acting as temporary repositories for financial transactions, also raises compliance concerns. Similarly, peer-to-peer transfers among players can facilitate unauthorized movement of funds.

Criminals may attempt to exploit third-party financial instruments, such as bank accounts or cards registered under different identities, or transfer funds across multiple gaming accounts, further complicating traceability. Financial services linked to gambling, such as currency exchanges, credit facilities, or use of multi-operator platforms, present an additional layer of risk.

To counter these threats, Luckyroo N.V. enforces stringent transaction monitoring protocols, applies EDD processes where appropriate, and maintains full compliance with global AML/CTF/CPF regulations.

Factors considered to evaluate Transaction Risk:

- Account monitoring (deposit, withdrawals and account activity)
- Transaction monitoring (activity and analysis screening results for deposits and withdrawals)
- Transaction monitoring to track specific patterns in client' activities and detect fraud

Factors considered to evaluate Product or Services Risk:

- Risk typologies associated with each product or service
- The level of transparency, or opaqueness, the product, service, or transaction affords

- The complexity of the product, service, or transaction
- The value or size of the product, service, or transaction

Geographical Risk

Geographical risk is determined by the location of a client and the origin of their financial resources, which may indicate elevated exposure to ML, TF, or Counter-Proliferation Financing (CPF) threats. Jurisdictions associated with weak AML/CFT controls, high corruption levels, or international sanctions pose heightened risk. Countries identified in relation to terrorism or weapons proliferation are subject to strict oversight.

To evaluate such risks, Luckyroo N.V. relies on reputable regulatory and international data sources, including but not limited to:

- Reports from the Financial Action Task Force (FATF), identifying high-risk countries under increased monitoring;
- Caribbean Financial Action Task Force (CFATF) public statements concerning regional financial crime issues;
- U.S. Department of State International Narcotics Control Strategy Reports (INCSR), highlighting financial crime trends;
- The European Commission's list of high-risk third countries with AML/CFT deficiencies;
- Office of Foreign Assets Control (OFAC) sanctions lists targeting terrorism-linked jurisdictions;
- Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on perceived levels of corruption.

Luckyroo N.V. applies a structured geographic risk classification methodology to differentiate between high-risk and low-risk countries. Enhanced Due Diligence is employed for users in higher-risk jurisdictions, and financial activity involving sanctioned territories is restricted. Risk classification protocols and monitoring systems are continuously updated to reflect changes in global assessments, ensuring ongoing compliance with AML/CTF/CPF regulations and maintaining a secure, transparent operating environment.

Distribution Channel Risks and Mitigation Measures

The methods by which Luckyroo N.V. engages with its clients also introduce potential exposure to money laundering, terrorist financing, and fraudulent activity. Channels that facilitate anonymity particularly those enabling financial transactions or user interactions without proper identification pose increased risk if not appropriately controlled.

To mitigate these vulnerabilities, the company enforces advanced verification measures for all client interactions involving anonymous features. Technological solutions, including biometric

authentication and sophisticated identity verification tools, are employed to reduce risks associated with fraud and unverified transactions.

By applying rigorous monitoring procedures and ensuring secure authentication across all distribution points, Luckyroo N.V. reinforces its commitment to international compliance standards and strengthens the security and transparency of its gaming platform against financial crime threats.

Factors considered to evaluate Delivery Channel Risk:

- Whether the Company with the client conducted on a non-face to face basis
- Whether the Company personally knows the customer and conducts business on face-to-face basis
- Client not known by the Company but well known in the industry and came to the Company by trusted sources

Technological Developments Risk Assessment

Prior to the launch of any new technology, digital product, delivery method, or operational process, Luckyroo N.V. conducts a formal and documented technological risk assessment. This process is mandatory and forms a core component of the Company's risk-based approach to AML/CTF/CPF compliance.

The risk assessment must be:

- Completed and reviewed prior to deployment, ensuring no new technology is introduced without first understanding its vulnerabilities and potential misuse.
- Fully documented in writing, including details of the product or system being assessed, identified risks, mitigation measures, residual risk levels, and decision-making rationale.
- Retained in internal compliance records and made available to the Curaçao Gaming Control Board (GCB) upon request.

Documented assessments are required for:

- New gaming platforms, digital tools, or payment channels.
- Any update to existing infrastructure that significantly changes risk exposure.
- The use or integration of AI systems, blockchain, or third-party services.
- Innovations involving anonymous payment mechanisms or remote account access.

This approach ensures all technological advancements are introduced responsibly, with due consideration for AML/CTF/CPF risks and are aligned with the supervisory expectations of the GCB.

Luckyroo N.V. is dedicated to ensuring that advancements in technology are not exploited for the purpose of financial crimes such as money laundering (ML) or terrorist financing (TF). As innovation continues to transform the iGaming sector, the company implements robust controls and a proactive risk management framework to identify and mitigate any vulnerabilities associated with technological change. Through the integration of thorough risk evaluation processes, Luckyroo N.V. safeguards its compliance obligations across all new business practices, service models, and product innovations.

Procedures for Risk Identification and Assessment

In order to detect and manage risks associated with technological innovation, Luckyroo N.V. conducts in-depth assessments in the following scenarios:

- The launch of a new product or feature on the gaming platform;
- The introduction of operational practices aimed at improving efficiency or enhancing user engagement;
- The adoption of novel service delivery mechanisms, including modern payment technologies or digital account access tools;
- The deployment or integration of emerging technologies into current or future gaming infrastructure, such as blockchain solutions, AI-powered services, or advanced cybersecurity protocols.

Prior to implementing any new technology, a comprehensive review is conducted to assess potential vulnerabilities that could be exploited for criminal activity. This process involves identifying and analyzing associated risks and ensuring all findings are thoroughly documented. The assessment is aligned with both domestic and international AML/CTF regulatory frameworks, reinforcing the company's ability to identify, manage, and mitigate technology-driven threats related to financial crime.

Implementation of Risk Mitigation Strategies

Upon identification of potential risks, Luckyroo N.V. promptly adopts appropriate mitigation measures to reinforce its defenses against emerging threats. These may include:

- **Strengthening of Security Protocols** – The implementation of multi-factor authentication (MFA), biometric identity verification, end-to-end data encryption, and artificial intelligence (AI)-based fraud detection tools to safeguard systems from misuse;
- **Enhancement of Transaction Monitoring Capabilities** – Upgrading monitoring platforms to detect atypical financial behavior using automated systems capable of flagging transaction patterns indicative of ML or TF;
- **Policy Adaptation** – Revising AML/CTF policies to address new risk factors introduced by evolving technology. The company ensures that its compliance framework remains agile, keeping pace with the dynamic nature of cybercrime and financial crime techniques.

Through ongoing monitoring and adjustment to technological developments, Luckyroo N.V. upholds its commitment to maintaining a secure and compliant operational environment. This forward-looking strategy protects the integrity of the company's financial ecosystem and affirms its alignment with global AML/CTF obligations. By doing so, the company ensures that innovation is not pursued at the expense of regulatory compliance or financial security.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Anti-Fraud key personnel to maintain effective internal controls and CDD measures as reflected in relevant policies.

Sector-Specific Risks in iGaming

Given the specific vulnerabilities within the online gambling industry Luckyroo N.V. has tailored its compliance controls to meet the challenges unique to the sector. Gambling platforms can be exploited to obscure the origin of funds, particularly through layered betting patterns, rapid fund turnover, and irregular payout behaviors. Criminals may use these tactics to convert illicit funds into seemingly legitimate winnings.

To counteract this, the company ensures that all deposits and withdrawals are routed exclusively through licensed financial institutions. Payments using anonymous or untraceable instruments, such as certain cryptocurrencies or unregistered prepaid cards, are restricted or entirely prohibited. Monitoring tools have been configured to detect unusual betting patterns, excessive deposit frequency, and sudden withdrawals that deviate from typical gaming behavior.

Employee training plays a vital role in strengthening the company's overall risk posture. Compliance staff and client-facing teams are routinely trained to recognize red flags, report suspicious activity, and stay informed of evolving criminal methodologies within the gambling landscape.

Mitigation Measures

When a risk is identified whether at the client, transaction, jurisdictional, or service level, Luckyroo N.V. responds with tailored mitigation strategies. EDD is applied to higher-risk profiles, requiring additional documentation and background checks. The company collects detailed information on the source and intended use of funds, while conducting ongoing screenings against global sanctions lists and watchlists.

Sophisticated transaction monitoring systems operate continuously in the background, equipped with real-time alerting capabilities. These systems analyze transaction flow and behavior to detect anomalies, flagging them for internal review. Alerts generated are triaged and, when necessary, escalated for formal investigation and reporting to the Financial Intelligence Unit (FIU).

To protect against identity fraud, strict verification processes are enforced. These include cross-referencing client data against sanctions databases, screening for duplicate accounts, and performing regular updates to maintain the accuracy of stored information.

Monitoring, Policy Adaptation and Reporting

Luckyroo N.V. understands that financial crime risks are dynamic, requiring constant vigilance. To ensure our controls remain effective, we conduct periodic internal reviews of transaction activity, client risk ratings, and compliance procedures. These findings inform policy updates and the adaptation of monitoring tools, ensuring alignment with both regulatory changes and emerging criminal tactics.

All suspicious transactions are promptly reported to the appropriate authorities in accordance with regulatory obligations. Record-keeping is maintained at a high standard covering client onboarding details, transaction data, risk classification documentation, and due diligence records for the required

legal retention period. These records are securely stored and made available for inspection during audits or regulatory reviews, reflecting the company's commitment to transparency and accountability.

Integrated Risk Governance

Through this holistic and risk-focused compliance strategy, Luckyroo N.V. demonstrates its commitment to preventing financial crime within the iGaming sector. By integrating compliance into every level of operations from onboarding to transaction oversight the company ensures that it not only complies with Curaçao's AML/CTF/CPF requirements but also contributes to the integrity and trustworthiness of the broader financial system.

Risk Assessment Documentation and Accessibility

Luckyroo N.V. maintains a comprehensive Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) in accordance with the requirements set out in the Curaçao Gaming Control Board AML/CTF/CPF Regulations. These assessments are structured, evidence-based, and tailored to the nature, size, and complexity of the company's operations and customer base. The BRA identifies and evaluates inherent risks associated with products, services, delivery channels, geographic exposures, and customer segments, while the CRA is used to determine individual customer risk ratings based on factors such as source of funds, transaction behavior, jurisdiction, and PEP status.

The BRA and CRA are developed using a risk-based methodology, updated regularly to reflect changes in risk exposure, and used to inform the implementation of proportionate control measures across the business. These documents are retained in written form and are made available to the Curaçao Gaming Control Board (GCB) or other competent authorities immediately upon request.

7. Client Due Diligence Guidelines (CDD, EDD) and Acceptance Policy (CAP)

When establishing a business relationship with clients it is imperative to identify whether a client wishing to use the Company's online platform poses any money-laundering, terrorist financing or proliferation financing threats to its ecosystem. CDD forms the basis of the risk-based assessment for risk scoring purposes based on the analysis of various types of suspicious activities including behavioral indicators, transactional indicators, client profile and product and services' indicators. In the context of AML, client due diligence process is a procedure which includes the identification of the potential client, verification of his/her identity and age, collection of additional information to construct an economic profile of the account holder, assign a risk rating, and monitor his/her behavioral and transactional patterns for any deviations that may be construed as a violation of AML/CFT legislation and policies. Research into the clients can be done via open- source tools such as social media checks, property ownership checks, employment checks, insolvency checks etc. Due Diligence measures may be simplified when the analysis of the initial client data places such applications in a low-risk category, whereas Enhanced Due Diligence (EDD) is applied to cases that require additional screening due to the system flagging certain data entries such as PEPs (politically-exposed persons), clients from high-risk jurisdictions etc .

Luckyroo N.V. created a risk scoring system by categorizing clients in accordance with set risk profiles which are construed from the physical location of the clients, their transactional behavior and the products they use. The integrity of the Luckyroo N.V. 's gaming environment is maintained through the application of protocols based on utilizing advanced technology and third-party databases including a proprietary anti-fraud system for onboarding and transaction monitoring, artificial intelligence tools

(AI), biometric identification in some instances and RegTech screening tools such as WorldCheck, LexisNexis, SEON etc.

The company is dedicated to maintaining compliance with regulatory standards that prohibit the establishment of anonymous or fictitious accounts within the casino sector. To effectively combat risks related to money laundering, terrorist financing, and proliferation, it is imperative to verify player identities and comprehend their business relationships. A comprehensive Client Due Diligence (CDD) policy is essential for evaluating risks and ensuring adherence to all regulatory obligations. Any activities deemed suspicious will be reported to the Financial Intelligence Unit (FIU) and, if necessary, to the Public Prosecutor's Office.

A Client Acceptance Policy (CAP) has been established to categorize players into low, medium, and high-risk profiles based on geographical location, transaction behavior, income source, and other factors. The CAP outlines enhanced due diligence measures and specifies scenarios where services will be denied due to elevated ML/TF risk. For more detailed information please refer to the **Appendix IV (Client Acceptance Policy)**.

7.1. The company applies CDD measures

Transactions of NAF 4,000 or more: CDD measures are applied to any single transaction that meets or exceeds this threshold.

Occasional transactions exceed NAF 4,000: This includes infrequent transactions that surpass the specified limit.

Suspicion of illicit activities: Any indication of money laundering or terrorist financing will trigger CDD protocols.

Uncertainties in client identification: If previously obtained identification data raises doubts, CDD measures will be activated.

Linked transactions: This applies to either a single transaction or multiple transactions that collectively exceed NAF 4,000. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD. High-risk transactions will require Enhanced Due Diligence (EDD).

The company's CDD procedures will encompass the following actions:

Identity Verification: Players will be identified using credible, independent documents or data. This process includes confirming the ultimate beneficial owner of legal entities and understanding their ownership structure.

Ongoing Monitoring: Continuous due diligence will be conducted to monitor transactions, ensuring alignment with the company's understanding of the player and their risk profile, including the source of funds as needed.

Confidential Reporting: Employees are instructed to maintain confidentiality regarding reports made to the FIU, thereby preventing players from being alerted. If suspicions of money laundering or terrorist financing arise, the company will bypass standard CDD processes and report directly to the FIU.

7.2. To establish a player's identity, the following information will be collected:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- For low-risk scenarios, only basic information will be required. In higher-risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.
- Risk Evaluation: Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- Verification Methods: Identity verification will be executed through:
 - Government-issued photo identification (e.g., passport or ID card).
 - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
 - Verification of the address through communication methods such as letters, email, or phone.
 - Biometric checks, cross-referencing database information, IP addresses, and funding methods.
 - If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher risk

clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium-risk players, basic employment or business information will suffice, supplemented by independent verification for higher-risk individuals.

7.3. Timing of Client Due Diligence Measures

Luckyroo N.V. enforces the timely implementation of Client Due Diligence (CDD) procedures to ensure full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These procedures are designed to proactively identify and verify clients in accordance with regulatory requirements and internal risk assessments.

CDD Triggered by Transaction Thresholds

At the point of account registration, Luckyroo N.V. collects and verifies core client information, including full legal name, permanent residential address, and date of birth. Additionally, clients undergo Politically Exposed Person (PEP) screening and are cross-checked against relevant sanctions lists to ensure they are not linked to prohibited or high-risk entities.

In line with the company's risk-based approach, full identity verification is completed prior to processing any financial transaction that reaches or exceeds the threshold of NAF 4,000. This requirement applies to both individual transactions and cumulative transactions such as multiple deposits, withdrawals, or player-to-player transfers that collectively meet the threshold within a relevant time frame.

Luckyroo N.V. actively monitors all financial activity on a continuous basis. Transaction data is aggregated daily to ensure that the cumulative behavior of each player is considered when assessing risk exposure and determining the need for additional due diligence.

When the threshold of NAF 4,000 is met, the company conducts a comprehensive client risk assessment. This includes reviewing all previously collected information, completing any outstanding CDD obligations, and updating the client's risk classification as needed.

Early Execution of CDD Procedures

As a proactive measure, Luckyroo N.V. aims to complete CDD procedures at the earliest opportunity preferably during account registration regardless of whether a financial threshold has been reached. By verifying client identities prior to their participation in financial transactions, the company reduces the likelihood of criminal actors exploiting the platform before thorough due diligence has been conducted.

Temporary Restrictions for Incomplete CDD

In circumstances where a client reaches the NAF 4,000 threshold before completing full CDD verification, Luckyroo N.V. applies specific transactional restrictions to preserve regulatory compliance:

If the threshold is met due to a deposit, the client is prevented from making further deposits or withdrawals. However, they may continue using existing funds for gameplay activities.

If the threshold is reached due to a withdrawal request, the client's account is temporarily frozen, and all gaming activity is suspended until the verification process has been finalized.

Addressing CDD Non-Compliance

If a client fails to submit the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, Luckyroo N.V. initiates corrective action. The business relationship is terminated, and depending on the circumstances, the company takes the following steps:

If the situation gives rise to a reasonable suspicion of ML or TF, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU).

In the absence of such suspicion, the remaining funds are returned to the original deposit source (e.g., the client's verified bank account or digital wallet).

If there are lingering concerns about possible financial crime, the company evaluates whether the funds should be frozen in accordance with its internal escalation procedures and regulatory requirements.

Preventing Tipping-Off

Luckyroo N.V. is mindful of the risks associated with tipping off a client during account restriction or closure. In such cases, the company ensures that all actions are carried out discreetly and in accordance with legal obligations. Staff are guided by internal procedures designed to avoid breaching anti-tipping-off provisions while maintaining full regulatory compliance.

By ensuring that CDD measures are implemented swiftly and in alignment with financial activity thresholds, Luckyroo N.V. strengthens its defenses against financial crime, upholds transparency, and safeguards the integrity of its gaming platform across all operational channels.

Continuous Surveillance of Existing Clients

Luckyroo N.V. applies Client Due Diligence (CDD) not only at the onboarding stage but also throughout the duration of the client relationship. The company is committed to maintaining a high standard of compliance by performing ongoing monitoring and routine reassessments, ensuring that all client activity remains consistent with prevailing Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations.

Ongoing Review and Risk-Based Monitoring

Client relationships are subject to continuous due diligence measures. This includes the regular monitoring of transactions and the reassessment of client risk profiles in light of new behaviors or patterns. Where necessary, the company re-evaluates previously collected data to ensure it remains accurate, complete, and relevant. Any deviation from expected conduct prompts further review and, where applicable, the application of enhanced scrutiny.

For clients who were previously onboarded with limited or incomplete CDD, Luckyroo N.V. initiates retrospective due diligence procedures. These are prioritized based on risk, with high-risk clients undergoing immediate verification. Periodic updates are also conducted in accordance with both internal policies and regulatory guidance to ensure that CDD measures remain aligned with risk exposure and evolving compliance standards.

Reapplication of CDD Based on Risk Triggers

Luckyroo N.V. applies full CDD measures to existing clients under specific conditions that indicate increased risk or regulatory necessity. These conditions include, but are not limited to:

A material change in the client's behavior or risk profile, such as sudden high-value transactions, relocation to a higher-risk jurisdiction, or being identified as a Politically Exposed Person (PEP).

Legislative or regulatory amendments that require updated or additional client verification.

The client engaging in one or more transactions totaling NAF 4,000 or more, which automatically triggers full identity verification and documentation review under the company's CDD policy.

Remediating Gaps in Historical CDD

In instances where clients were previously allowed to transact without complete CDD such as during legacy onboarding procedures or prior to the implementation of current regulatory standards Luckyroo N.V. takes corrective action. High-risk clients are prioritized for immediate verification, while others are subject to a scheduled review based on the level of risk they present.

CDD is applied using a proportional and risk-sensitive approach, ensuring that resources are allocated where they are most needed and that lower-risk clients are still monitored effectively. Verification processes may include updated identity checks, refreshed PEP and sanctions screenings, and a reassessment of the client's source of funds and wealth.

By extending due diligence practices beyond initial onboarding and embedding them into the ongoing management of client relationships, Luckyroo N.V. strengthens its regulatory compliance, reduces its exposure to financial crime, and upholds the integrity of its platform across all client segments.

Termination of Business Relationships

Luckyroo N.V. maintains the right to terminate business relationships with clients who fail to comply with Client Due Diligence (CDD) requirements or who present heightened financial crime risks. This measure ensures the company's adherence to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations while preserving the security and integrity of its operations.

Business relationships are subject to termination when a client engages in suspicious or unexplained financial activities, fails to submit required CDD documentation within the prescribed timeframe, or is determined to pose a significant risk of involvement in money laundering or terrorist financing. The decision to terminate a relationship is subject to formal internal review and must be approved by senior management.

Prior to termination, a final review of the client's account activity is conducted to identify any outstanding irregularities. If any transaction raises suspicion of ML, TF, or PF Luckyroo N.V. submits a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU) without delay. All records associated with the terminated relationship are retained securely for a minimum of five years in accordance with regulatory requirements. This approach reinforces the company's commitment to proactive risk management and ensures regulatory compliance through the entire client lifecycle.

Where risk cannot be adequately mitigated such as uncooperative clients, unresolved discrepancies, or confirmed links to sanctioned entities Luckyroo N.V. will terminate the business relationship and report such instances to the Financial Intelligence Unit (FIU)

Third-Party Reliance for Client Due Diligence

Luckyroo N.V. may, under controlled circumstances, rely on qualified third parties to carry out specific components of the Client Due Diligence (CDD) process. Such reliance is implemented strictly within the boundaries of applicable AML/CTF/CPF laws and does not absolve the company of its legal responsibility to ensure full compliance. Luckyroo N.V. remains ultimately accountable for the accuracy, completeness, and timeliness of all CDD-related activities performed on its behalf.

When relying on a third party, the company ensures that all relevant client identification and verification information is accessible without delay upon request. Third-party arrangements are governed by formal agreements that clearly outline data-sharing protocols, compliance obligations,

and procedures for independent compliance audits. These agreements require the third party to be a regulated entity subject to robust AML/CFT supervision and to maintain an independent relationship with the client.

Importantly, Luckyroo N.V. differentiates between third-party reliance and outsourcing. In a reliance scenario, the external party performs selected CDD tasks independently, while Luckyroo N.V. retains full responsibility for assessing client risk, verifying Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring. In an outsourcing arrangement, the third party operates under Luckyroo N.V.'s direct oversight, following its internal policies and regulatory framework.

Before engaging with any third-party service provider, Luckyroo N.V. conducts a comprehensive risk assessment of the provider's jurisdiction, evaluating its regulatory environment and compliance history. This is supported by intelligence from international

watchdogs and enforcement bodies. Regular assessments both quantitative and qualitative are performed to monitor the third party's performance and ensure the effectiveness of their procedures. These reviews verify that decisions regarding business relationships and risk classification remain under the exclusive control of Luckyroo N.V.

Through structured oversight and stringent regulatory controls, Luckyroo N.V. ensures that any third-party involvement in CDD processes contributes to a secure, transparent, and compliant operational environment.

7.4. Beneficial Ownership Identification and Control Structure Verification

Luckyroo N.V. undertakes all reasonable measures to identify, verify, and understand the Ultimate Beneficial Owners (UBOs) and the ownership and control structures of legal entity clients, in full compliance with AML Regulation III.2.2 and relevant international best practices.

This obligation extends beyond basic identification of beneficial owners and requires a full understanding of how ownership and control are exercised within the customer's structure, both at onboarding and throughout the course of the business relationship.

To meet this obligation, Luckyroo N.V. applies the following measures:

- Identify and verify natural persons who ultimately own or control 25% or more of the equity, voting rights, or capital of a legal entity, whether directly or indirectly.
- Where no individual meets the ownership threshold, identify any persons who otherwise exercise effective control, such as through:
 - Voting arrangements, contractual relationships, or positions of influence (e.g., board control or management power).
 - Indirect control mechanisms, such as trusts, nominee arrangements, bearer shares, or layered ownership through multiple legal entities.
- Conduct multi-tiered analysis in cases where ownership is obscured through multiple corporate layers or complex holding structures, to trace and identify the natural person(s) exercising ultimate control.

- Obtain and review reliable documentation such as:
 - Shareholder registries, articles of incorporation, beneficial ownership registers.
 - Declarations from legal representatives clarifying control and ownership hierarchy.
 - Organizational charts and financial disclosures when necessary.
- Where no individual qualifies under the above, identify the most senior managing official as a fallback UBO, in accordance with the “last resort” principle under FATF and CGA guidance.
- Verify beneficial ownership and control details using independent and reliable sources, and ensure this information is:
 - Accurately recorded and readily available for competent authorities.
 - Regularly reviewed and updated, particularly when:
 - There is a change in ownership or control.
 - The customer’s risk profile changes.
 - Trigger events occur (e.g., threshold transactions, suspicious activity).

Luckyroo N.V. does not enter or continue business relationships with legal entities whose beneficial ownership or control structures are non-transparent, unverifiable, or otherwise obstructive to due diligence.

8. Transaction Monitoring

Transaction monitoring in the betting and gambling industries is a critical component of regulatory compliance and anti-money laundering (AML) efforts. Given the high volume of transactions and the potential for misuse, these industries are closely monitored by regulatory bodies to prevent illicit activities such as money laundering, fraud, and financing of terrorism. Luckyroo N.V.’s objective is to mitigate challenges arising from the high volume and velocity of transactions where makes challenging to monitor each transaction effectively, and the use of cryptocurrencies and other digital payment methods that complicate the monitoring process.

In a nutshell, the Curacao regulatory landscape focuses on defining the indicators that may suggest the transaction is of an unusual nature so that it may be reported to the Curacao Financial Intelligence Unit (FIU Curacao). Therefore, an adequate transaction monitoring system is a vital part of complying with the licensing requirements in Curacao.

Luckyroo N.V.’s anti-fraud team is in charge of operating a proprietary anti-fraud system which analyzes players’ data on the basis of the automatic checks performed through a number of electronic systems such as WorldCheck and manual checks performed by a team of analysts via various data sources. Any discrepancies identified by the first line of defense are escalated to the team lead and then may be ultimately reported to the AML/CFT Officer in writing through an internal suspicious activity report (SAR).

This system is an automated monitoring system which allows to monitor transactions in real-time, flagging suspicious activities based on predefined rules and thresholds. The anti-fraud team uses machine learning and data analytics to enhance detection capabilities and reduce false positives. Additionally, the system is configured in a such a way as to focus on high-risk transactions, such as large deposits, frequent transfers, and cross-border transactions and the parameters reflect current and emerging threats to capture bad actors by flagging suspicious activity internally, and, where necessary, to financial intelligence units (FIUs).

8.1. Components of Luckyroo N.V.'s transaction monitoring system

Automated System: Advanced software solutions are employed to monitor transactions in real-time. These systems use algorithms and machine learning to identify patterns and anomalies that may indicate suspicious activities.

Risk Assessment: clients and transactions are assessed for risk based on various factors, including the amount and frequency of transactions, geographic location, and client behavior.

Alert Generation: When suspicious activity is detected, the system generates alerts that are reviewed by Compliance Officer. Alerts are based on predefined rules and thresholds, such as unusually large transactions or frequent deposits and withdrawals.

Common techniques include geolocation tracking, source of funds verification for high-value transactions, behavioral analysis by monitoring changes in betting patterns or gambling behavior that deviate from the norm for a specific client as well as transaction velocity (quick movement of funds between accounts and/or frequent high-value transactions within a short period).

CDD is triggered in the following scenarios: creation of an online account; doubts about the authenticity of the provided information and documents; suspicious client profile and/or transactional activity, unauthorized attempts to change the player's profile and a transaction or transactions that appear to be linked amount to 4000 NAF or more. When a transaction or a series of transactions that appear to be linked amounts to more than 4000 NAF (or equivalent in another currency), the CDD measures are applied automatically (the wagering of a stake, the deposit of funds or the collection of the winnings through the withdrawal of the funds constitute a transaction in such cases). Periodic reviews of the existing records and ongoing monitoring of the transactional patterns of the regular players also form an integral part of the CDD measures.

As part of combating money-laundering, fraud and terrorist financing, players' IP addresses are tracked via an embedded tool in the proprietary anti-fraud system in order to ensure the site is accessed from non-restricted countries. This measure also helps detect suspicious activity such as attempts to set up multiple accounts by the same individual, or block individuals who have been blacklisted or self-excluded. The proprietary software also monitors data as regards the players' transaction history, betting amount, information on wins and losses, players' geolocation, pattern of gambling activity and duration of playing. These tools may be used in instances where a client risk's rating is deemed to be high due to presence of some behavioral or transactional triggers that point to a potential AML/CFT breach.

In cases where the CDD measures cannot be applied, the account gets locked during an attempt to complete CDD and ultimately the business relationship with the client gets terminated due to the failure

to satisfy AML/ CFT legislative requirements and the funds are refunded back to the client through the same payment channel and account used to deposit the funds.

9. Politically- Exposed Persons (PEPs)

Enhanced Due Diligence (EDD) is a crucial process in the online betting and gambling industries aimed at preventing money laundering, fraud, and other illicit activities. EDD refers to the additional measures taken by companies to thoroughly verify the identity and background of their clients, particularly those posing higher risks. High-risk clients in the online gambling and betting setting are those who have high transaction volumes, deposit or withdraw large amounts, exhibit unusual betting patterns or are Politically Exposed Persons (PEPs). A PEP is an individual who recently held or is currently holding a prominent public position such as a head of state, member of the Parliament, government, directors of international organizations etc. Family members of PEPs and close associates are also considered PEPs, so their applications are also treated as high-risk by the Anti- Fraud team and relevant risk management procedures are activated when processing such requests through the senior management.

At Luckyroo N.V. PEPs' cases are handled by the senior management team whose approval is necessary to transact with such individuals. Furthermore, an internal register of such cases is kept by the Compliance Officer.

10. Sanctions Management, FATF High-Risk List, License Restrictions

Sanctions screening is the process of checking individuals, organizations, and transactions against various sanctions lists to prevent illegal activities and ensure compliance with international regulations. The purpose of sanctions screening is to comply with international, national, and regional sanctions regulations, prevent financial crimes such as money laundering and terrorism financing and to protect the reputation and integrity of the betting and gambling industry and Luckyroo N.V. in particular. Whereas EDD focuses on enhanced verification of high-risk clients, sanctions screening specifically checks against sanctions lists to identify prohibited entities.

As a Curacao-based entity with an EU-based payment agent Luckyroo N.V. complies with the key sanctions lists which are part of the international regulatory framework, including:

- United Nations Security Council (UNSC) Sanctions

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

- European Union (EU) Sanctions

https://www.eeas.europa.eu/eeas/european-union-sanctions_en

- United States (OFAC) Sanctions: Office of Foreign
- Assets Control. <https://sanctionssearch.ofac.treas.gov>
- UK Sanctions: HM Treasury Sanctions

<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>

- Other Jurisdictions: Local sanctions regulations.

If a match is identified on a sanctions list, Luckyroo N.V. will immediately freeze associated assets without prior notice and notify the FIU in accordance with the Process for Freezing of Resources as published by the National Gazette (2016). Sanctions screening tools are updated in real-time, and a review of Curaçao Gaming Control Board sanctions amendments is conducted at least monthly. All updates are reflected promptly in internal systems. Detailed Sanction Policy is described in **Appendix III**.

Update Mechanism and Frequency

Sanctions lists are updated at least daily and immediately upon publication of new updates by the competent authorities. Luckyroo N.V. uses automated sanctions-screening tools that synchronize with official sources in real time to ensure that the most current sanctions information is applied. In addition, the Compliance Officer conducts a minimum monthly review of any amendments or circulars published by the Curaçao Gaming Control Board or relevant government authorities to confirm alignment with local obligations.

Responsibilities

The Compliance Officer (or Sanctions Officer, where designated) is responsible for ensuring that sanctions lists are up to date, verifying tool synchronization, reviewing any alerts or potential matches, escalating confirmed matches, and ensuring adherence to regulatory requirements.

All sanctions-screening results, update logs, alerts, and match decisions are documented and retained for a minimum of five (5) years in accordance with applicable AML/CFT and sanctions regulations.

11. Suspicious Activity Reporting Guidelines

Reporting suspicious activities in the gambling and betting industries is a critical component of maintaining the integrity of these sectors and preventing them from being exploited for illegal purposes such as money laundering, fraud, and corruption. Suspicious activity is reported for legal compliance purposes as failure to report can result in significant fines and legal consequences for individuals and businesses. It also helps ensure client protection and helps safeguard clients from fraud and exploitation, ensuring a fair and safe environment for betting and gaming. Suspicious activity includes unusual transactions, structuring, unusual account activity and non-typical behavioral pattern, either too excessive or too disinterested in the betting outcomes, for instance. Unusual gambling patterns are investigated first to determine whether the exact nature of the transaction is just unusual or there are grounds to believe that it may be affiliated with the proceeds of a crime. According to article 1 of the Norut, it is an internet gambling entity's duty to report unusual transactions through the FIU Curacao's goAML portal which has been in use since January 1, 2021. Therefore, if the nominated officer determines that the internally reported suspicious activity should be disclosed to the regulatory authorities, he does so via the portal to comply with the Company's AML/CFT reporting protocol and obligations. In the meantime, the business relationship with the suspected client is to be paused or terminated, depending on the circumstances.

In cases where employees of the Company know, suspect or have reasonable grounds to believe that a person is attempting to finance terrorism or launder money, a relevant reporting protocol is activated,

and a suspicion report must be submitted to the nominated officer who then determines whether there are grounds for further regulatory action.

Suspicious activity may include using several anonymous payment methods

i.e. prepaid cards; location of the payment method does not correspond to the geolocation of the client; depositing a large sum and withdrawing it after no gaming or little gaming activity; a withdrawal request to a third-party payment method.

Suspicious activity may include using an intermediary for document-related requests; source of wealth does not match the reported financial data; frequent changes of ownership in a short time; lack of willingness to provide due diligence documentation.

Luckyroo N.V. keeps detailed records of all transactions and activities that seem suspicious, including dates, amounts, methods, and any other relevant details. As regards clients, the anti-fraud and AML teams document all available information about the individuals or entities involved, including names, addresses, account numbers, and identification.

11.1. Identifying Unusual Transactions

Luckyroo N.V. defines an unusual transaction as any financial activity that deviates materially from a client's established behavior or declared financial profile. These may include large or unexpected money movements, transactions involving unknown or unverified third parties, or financial activity lacking a clear legal or economic purpose.

The company relies on advanced transaction monitoring systems to detect such anomalies. When flagged, these transactions are forwarded to the Compliance Officer for deeper review. Staff members are trained to recognize behavioral and transactional red flags and to act promptly in escalating concerns.

The following categories of transactions are considered particularly noteworthy and may trigger further examination or reporting:

Previously Reported Activities: Transactions already identified and forwarded to judicial or law enforcement agencies such as the police or public prosecutor for potential links to ML or TF are automatically categorized as unusual.

Dealings with Sanctioned Persons or Entities: Any transaction involving a party listed under the Sanctions National Ordinance (N.G. 2014 no. 55), or other relevant sanction regimes, is flagged and treated as unusual.

High-Value Transactions: Transactions equal to or exceeding NAF 5,000 regardless of the method of payment are subject to scrutiny. This includes:

Deposits or withdrawals at or above the threshold.

Purchases of gaming tokens, digital credits, or chips meeting or exceeding the limit.

Redemptions or payouts of winnings at or above the specified amount.

The threshold also applies to a series of transactions that cumulatively total NAF 5,000 or more within a single gaming day. Such cumulative activity is evaluated in aggregate when determining whether reporting is necessary.

In cases where there is a reasonable basis to suspect that a transaction is connected to ML, TF, or PF whether due to the nature of the transaction, the behavior of the client, or other risk indicators it must be treated as suspicious and subject to internal escalation procedures.

Timely Reporting to the FIU

Once a transaction is determined to be unusual or suspicious, Luckyroo N.V. is obligated to file a report with the Financial Intelligence Unit (FIU) without delay, in accordance with AML Regulation IV.1. This requirement applies whether the transaction has been completed or merely attempted. The Compliance Officer is responsible for submitting the Unusual Transaction Report (UTR) immediately after the suspicion is confirmed, without waiting for additional approvals or administrative processes.

Confidentiality in Reporting

Maintaining strict confidentiality around Suspicious Activity Reports (SARs) is fundamental to preserving the effectiveness of the company's compliance regime and fulfilling its legal obligations. Employees are strictly prohibited from disclosing any details of a SAR to the person under review or to any unauthorized third party. Breaches of this confidentiality can undermine investigations, result in regulatory violations, and constitute a tipping-off offence under applicable legislation.

Only authorized personnel such as the Compliance Officer and designated members of the compliance team may handle SAR-related information. All such communications must be treated with the highest level of discretion. Luckyroo N.V. provides regular training to ensure staff understand the importance of maintaining confidentiality in all aspects of the reporting process.

Violations of this confidentiality policy are treated as serious compliance breaches and may lead to disciplinary action, including termination of employment. These protocols are critical to maintaining the integrity of the reporting framework and the company's ability to respond effectively to financial crime risks.

By fostering a culture of awareness, discretion, and accountability, Luckyroo N.V. strengthens its ability to identify suspicious behavior, uphold its obligations under AML/CTF/CPF regulations, and support broader efforts to prevent financial crimes across the iGaming sector.

12. Compliance Officer

Compliance Officer, or Money Laundering Reporting Officer is a designated individual who oversees compliance with AML regulations at Luckyroo N.V. It is a crucial role which encompasses being authorized to communicate with the relevant authorities in Curacao as well as supervise a team of AML compliance officers and their day-to-day operations, including maintaining robust age verification protocols, promoting responsible gambling practices, preventing gambling-related addiction, promoting self-exclusion tools.

The Compliance Officer of Luckyroo N.V. operates with full independence and is granted the necessary authority to perform all duties related to the Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. The Compliance Officer has unrestricted and direct access to all relevant customer information, transaction

data, internal systems, and personnel, as required to fulfill their compliance obligations effectively. To preserve independence and avoid conflicts of interest, the Compliance Officer reports directly to the Board of Directors and is not involved in any operational or commercial functions of the company that could compromise objectivity. The Board ensures the Compliance Officer is adequately resourced, empowered, and supported in executing the AML/CTF/CPF program in accordance with Regulation V.3 of the CGA AML Guidelines. This structure safeguards the autonomy of the compliance function and ensures timely escalation of significant risks or breaches to the highest level of governance.

The Compliance Officer is also responsible for disclosing suspicious activity, including suspicious transactions, to the FIU in Curacao. Internally, the AML/CFT Officer is requested to prepare quarterly AML reports for the Board of Directors to keep the Board members informed of any recommended changes that may be required to manage the AML/CFT compliance program.

The Compliance Officer is tasked with several critical functions to ensure the effectiveness of our AML program. These primary duties include:

- **Policy Implementation:** Overseeing the execution of AML policies and procedures to ensure alignment with current regulations.
- **Central Point of Contact:** Serving as the main contact for all AML-related issues.
- **Policy Review:** Regularly reviewing and updating AML policies to address evolving regulatory standards and emerging risks.
- **Training Oversight:** Managing the AML training program to ensure employees are adequately informed about AML requirements and their roles in maintaining compliance.
- The Compliance Officer is entrusted with several essential responsibilities:
- **Transaction Monitoring and Reporting:** Continuously analysing transactions and client activities to identify suspicious behaviour. They are responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) when necessary and maintaining accurate records of these reports.
- **Policy Development and Updates:** Crafting and revising AML policies and procedures to adhere to the latest Curaçao gaming regulations and international best practices. This includes adapting the AML framework to address new risks and regulatory changes.
- **Employee Training and Awareness:** Ensuring that all staff receive comprehensive AML training and understand their responsibilities in detecting and reporting suspicious activities. The Compliance Officer must regularly update training materials to reflect legislative or policy changes.
- **Regulatory Liaison:** Acting as the primary contact with regulatory bodies, law enforcement, and other relevant authorities on AML matters. This includes responding to information requests and participating in regulatory inspections or audits.
- **Compliance Audits:** Conducting regular reviews and audits of the AML program to evaluate its effectiveness and compliance with legal requirements. The Compliance Officer is responsible for addressing any identified issues and implementing necessary corrective measures.

- **Record-Keeping:** Maintaining detailed records of all AML-related activities, including SARs, internal reports, training sessions, and policy updates. These records must comply with legal requirements and be readily available for regulatory review.
- Through the execution of these functions and responsibilities, the Compliance Officer plays a vital role in safeguarding the organization against money laundering and terrorist financing risks, ensuring rigorous compliance with Curaçao's AML regulations.

13. Senior Management Responsibility

The Company's senior management is fully engaged in the process of assessment of inherent risk categories. It is required by the Board of Directors that a nominated AML/CFT Officer regularly updates the Members on any significant deviations related to the control environment and produces an annual report covering the operator's systems and controls that mitigate the risks of money-laundering, terrorist financing and proliferation financing. Periodic reviews of the relevant policies and procedures take place quarterly based on monthly risk assessments' results and the AML/CFT Officer may request the approval of the Board of Directors for any changes in Luckyroo N.V.'s AML/CFT policy in order to remedy any identified weaknesses in the internal controls and risk management practices, should they arise.

Policy Review and Risk Assessment

Senior management is accountable for conducting comprehensive reviews of all relevant policies and procedures at least once each year. These reviews are guided by monthly risk assessments, enabling the identification and timely addressing of any potential vulnerabilities in internal controls and risk management practices. If any deficiencies are identified, the AML/CTF/CPF Officer can recommend necessary adjustments to the Board for approval, thus enhancing the company's risk management and compliance framework.

Employee Training Programs

In alignment with global best practices, senior management is responsible for overseeing the creation and execution of extensive employee training programs. These initiatives are designed to increase awareness and understanding of AML/CTF/CPF risks among all employees, especially those in critical roles, ensuring they are equipped to effectively recognize and respond to suspicious activities.

Internal Control Framework

Senior management also ensures that the company maintains a robust internal control framework. This includes establishing adequate segregation of duties, implementing clear authorization processes, conducting ongoing monitoring, and ensuring thorough documentation. To uphold regulatory compliance and enhance the effectiveness of the AML/CTF/CPF program, regular independent audits and assessments are performed to provide objective evaluations and identify areas for improvement.

14. Employee Training and Screening Program

Employees in the betting and gambling industries are on the front lines of AML compliance. Luckyroo N.V. conducts its operations with a high standard of ethics, ensuring full compliance with laws and

regulations governing financial transactions. The company has implemented policies and procedures for screening employees for criminal records, as part of its ongoing commitment to integrity.

To ensure the integrity and competence of personnel engaged in activities relevant to anti-money laundering (AML) and counter-terrorist financing (CTF) obligations, the Company maintains a structured Employee Screening Program in accordance with CGA AML Regulation V.4. Please see Appendix II.

Luckyroo N.V.'s employees play a crucial role in Anti-Money Laundering (AML) compliance within the betting and gambling industries. Their actions and vigilance are essential in preventing these sectors from being exploited for money laundering and other illicit activities. They are made aware of the fact that failing to report potential breaches of AML Policies may lead to administrative and criminal charges.

The Company's employees, especially those in client-facing roles or positions that involve handling financial transactions, must have a thorough understanding of the company's AML policies and procedures. This includes knowing the types of transactions that should be considered suspicious, the process for reporting such transactions, and the importance of maintaining client confidentiality.

A key part of an employee's role in AML compliance is to be vigilant and identify any activities that seem unusual or do not fit with the normal behaviour of a client. This could include large and inconsistent bets, frequent changes in betting patterns, or transactions that seem to have no apparent purpose other than to move money through the system.

Once an employee identifies a potentially suspicious transaction, they must report it through the appropriate channels to the Compliance Officer. The reporting protocol involves filling out a Suspicious Activity Report (SAR) and using the company's internal reporting system. Employees are trained on how to report suspicions and the importance of doing so promptly on an annual basis or more frequently in line with the needs of a particular department.

Employees involved in client onboarding or account management are responsible for conducting due diligence checks on clients. This includes verifying their identity, understanding the source of their funds, and ensuring that they are not listed on any sanctions or watch lists. Employees are trained on how to conduct such checks diligently and escalate any concerns where necessary.

Employees involved in AML compliance at Luckyroo N.V. understand the importance of maintaining the confidentiality of their reports and any information related to suspicious activities. They are made aware of data protection laws and ensure that client information is handled in compliance with these regulations.

Luckyroo N.V. upholds the highest standards of integrity and professionalism among its personnel, recognizing employees as critical to the company's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework. In line with Regulation V.4 of the CGA AML Guidelines, the company maintains a formal Employee Screening Program, applied both prior to employment and on an ongoing basis thereafter.

1. Pre-Employment Screening

Before onboarding any new employee, especially those in sensitive, client-facing, or compliance-related roles, the company conducts thorough background checks, including:

- Verification of identity and right to work using government-issued documentation.

- Criminal background checks to detect any prior financial or integrity-related offenses.
- Employment and reference verification to confirm qualifications and experience.
- Sanctions and PEP screening, using independent screening tools and global watchlists.

Candidates failing to meet the company's integrity or risk criteria are not employed.

2. Ongoing Employee Screening

Luckyroo N.V. continues to assess employee suitability after hiring through:

- Annual rescreening of employees in AML/CTF-sensitive roles.
- Event-driven screening, such as when suspicious activity, misconduct, or role changes occur.
- Monitoring for changes in sanctions exposure, PEP status, or relevant legal/regulatory risks.

All employee screening records are retained securely and confidentially, in compliance with data protection laws, for a minimum of five (5) years.

3. Training and Awareness

Employees, particularly those involved in onboarding, account management, or transaction processing, receive annual AML/CTF training tailored to their roles. This training ensures staff understand:

- The company's AML/CTF/CPF obligations.
- How to identify unusual behavior, such as:
 - Large or inconsistent bets.
 - Suspicious patterns of deposits/withdrawals.
 - Anonymous or third-party payments.
- How and when to file a Suspicious Activity Report (SAR).
- The importance of confidentiality and client data protection.

Employees are made aware that failure to comply with AML/CTF obligations may lead to disciplinary, administrative, or criminal consequences.

15. Record- Keeping

Luckyroo N.V. is subject to The Company complies with all the relevant legislation as regards having an audit trail in cases where it is asked to assist in the investigations by law enforcement agencies. Generated records are retained in electronic form for a period of 5 years in accordance with the data protection regulations from the date of the establishment of a business, commercial or a professional relationship with an employee, a client or a business partner.

To adhere to stringent record-keeping standards, our company implements robust procedures for managing documentation associated with AML/CTF/CPF. We maintain comprehensive records, which include client identification information, transaction details, suspicious activity reports (SARs), training logs, and audit records, all preserved for a minimum of five years.

- The company securely maintains detailed records, including:
- Client identification information.
- Transaction histories.
- Suspicious activity reports (SARs).
- Staff training logs.
- Audit records.

We ensure the security of these records through advanced encryption techniques and strict access controls to prevent unauthorized access. Regular audits are conducted to verify the integrity of the data and safeguard against potential breaches.

A systematic approach is adopted for organizing records, allowing for efficient retrieval by authorized personnel and regulatory bodies. We conduct continuous internal monitoring and periodic audits to ensure compliance with established protocols.

By effectively managing our records, the company not only meets regulatory requirements but also facilitates auditing processes and contributes to the overall integrity of the gaming industry.

16. AML Compliance Audit

Luckyroo N.V. recognizes internal auditing as a critical function for ensuring the integrity, effectiveness, and ongoing alignment of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework with applicable laws, regulations, and CGA guidelines. Internal audits are not merely procedural but serve as an essential governance tool, executed with independence and rigor, and culminating in formal reporting to senior management and the Board of Directors.

To this end, the Company conducts periodic AML compliance audits, at least annually and additionally in the event of significant regulatory changes, operational developments, or material compliance breaches. These audits are carried out by qualified internal or external parties who are independent from daily compliance operations and who possess the requisite expertise in financial crime risk management.

The audit scope includes, but is not limited to:

- **Evaluation of Policies and Procedures** – Reviewing whether the AML/CTF/CPF framework is up to date, aligned with legal standards, and effectively applied across departments.
- **Effectiveness of Risk-Based Approach** – Testing the design and implementation of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and other relevant methodologies.

- **Transaction Monitoring and SAR/STR Filing** – Assessing the adequacy of transaction surveillance tools and the timeliness, quality, and completeness of suspicious activity reporting.
- **CDD and KYC/KYB Compliance** – Sampling client files to verify that due diligence procedures, beneficial ownership checks, and document retention policies are implemented correctly.
- **Sanctions Screening Controls** – Verifying the application and currency of screening mechanisms against relevant international and domestic sanctions lists.
- **Employee Screening and Training** – Assessing adherence to employee screening requirements and the effectiveness of ongoing AML training programs.
- **Technology Risk Controls** – Reviewing systems supporting AML compliance, including data integrity, automated risk scoring, and access rights.

The outcomes of the internal audits are formally documented in comprehensive reports, which are submitted directly to senior management and the Board of Directors, in accordance with CGA AML Regulation Section V.7. These reports identify any deficiencies or areas for improvement and include clear recommendations and timelines for remediation.

Furthermore, audit findings that reveal material weaknesses, breaches, or risks to AML/CTF/CPF compliance are escalated immediately to the Compliance Officer and the Board, with follow-up audits conducted to verify implementation of corrective actions.

Luckyroo N.V. maintains an audit trail and full documentation of all internal audit activities for a minimum of five (5) years and makes such records immediately available to the Curaçao Gaming Control Board (GCB) upon request. The Company is committed to transparency, accountability, and continuous improvement in its AML/CTF/CPF compliance framework.

17. Regulatory Access and Cooperation

Luckyroo N.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Control Board (GCB) and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data
- Internal risk assessments
- Policies and procedures

- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance-related systems and platforms

Access shall be granted for both on-site and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Luckyroo N.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post-inspection findings, including corrective action plans and remedial steps as directed by the GCB.

18. Internal Audit and Reporting

Luckyroo N.V. shall establish and maintain an independent internal audit function for the purpose of evaluating the effectiveness, adequacy, and operational integrity of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework. Internal AML audits shall be conducted at least annually, or at such greater frequency as may be necessitated by the Company's risk exposure, regulatory developments, or material changes to business operations. Audits shall be performed by the Internal Audit team, or by an independent third-party auditor where required to ensure full independence, objectivity, and professional competence.

The scope of each internal audit shall include, but shall not be limited to: the review and testing of AML/CTF/CPF policies and procedures; assessment of the effectiveness of transaction monitoring systems and sanctions-screening controls; verification of the adequacy and accuracy of Suspicious Activity Report (SAR) filings; evaluation of customer due diligence and enhanced due diligence practices; examination of training programs and training effectiveness; and testing of governance, oversight, and record-keeping arrangements. The audit shall also assess whether the Company's systems and controls remain proportionate to its risk profile and compliant with statutory and regulatory obligations.

Upon completion of each audit, a formal Internal Audit Report shall be issued, setting out the audit methodology, findings, deficiencies identified, and recommended remedial actions. Such reports shall be submitted without delay to Senior Management and the Board of Directors, or any duly authorized committee with oversight responsibilities. Senior Management shall ensure that all identified deficiencies are addressed and rectified within defined and documented timeframes, and that implementation of corrective actions is monitored to completion.

All internal audit reports, supporting documentation, working papers, and remedial action logs shall be maintained in a secure and tamper-proof manner and retained for a minimum period of five (5) years, or longer where required by law or regulation. The internal audit function shall have unrestricted, unimpeded access to all systems, personnel, records, and information necessary to discharge its duties effectively and in full compliance with applicable regulatory expectations.

19. Appendixes

Appendix I

Player Risk Scoring Assessment

HOW TO USE THIS?
1. Only yellow and blue fields have to be filled.
2. Comment section is available, however, it is not necessary for calculation of risk level.
3. Majority of questions has dropdown list or checkbox. Correct answer(s) should be selected

NEW total score:	0.00
NEW risk level:	Low
Onboarding specialist:	
Last update date:	

Category	Score
low	0-1.4
medium	1.4-2.5
high	2.5 or more
unacceptable	At least 1 unacceptable

Client no.:	
Name:	

Risk Category	Question	Risk score	Risk level	Additional comments
Client	Customer's Age			
Geography	Customer's Citizenship			
Geography	Customer's Second Citizenship			
Geography	Customer's Country of Birth			
Geography	Customer's Country of Residence			
	Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?			
Client				
ACCOUNT PROFILE				
Client	Purpose of account registration?			
Client				
Client				
FUND SOURCE AND INCOME STATUS				
Client	Source of funds	average		
Client				
Client				
Client				
Client				
Client	Source of wealth	average		
Client				
Client				
Client				
Client				
INTENDED ACCOUNT ACTIVITY (DEPOSITS)				
Transactions	Average frequency of transactions	average		
Transactions	Expected total value of transactions per period (NAP)			
Transactions	Types of incoming payments			
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
INTENDED ACCOUNT ACTIVITY (OUTGOING PAYMENTS)				
Transactions	Average frequency of transactions	average		
Transactions	Expected total value of transactions per period (NAP)			
Transactions	Types of outgoing payments			
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
Transactions	Reasons for outgoing payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
GAMING BEHAVIOUR				
Products and Services	Please indicate services of interest	average		
Products and Services				
Products and Services				
Products and Services				
Products and Services				
Products and Services				

Risk Category:	To be:	Sum:	Weight:
Client	20%	0	
Geography	20%	0	
Products and Services	20%	0	
Transactions	20%	0	
Channels	15%	0	
Other	5%	0	
		0	

CONFIRMATIONS			
Channels Payment Channels Third-party involvement Access Onboarding	Adverse media level Client	average	
Manual risk level adjustment based on the expert judgement (±0.5): Other			Comment regarding manual risk adjustment: Summary of the applicant:

Appendix II

Employee Screening Program

This Employee Screening Program (“Program”) establishes the mandatory standards and procedures governing the vetting, assessment, and ongoing monitoring of all personnel employed or engaged by Luckyroo N.V.

This Policy is adopted to ensure full compliance with CGA AML Regulation V.4, which requires firms to implement adequate screening procedures for employees both prior to employment and on an ongoing basis.

The Company further adopts an Employee Screening Checklist, which forms an integral part of this Policy and must be completed in all cases as evidence of adherence to the screening requirements set out herein.

This Policy applies to:

- All full-time, part-time, temporary, and contract employees.
- Senior Management, the Compliance Officer and all staff involved in AML/CTF obligations.
- Individuals engaged through third-party or outsourced arrangements performing regulated or sensitive functions.

No individual may commence employment or assume duties in a sensitive role until all screening measures required under this Policy have been satisfactorily completed.

Requirements

Luckyroo N.V. shall ensure that all individuals are fit, proper, and suitable to perform their assigned duties. Screening procedures must be risk-based, proportionate to the sensitivity of the role, and documented.

The screening process consists of:

- (a) Pre-Employment Screening,
- (b) Fit-and-Proper Assessment (for designated roles),
- (c) Ongoing Screening, and
- (d) Completion of the Employee Screening Checklist.

Pre-Employment Screening

Human Resources (“HR”), in coordination with the Compliance Department, shall conduct the following mandatory pre-employment checks:

- Criminal Background Checks

A criminal record check shall be obtained to determine whether the applicant has been convicted of offenses relating to dishonesty, fraud, financial crime, money laundering, terrorist financing, or other conduct incompatible with the integrity expected of Company personnel.

- Verification of Identity

Applicants must present valid government-issued identification. HR shall verify identity authenticity and consistency.

- Verification of Academic and Professional Qualifications

All educational degrees, professional certifications, licenses, and other credentials relevant to the position must be independently verified.

- Employment History Verification

The Company shall confirm prior employment, roles, responsibilities, performance, and conduct, subject to applicable legal limitations.

- Reference Checks

At least two professional references must be obtained and documented. Adverse information must be escalated to Compliance for assessment.

Completion of the Employee Screening Checklist is mandatory before any offer of employment may be finalized.

Fit-and-Proper Assessment

A formal Fit-and-Proper Assessment shall be conducted to determine the individual’s suitability for the role, evaluating the following:

- Integrity and Reputation

Absence of adverse regulatory findings, criminal convictions, ethical misconduct, or behaviour inconsistent with professional honesty.

- Competence and Professional Capability

Assessment of qualifications, technical skills, AML/CTF experience, and the capacity to discharge regulatory obligations.

- Financial Soundness

Where permitted by applicable law, consideration of financial history including bankruptcy, insolvency, or financial misconduct.

- Independence and Conflict of Interest

Assessment of the ability to act independently and without real or perceived conflicts of interest.

A Fit-and-Proper Assessment Form shall be completed, reviewed by the Compliance Department, and retained with the Employee Screening Checklist.

Ongoing Screening and Monitoring

Periodic Screening

Employees in sensitive, compliance-related, or high-risk roles shall undergo screening at least annually, including but not limited to:

- Updated criminal record checks (where legally permissible),
- Role suitability evaluations,
- Conduct and performance reviews,
- Confirmation of continued independence and absence of conflicts.

Trigger-Based Rescreening

Additional screening is required when:

- An employee is promoted or transferred to a sensitive role,
- Allegations or indicators of misconduct are identified,
- Regulatory or business changes increase the risk profile of the role,
- External information gives rise to concerns regarding fitness or propriety.

Continuous Conduct Monitoring

Supervisors and the Compliance Department must report any concerns regarding employee behavior or integrity for immediate assessment.

Mandatory Checklist Completion

For each periodic or trigger-based rescreening, the Employee Screening Checklist must be updated and retained.

Documentation and Record-Keeping

The Company shall maintain complete and accurate records of all screening activities, including:

- Background check reports,
- Verification evidence,
- Fit-and-Proper Assessments,
- Completed Employee Screening Checklists,
- Internal approvals and escalation notes,
- Any adverse findings and remedial actions taken.

Records shall be retained for not less than five (5) years, or longer where required by law or regulation, and shall be made available to competent authorities upon request.

Responsibilities

Human Resources

- Administers pre-employment screening and maintains screening files.
- Ensures completion of the Employee Screening Checklist.
- Escalates concerns to Compliance.

Compliance Officer

- Oversees screening for AML/CTF-related roles.
- Conducts Fit-and-Proper Assessments.
- Approves employment in sensitive roles.
- Ensures compliance with CGA Regulation V.4.

Senior Management

- Ensures adequate resources and oversight.
- Approves any exceptions or escalated cases.
- Reviews periodic compliance reports.
-

Compliance and Enforcement

Failure to comply with this Policy, including failure to complete the Employee Screening Checklist or Fit-and-Proper Assessment, may result in disciplinary action up to and including termination of employment.

The Company affirms that this Policy satisfies the requirements of CGA AML Regulation V.4 and shall review the Policy annually to ensure continued regulatory compliance.

New Employee check list

Employee: _____

Starting date: _____

1.	Copy of national Identity card or passport	☐
2.	Work permit (if needed)	☐
3.	Proof of Residence	☐
4.	Certificate of clear criminal record	☐
5.	Non-Bankruptcy letter	☐
6.	Reference letter from previous employer	☐
7.	License/certificates	☐
8.	CV (Curriculum Vitae)	☐
9.	Good repute questionnaire	☐
10.	Diploma of high education	☐
11.	AML and IOM acknowledgement letter	☐
12.	Privacy Notice	☐
13.	Induction & Initial Training Policy/Acknowledgement form	☐
14.	Employment Agreement	☐

Appendix III

Sanctions policy

Background

Luckyroo N.V. is obliged to comply with laws imposing financial and other restrictions on dealings with certain entities, individuals and countries. This Sanctions Policy (hereinafter the “Policy”) sets out requirements and procedures designed to promote compliance with such laws (sanctions). Sanctions are a policy tool that national governments and multinational organisations use to constrain and deter perceived threats to their security, or to conform international conduct to recognised international standards. Sanctions arise in response to the conduct of countries, geopolitical rivals or transnational actors or trends. While national-level and multilateral sanctions regimes vary in content,

rules, and restrictions, and the substance and frequency of enforcement action, they tend to fall into one of the below categories:

- **Comprehensive sanctions.** These sanctions target entire countries or geographic regions (e.g., the Crimea Region of the Ukraine) and prohibit most activity involving those countries or jurisdictions. Comprehensive sanctions aim to alter government behavior by imposing economy-wide costs, restricting access to arms and tools of internal repression, and restricting access to a wide range of goods and services.
- **Regime-based sanctions.** These sanctions target current (or former) governments or regimes. They are not comprehensive: although they are associated with particular countries, they are primarily list-based, focused on officials involved in activity deemed to be a threat to national security, economy, or foreign policy and on their associates. These sanctions tend to be paired with limited export controls or embargoes and related financing prohibitions. Most regime-based sanctions aim to protect human rights, combat state-sponsored or grand-scale corruption, and support democratic processes, institutions, and the rule of law.
- **Sectoral sanctions.** These sanctions target entities in a key sector or sectors of a country's economy. Importantly, they may still allow for many ordinary business transactions with the country at issue, even with respect to the listed entities. The listed entities may not be themselves involved in targeted activity, but they may be identified due to their relationship to government decision-makers (to exert pressure on those decision-makers) or because of their importance to a country's economy or future growth prospects.
- **Special debt and/or equity sanctions.** These relatively complex prohibitions allow for the continuation of day-to-day business with targeted entities while restricting the ability of targets to deal in new or new equity (valuable for, e.g., raising capital for long-term projects). These sanctions have generally been applied to entities within specific economic sectors (e.g., energy) but have also been applied to entities owned or controlled by a target government.
- **Conduct-based sanctions.** These list-based sanctions, as described in an additional resource, are directed not at particular countries or governments but rather at anyone involved in defined types of malicious activity. Persons and entities can be designated for involvement in terrorism, proliferation of weapons of mass destruction, bribery/corruption, human rights violations, drug trafficking, organized crime, election interference, and cyber-enabled malicious activity. Conduct-based sanctions are meant to identify, disrupt, and deter sanctioned activities.

The key types of sanctions listed above may vary on the above characteristics even within a single category. Nor are these key types of sanctions mutually exclusive (e.g., regime-based sanctions may overlap with special debt and/or equity sanctions).

Sanctions Regimes

Due to the nature of the business of the Company, different regulatory regimes may have jurisdiction over its transactions, Clients, products and services. This section outlines the major sanctions regimes and the basis of their jurisdiction directly impacting the Company's operations.

The United Nations (UN)

Under Chapter VII of the UN Charter, The United Nations Security Council (UNSC) can take action to maintain or restore international peace and security. The UN sanctions are administered by sanctions committees associated with the Security Council and are complemented by Financial Action Task Force (FATF) Recommendations 6 and 7. UNSC resolutions are legally binding to the UN member states.

The Company complies with sanctions restrictions imposed by the UN across all its operations.

The European Union (EU)

Sanctions are one of the EU's tools to promote the objectives of the Common Foreign and Security Policy (CFSP): peace, democracy and the respect for the rule of law, human rights and international law. The EU implements all sanctions imposed by the UN. In addition, the EU may reinforce UN sanctions by applying stricter and additional measures. Where the EU deems it necessary, it may decide to impose autonomous sanctions.

EU restrictive measures only apply within the jurisdiction of the EU, that is: a) within EU territory, including its airspace; b) to EU nationals, whether or not they are in the EU; c) to companies and organisations incorporated under the law of a member state, whether or not they are in the EU. This also includes branches of EU companies in third countries; d) to any business done in whole or in part within the European Union; e) on board of aircrafts or vessels under the jurisdiction of a member state.

The Company complies with sanctions restrictions imposed by the EU across all its operations.

The United Kingdom (UK)

The UK financial sanctions apply, inter alia: a) within the territory and territorial waters of the UK and to all UK persons, wherever they are in the world, b) to all individuals and legal entities who are within or undertake activities within the UK's territory, c) to all UK nationals and UK legal entities established under UK law, including their non-UK branches; they must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

The Company complies with sanctions restrictions imposed by the United Kingdom to the extent that such sanctions do not contradict the laws of the European Union.

The United States (US)

In terms of applicability, the US sanctions fall into two categories:

- **primary US sanctions;** applicable to US persons, including all US citizens and permanent resident aliens regardless of where they are located, all persons and entities within the US, all US- incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.
- **secondary US sanctions:** when applied, potentially subject non-U.S. persons to sanctions even if they are conducting business entirely outside of the United States and there is no US nexus in a relationship or a transaction. A number of sanctions programmes administered by the Office of Foreign Assets Control (OFAC) of the Department of the Treasury include secondary sanctions, including but not limited to Russia, Iran, Hong Kong/China sanctions programmes.

To the extent that is permissible under the local laws and the EU laws and regulations, the Company complies with both primary and secondary sanctions restrictions imposed by the US. Where compliance with secondary US sanctions is not permissible, e.g., regulation (EC) No 2271/96 and Joint Action 96/668/CFSP of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, pp. 1 and 7), the Compliance Officer must escalate the matter to the Director(s) and the Board of Directors as a whole.

Policy Statement

Under this Sanctions Policy, the Company must:

- Where required by law, block accounts and other assets of sanctioned entities and individuals.
- In all other instances, prohibit or reject unlicensed trade and financial transactions with sanctioned jurisdictions, entities, and individuals.
- Exit relationships with Clients confirmed to be subject to sanctions, regardless of whether this is required by local law in the jurisdiction where the account or relationship is based. In the event that an exit is not permissible under local law, this should be escalated to the Director(s) and the Board of Directors as a whole.
- The Company must not knowingly engage in any transactions and/or business relationships structured to or aimed at the circumvention of applicable sanctions restrictions.

Failure to comply with this Policy may expose the Company to regulatory action or fines, civil or criminal liability as well as possible reputational damage.

Staff responsible for breaches of sanctions related laws and regulations may also be exposed to

criminal liability or fines. Staff who fail to comply with this Policy may be subject to disciplinary action, including dismissal.

Roles and Responsibilities

The Board of Directors

The responsibilities of the Board of Directors with regard to the Company's Sanctions Policy shall include:

- Reviewing and approving this Policy as required.
- Ensures effective communication of the importance of sanctions compliance throughout the organisation.
- Provides oversight to ensure the AML/CTF and sanctions compliance function receives adequate support and resources at every organisational level and has sufficient authority and independence to effectively exercise its responsibilities.
- The Board receives and considers regular compliance reports presented by the Compliance Officer, covering both AML/CTF and sanctions compliance.
- Appointing a qualified Compliance Officer with overall responsibility for the proper application the sanctions policy and provides this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board and the business lines.

The Director(s)

The Director(s) shall receive and evaluate regular compliance reports provided by the Compliance Officer and, where required, authorize changes based on the Compliance Officer's recommendations.

The Director(s) will also receive reports on particularly significant changes that may present risk to the Company as well as conflict of law and make the final decision regarding other sanctions-related issues escalated by the MLCO as required by this Policy.

The Compliance Officer

The responsibilities of the Compliance Officer with regard to the Company's Sanctions Policy shall include:

- undertaking sanctions risk analysis of alerted transactions and/or potential and existing Clients including assessment of documentary evidence provided by Clients;
- proposing any necessary amendments to this Sanctions Policy and submitting them to the Board for approval;

- ensuring that all relevant employees are periodically informed of any changes in sanctions legislation, policies and procedures, as well as current developments and changes in sanctions evasion activities particular to their jobs;
- reviewing Client identification information to ensure that all the necessary information has been obtained.

All Other Employees

All Company employees should maintain continual awareness of the risk that sanctioned parties/transactions pose to the Company and its Client base and must not allow the Company to be used as a conduit for sanctions evasion. To support this, all staff are required to:

- Comply with this Sanctions Policy, related procedures, and applicable sanctions laws and regulations.
- Remain alert and promptly report to the Compliance Officer possible sanctions violations, or Clients found to be engaging in sanctions evasion activities or violations of this Policy or related procedures.
- Refrain from providing advice or other assistance to individuals or entities who seek to violate or attempt to violate any sanctions law or regulation, this Policy, or related procedures.
- Complete all required sanctions compliance training in a timely manner.
- In discussion or correspondence with Clients, staff are strictly prohibited giving any form of advice which might be seen as helping Clients to structure transactions or accounts in a way which could constitute sanctions evasion.

Sanction Screening

The Company must ensure that sanctions screening is performed on existing and prospective Clients, connected parties, transactions and third parties against sanction lists.

The specialized third party risk management solution selected by the Company shall ensure ongoing sanction screening process after a business relationship is established. The potentially matching data from various sanctions and watchlists is compared against the applicant profile to establish an exact match, before a match status is assigned. The following types of status may be assigned:

True positive: Applicant data exactly matches one or several watchlist records.

Potential match: Name of the applicant matches one or several watchlist records, but the age/year of birth data is missing, or the applicant is suspected of committing a crime.

False Positive: Applicant data does not match any of the watchlist records.

- Applicant data matches the watchlist record exactly, but additional information clearly shows that the applicant and the person on the record are different people.
- Applicant data matches the watchlist record, but the record does not include criminal or suspicious information about a person. For example, if the applicant is a crime journalist, and their name features on the article as the author.

Unknown: Applicant name in the document contains only one word.

Applicants with “True Positive” and “Potential Match” statuses are delegated to the Compliance Officer for further processing. If applicants are declined based on a watchlist match, they are assigned a respective rejection tag:

- Sanctions
- PEP
- Criminal records
- Adverse Media

The sanction lists screened include (non-exhaustive list of sources):

European External Action Service (EEAS)	
CFSP Consolidated Financial Sanctions List	Consolidated list of all persons, groups, and entities subject to EU financial sanctions. The CFSP list is the official EU database. It includes the financial sanctions from the anti-terror regulations, the country-specific embargo regulations, and other sanctioning regulations such as those against cybercrime or serious human rights violations.
Council of the European Union	
EU – Russia embargo: Restrictions for dual-use goods intended for listed organisations.	This list contains Russian organizations concerned by the sanctions laid down in light of Russia’s actions to undermine Ukraine's stability. The list contains the entries of annex IV of Council Regulation (EU) No. 833/2014 of July 31, 2014, and amended by Council Regulation (EU) No. 960/2014 on September 8, 2014.

EU – Russia embargo: Restrictions on access to the capital market.	It lists Russian entities that are more than 50% state-owned and are subject to the sanctions laid down with respect to Russia's actions contributing to Ukraine's destabilization. The list consolidates the entries of annex III of Council Regulation (EU) No. 833/2014 of July 31, 2014, and of annexes II and III of the related amending regulation 960/2014 of September 8, 2014.
UK lists - HM Treasury – The UK government's economic and finance ministry	
BOE Consolidated List of Financial Sanctions Targets in the UK	Database of all listed persons, groups, and entities subject to financial sanctions by the UN and the UK.
List of entities subject to capital market restrictions (former Ukraine Sovereignty List)	The List of entities subject to capital market restrictions, provided by HM Treasury, lists Russian entities that are more than 50 % state-owned and are subject to the sanctions laid down with respect to Russia's actions contributing to Ukraine's destabilization. These sanctioned organizations are subject to other financial and investment restrictions and are therefore not included in the OFSI Consolidated List of Financial Sanctions Targets in the UK (BOE list). The list consolidates the entries in Schedule 2 of the Russia (Sanctions – EU Exit) Regulations 2019.
Foreign, Commonwealth & Development Office Sanctions List	With the UK Sanctions List, the British government provides a list of persons, entities, or means of transport that are subject to both financial sanctions and restrictions on entry, trade, and other restrictions depending on the respective national sanctions regimes of the United Kingdom. This is based on the Sanctions and Anti-Money Laundering Act 2018 (SAML) and UN Security Council resolutions.
US lists - Department of Commerce – Bureau of Industry and Security (BIS)	
Denied Persons List	The Denied Persons List contains the names of those who have violated US export regulations and against whom the Bureau of Industry and Security has therefore issued a denial order. The listed persons have been denied all exporting privileges, meaning that no US goods can be provided to or purchased from them. Businesses that violate such a denial order are in violation of US export regulations and risk being listed on the DPL themselves.
Entity List	The Entity List lists persons and entities implicated by American authorities as posing a significant threat in the proliferation of weapons of mass destruction or missile technology.

Military End User List	The Military End User List contains companies that are classified by the US government as military end users. According to the findings of the US authorities, the listed companies pose a significant risk of a military end-use of the goods from Supplement No. 2 to Part 744 EAR.
US lists - Department of the Treasury – Office of Foreign Assets Controls (OFAC)	
Specially Designated Nationals List	The SDN list contains the names of all persons, groups, and entities worldwide implicated by American authorities as involved in terrorist activities threatening US security. Active SDN sanctions programs: - Balkans-Related Sanctions - Belarus Sanctions - Blocking Property of Certain Persons Associated with the International Criminal Court Sanctions - Burundi Sanctions - Central African Republic Sanctions - Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) - Counter Narcotics Trafficking Sanctions - Counter Terrorism Sanctions - Cuba Sanctions - Cyber-related Sanctions - Democratic Republic of the Congo-Related Sanctions - Foreign Interference in a United States Election Sanctions - Global Magnitsky Sanctions - Hong Kong-Related Sanctions - Iran Sanctions - Iraq-Related Sanctions - Lebanon-Related Sanctions - Libya Sanctions - Magnitsky Sanctions - Mali-Related Sanctions - Nicaragua-Related Sanctions - Non-Proliferation Sanctions

	- North Korea Sanctions - Rough Diamond Trade - Somalia Sanctions - Sudan and Dafur Sanctions - South Sudan-Related Sanctions - Syria Sanctions - Syria-Related Sanctions - Transnational Criminal Organizations - Ukraine-/Russia-Related Sanctions - Venezuela-Related Sanctions - Yemen-Related Sanctions - Zimbabwe Sanctions
OFAC-CSL Consolidated Sanctions List (OFAC)	With the Consolidated Sanctions List, the OFAC provides a consolidated list of all persons and entities of its non-SDN sanctions programs. The Consolidated Sanctions List is not part of the Specially Designated Nationals and Blocked Persons List (SDN) of the OFAC. Nevertheless, it is possible that individual entries are also included in the SDN list. The OFAC Consolidated Sanctions List includes the following sanctions lists, for example: - Foreign Sanctions Evaders (FSE) List - Sectoral Sanctions Identification (SSI) List - Palestinian Legislative Council (NS-PLC) List - Non-SDN Iranian Sanctions Act (NS-ISA) List - List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List) - Non-SDN Menu-Based Sanctions (NS-MBS) List - Non-SDN Communist Chinese Military Companies (NS-CCMS) List
United Nations Security Council	
UN Consolidated United Nations Security Council Sanctions List	Consolidated list of all persons, groups, and entities subject to UN Security Council sanctions. The consolidation is to facilitate the implementation of the measures introduced by the UN. The listed persons and entities are subject to various sanctions regimes that provide for different measures.

In case of positive matches against sanctions lists, the action performed by the MLCO will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, or debt/equity

restrictions etc.) as well in consideration with any potential conflict of law.

Sanctions Evasion

UN, U.S., and EU sanctions programs include prohibitions on evasion of their principal provisions, with authorities increasingly focusing on evasion as its own category of sanctioned activity.

Examples of attempts to evade sanctions may include:

- Client (natural or legal person) who is not on any applicable sanctions list purchases cryptocurrency on behalf of a business entity owned by a sanctioned party.
- Where a payment is rejected by the Company, and the Client re-issues the payment after changing or removing information, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries (activity known as “wire stripping”).
- Client physically located in the U.S. utilizes VPN to mask IP address, thereby making it possible to engage in a transaction that is permitted in the EU but prohibited for the US Persons; or
- Payments to a party who is located in a non-sanctioned jurisdiction and acting as a “front company” or acting as an intermediary for sanctioned parties or parties in sanctioned jurisdictions.

Potential sanctions evasion activities may be detected by the Company’s staff at various levels of seniority and across different functions, i.e. through engagement with the existing or prospective Clients, business partners, transaction monitoring, ongoing due diligence (ODD) and other. All suspected attempts to evade or circumvent sanctions must be immediately escalated to the Compliance Officer who, after assessing the scenario, may decide that the case should be escalated to the relevant authorities.

In addition to sanctions screening, the Company utilizes its AML/CTF transaction monitoring, Client due diligence (CDD) and other processes to identify potential sanctions evasion activities by its Clients, third parties, and staff.

When performing the review and approval of Clients identified as high-risk according to the Company’s ML/TF risk assessment methodology, the Compliance Officer also reviews the Client for potential sanctions evasion activities.

The results of the investigation shall be recorded in line with the Company’s AML Policy. Potential sanctions evasion activities, if detected, must be included in the AML/CTF and sanctions compliance reporting documents submitted by the Compliance Officer to the Executive Director(s) and the Board.

Asset Freezing

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately

imposes an across-the-board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Luckyroo N.V, the assets include cryptocurrency and fiat currency.

Sanctions Compliance Training

Sanctions compliance training is one of the pillars of the Company’s sanctions compliance programme. The Compliance Officer is responsible for reviewing and updating (where required) the sanctions compliance programme.

The compliance training falls under two categories:

1. Annual General Audience (All Staff) training,
2. Risk-Based/Ad-Hoc training to Staff who perform functions considered to be higher risk from a sanctions perspective, such as roles that entail Client contact, processing Client transactions, or otherwise evaluating Client data, must receive additional targeted training to supplement the annual sanctions learning provided to all Staff.

All Staff must receive annual General Audience (All Staff) sanctions compliance training. All new hires must receive the training within 30 (thirty) days of on-boarding. The General Audience (All Staff) sanctions compliance training shall include, at a minimum:

- Major sanctions regimes (UN, EU, UK, US).
- Major sanctions programs and requirements.
- Sanctions evasion methods and techniques.
- Sanctions risk indicators (‘red flags’).
- Sanctions compliance roles and responsibilities of the Company’s staff.
- Consequences of non-compliance.

All training records, including the training content (e.g. presentation slides, post-course assessment) and attendance records must be kept in line with the record-keeping requirements.

Outsourcing

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

Record-Keeping And Record Retention

The Company adopts one set of record-keeping and record retention rules and requirements to all sanctions-related items as set by the Company’s AML Policy.

Appendix IV

Client Acceptance Policy

Statement of the Policy

Luckyroo N.V. has implemented this Customer Acceptance Policy (“CAP”) to establish clear standards and procedures for assessing and approving customers who wish to access its online gaming and betting services. The purpose of this policy is to protect the company from being exploited for unlawful activities such as money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit behaviour, while ensuring full compliance with Curaçao’s legal and regulatory framework.

This policy is aligned with the guidance of the Curaçao Gaming Control Board and forms part of Luckyroo N.V.’s wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also incorporates international best practices, including the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives, and the Wolfsberg Principles.

To comply with Curaçao legislation, the policy integrates the requirements of the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

This policy applies to all directors, officers, employees, contractors, and any third parties involved in onboarding and verification activities. No customer is allowed to deposit, withdraw, or engage in gaming activities until they have met all acceptance criteria and successfully completed the required identification, verification, and screening procedures.

2. Scope of the Policy

This policy applies to every individual or entity that wishes to open an account with Luckyroo N.V., regardless of the registration channel used. This includes account creation through the company’s official website, mobile applications, affiliate partnerships, or third-party platforms.

The provisions of this policy cover the entire customer relationship, starting from the initial registration and continuing through all stages of account activity until closure or termination. It applies to all products and services provided by Luckyroo N.V. under its Curaçao gaming licence OGL/2024/1371/0694.

3. Customer Acceptance Integration

Luckyroo N.V. only accepts customers who meet all applicable legal, regulatory, and internal compliance requirements. Every applicant must be verified to confirm they have reached the legal age for gambling, which is at least eighteen (18) years or higher where required by the laws of their jurisdiction. Applicants are also required to provide accurate and verifiable personal details, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not allow the registration of customers who are residents of, located in, or

conducting transactions from jurisdictions restricted under Curaçao's regulatory framework, international sanctions regimes, or Luckyroo N.V.'s internal prohibited jurisdictions list. As part of the onboarding process, every applicant is screened against international and local sanctions lists, including those maintained by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any lists issued by the Curaçao Gaming Control Board.

All funds used for gaming and betting activities must come from legitimate, lawful sources. Where the company's risk assessment indicates the need for additional scrutiny, customers are required to provide supporting documentation to verify the origin of their funds and, if applicable, their source of wealth. Luckyroo N.V. also reserves the right to deny service to any individual or entity with a history of fraudulent behaviour, chargebacks, bonus abuse, self-exclusion due to problem gambling, or any other violation of gambling regulations.

4. Risk-Based Approach

Luckyroo N.V. applies a thorough Risk-Based Approach (RBA) during both the onboarding process and the ongoing assessment of its customers. This approach ensures that the level of due diligence applied is proportionate to the customer's individual risk profile. The evaluation takes into account a range of factors, including the customer's personal and financial background, the types of products and services they use, any geographic risks associated with their location or funding sources, and potential risks arising from the technologies or channels they use to access the platform.

Customer Risk Profile

Luckyroo N.V. assesses every prospective customer to determine their level of exposure to risks such as money laundering, terrorist financing, or proliferation financing. This assessment ensures that due diligence measures are applied proportionately to each customer's profile.

Customers who present clear, transparent, and verifiable financial backgrounds — for example, those with stable employment in low-risk sectors and gambling activity that aligns with their declared income — are typically classified as low risk.

Conversely, customers may be considered high risk if they exhibit certain characteristics, such as having multiple or opaque income sources, employment in industries with elevated AML risk like cryptocurrency or unregulated financial services, or transaction patterns that appear inconsistent with their stated financial profile. Politically Exposed Persons (PEPs), their family members, and close associates are automatically categorised as high risk and are subject to stricter controls.

High-risk cases are managed through Enhanced Due Diligence (EDD), which may include more detailed verification procedures, additional documentation requirements, and ongoing monitoring. Examples of high-risk scenarios include:

- Customers with multiple or irregular income sources, who must provide evidence such as payslips, tax returns, business records, or investment statements.
- PEPs or their close associates, whose accounts require senior management approval, detailed source-of-wealth and source-of-funds checks, and ongoing enhanced monitoring.
- High or disproportionate spenders, where gambling activity exceeds what would reasonably match a customer's financial profile, requiring additional documentation and scrutiny.

- Customers exhibiting sudden, unexplained changes in gambling patterns or those using third parties to transact on their behalf, triggering immediate review and investigation.
- Attempts to operate multiple accounts, which are identified through internal monitoring systems and consolidated for a full transactional review.
- Unknown customers attempting to redeem large volumes of chips, or customers linked to junket operators, both of which require strict verification and EDD measures.

Luckyroo N.V. also conducts ongoing monitoring to ensure customer risk profiles remain accurate and up to date. Periodic reviews are scheduled, and additional checks are triggered whenever significant changes are detected, such as unusual transaction patterns, large unexplained deposits, or changes to a customer's personal or financial circumstances. Where risk levels increase, the company applies enhanced controls — including EDD, closer transaction monitoring, or restrictions on account activity — to ensure risks remain effectively mitigated and regulatory obligations are consistently met.

Geographic Risk Assessment

Luckyroo N.V. uses a dynamic geographic risk framework to evaluate potential risks linked to a customer's location or the origin of their funds. This framework is regularly updated based on trusted and authoritative sources, including publications and lists from the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high-risk country listings, the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from jurisdictions subject to international sanctions are not accepted under any circumstances. Those from high-risk jurisdictions may be considered for onboarding only after Enhanced Due Diligence (EDD) is completed and senior compliance approval is granted.

Jurisdictions are considered high risk when they exhibit one or more of the following characteristics: inadequate anti-money laundering and counter-terrorist financing frameworks or poor enforcement of such measures, systemic corruption that increases the likelihood of illicit funds entering the platform, association with international sanctions related to terrorism or weapons proliferation, or active presence of terrorist organizations.

To maintain accurate classifications, Luckyroo N.V. continuously monitors relevant global and regional sources. These include FATF high-risk and monitored jurisdictions lists, CFATF advisories, the European Commission's list of countries with strategic AML/CFT deficiencies, OFAC sanctions lists, U.S. State Department reports, and corruption indices or reports indicating potential links to terrorist financing.

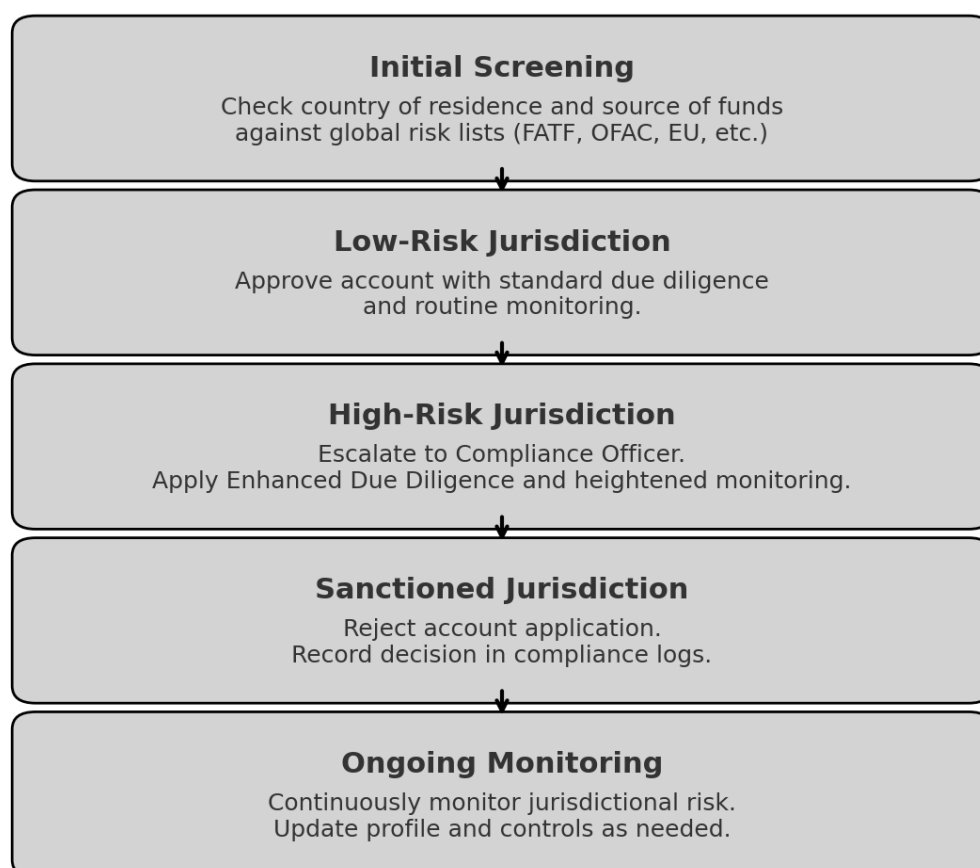
When a customer's country of residence or source of funds appears on a high-risk or sanctioned list, the case is escalated to the Compliance Officer. In such instances, EDD measures are mandatory, including in-depth identity verification, a thorough review of the source of funds and source of wealth, and enhanced transaction monitoring for as long as the relationship continues.

Geographic Risk Assessment Process

1. **Initial Screening** – The customer's location and funding sources are checked against global lists and reports to determine their risk level.

2. **Low-Risk Jurisdiction** – The account may be approved under standard due diligence procedures with routine monitoring.
3. **High-Risk Jurisdiction** – The application is escalated to compliance for review. Onboarding is only approved if all EDD criteria are satisfied, and heightened monitoring is applied.
4. **Sanctioned Jurisdiction** – The application is rejected, and records are retained in compliance logs.
5. **Ongoing Monitoring** – Customer profiles are dynamically updated, and additional controls are applied if jurisdictional risk changes over time.

Geographic Risk Assessment Flow



Product, Service, and Transaction Risks

The level of risk associated with a customer is also determined by the products, services, and transaction types they use. Certain activities naturally carry a higher degree of risk due to reduced transparency and traceability. Examples include peer-to-peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi-anonymous payment methods such as prepaid cards or specific cryptocurrencies.

Accounts that are used mainly for financial transactions rather than genuine gameplay — such as those making large deposits followed by minimal or no betting activity before withdrawals — are treated with caution and subject to closer review. Likewise, the use of payment instruments not registered in

the account holder's name automatically triggers additional verification measures to confirm legitimacy.

To mitigate these risks, Luckyroo N.V. actively monitors and manages several key risk areas. Funds deposited into gaming accounts must always originate from lawful and verifiable sources. If there are signs that funds may be linked to criminal activities such as fraud, theft, or trafficking, customers are required to provide evidence of the legitimate source of those funds, and any suspicious transaction is reported to the Financial Intelligence Unit (FIU) in line with legal requirements.

Anonymous or semi-anonymous payment channels, including prepaid cards and certain virtual assets, are treated as high risk and subject to enhanced verification procedures, with full documentation of the source of funds. Accounts must also be used solely for genuine gaming purposes. Any behaviour suggesting misuse, such as depositing and withdrawing without significant gameplay, triggers an immediate review and may lead to account suspension during investigation.

Transactions involving third-party payment methods are flagged and subject to full verification of both the customer and the third party, including establishing the relationship between them and confirming the legitimacy of the funds. Similarly, transfers between gaming accounts are generally prohibited unless a legitimate and documented reason exists, in which case approval from the Compliance Officer is required, and full records of the transaction are maintained.

Operating multiple accounts or wallets — including those on different platforms under the company's control — is considered a red flag. Internal monitoring systems are designed to detect and link related accounts, ensuring consolidated oversight and the ability to conduct a thorough review of all connected activity. Customers who frequently change their payment methods or banking details may also be attempting to obscure the origin of funds; such patterns prompt a detailed profile review and, where appropriate, the application of Enhanced Due Diligence (EDD).

Luckyroo N.V. applies robust identity verification and authenticity checks to prevent and detect identity fraud. Any suspected cases are escalated to the relevant authorities in line with regulatory obligations. Additional controls are applied to the use of electronic wallets, particularly where providers are licensed in jurisdictions with weak AML or CTF oversight or where their structures make it difficult to trace funds. Customers using e-wallets are required to verify the source of their funds, and the provider's licensing and compliance standards are checked before any transaction is approved.

Channel and Technology Risk

The level of risk associated with a customer also depends on the channels and technologies used to access Luckyroo N.V.'s services. Remote onboarding, while convenient, carries a higher risk of identity fraud or impersonation. To address this, the company relies on advanced digital Know Your Customer (KYC) solutions that include biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

Before introducing any new technologies, payment solutions, or platform features, Luckyroo N.V. conducts a comprehensive risk assessment to ensure the innovation cannot be misused for money laundering, fraud, or other illicit purposes.

Several factors are monitored closely to manage channel and technology-related risks. Any method that allows customers to remain anonymous is considered high risk and triggers enhanced verification measures. These measures include identity document validation, biometric checks, and real-time screening against sanctions and Politically Exposed Person (PEP) lists.

Remote interactions, although common in the industry and not inherently high risk, still demand strong safeguards. Luckyroo N.V. uses secure verification technologies such as biometric checks, liveness detection, and automated document validation to prevent impersonation and fraud during onboarding and transactions.

When third parties are involved in customer interactions, the risk profile increases, especially if the intermediary is not subject to AML/CFT obligations. In such cases, Luckyroo N.V. performs due diligence not only on the customer but also on the third party. This process includes verifying the intermediary's regulatory status, assessing its compliance framework, and ensuring all provided information is accurate and verifiable.

Channel and Technology Risk – Staff Checklist

Anonymous Channels Apply enhanced verification: ID validation, biometric checks, and sanctions screening.
Remote Onboarding Use biometric authentication, liveness detection, and document authenticity checks.
Remote Transactions Enable multi-factor authentication and monitor for device/IP anomalies.
Third-Party Interactions Verify intermediary licensing, assess AML/CTF framework, and validate provided data.
New Technologies Perform pre-launch risk assessment and compliance approval.

Risk Indicators

Luckyroo N.V. applies a structured set of risk indicators to assess the level of risk associated with every customer relationship. These indicators form part of the company's Risk-Based Approach (RBA) and ensure that the level of due diligence applied is always proportionate to the customer's overall risk profile.

The evaluation covers multiple categories:

- **Customer Risk Profile** – factors such as multiple or irregular income sources, Politically Exposed Persons (PEPs), high or disproportionate spending, sudden changes in spending behaviour, involvement of third parties, multiple accounts, unknown chip redemptions, or links to junket operations.
- **Product, Service, and Transaction Risk** – warning signs such as proceeds of crime, anonymous or unregulated payment methods, misuse of accounts, third-party funding, frequent changes in payment instruments, identity fraud, or the use of multiple e-wallets.
- **Geographic Risk** – customers connected to jurisdictions with weak AML/CFT frameworks, high levels of corruption, international sanctions, terrorism links, or countries listed by FATF, CFATF, OFAC, or Transparency International's CPI.
- **Channel and Technology Risk** – customers accessing services through anonymous or unverified channels, onboarding remotely without sufficient identity validation, or relying on

unregulated third-party intermediaries.

To determine the customer's overall risk, the company uses an internal Risk Calculator that assigns a weighted score to each indicator. The total score determines the customer's classification:

Risk Level	Requirements
Low Risk	Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile.
Medium Risk	Standard CDD plus additional verification steps and closer ongoing monitoring.
High Risk	Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.

This risk-scoring approach ensures a consistent and methodical assessment of customers, allowing the company to allocate its resources effectively and meet its regulatory obligations.

Risk Indicators Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gaming.	Professional-level gambling or consistent high-stakes play.	Bonus exploitation or behaviour aimed at financial abuse of promotions.
Source of Funds	Regular salary, savings, pensions, or other low-risk income.	Business income, legitimate casino winnings, sale of personal assets, inheritance, or documented loans/gifts from family or friends.	Unverified cryptocurrency, offshore accounts, or other unverifiable sources.

Source of Wealth	Long-term employment income, ownership of established businesses, verified inheritance, or steady investment growth.	Sale of property or business, significant lottery or gambling winnings.	High-risk investments such as cryptocurrency or forex trading, offshore holdings, or unverifiable assets.
Transaction Frequency	Occasional, typically monthly.	Regular, often weekly.	Frequent, typically daily.
Transaction Value (NAF)	Up to 1,000.	Between 1,000 and 4,000.	Over 4,000.
Incoming Payments	Standard bank transfers or debit/credit card deposits.	E-wallet or prepaid card deposits.	Cryptocurrency, third-party funding, deposits from high-risk jurisdictions, unusually high deposits, or use of unregulated processors.
Outgoing Payments	Normal withdrawals of winnings or deposit refunds.	Bonus-related cash-outs, frequent withdrawals, or large single withdrawals above 4,000.	Cryptocurrency withdrawals, third-party payments, chargebacks, or suspicious withdrawal patterns linked to other accounts.
Gaming Behaviour	Casual, moderate, and consistent play patterns.	Frequent high-stakes betting, extended play sessions, or fluctuating wagering amounts.	Aggressive betting patterns, rapid stake increases, loss-chasing, multiple accounts, collusion, or other fraudulent indicators.
Payment Channels	Traditional bank transfers.	Verified e-wallets.	Cryptocurrency or other anonymous or unverified payment methods.

Adverse Media	No negative information identified.	Questionable or unverified reports of misconduct.	Confirmed involvement in criminal or illicit activities.
----------------------	-------------------------------------	---	--

Guidance on Using the Risk Indicators

These indicators are designed to help staff assign an accurate risk profile to each customer during onboarding and throughout the customer relationship. Each factor should be assessed individually, and the combined results should inform the overall risk classification.

- Customers with mostly low-risk indicators are assigned a low-risk profile and subject to standard Customer Due Diligence (CDD).
- Customers with a mix of low and medium-risk indicators are classified as medium risk and require additional verification and closer monitoring.
- Customers displaying one or more high-risk indicators must undergo Enhanced Due Diligence (EDD), senior management approval before onboarding, and ongoing heightened monitoring.

Risk profiles should be reviewed regularly and adjusted when customer behaviour, transaction patterns, or external risk factors change. This approach ensures that the company's risk management remains dynamic and aligned with regulatory expectations.

5. Onboarding Procedures

Luckyroo N.V. follows a structured and well-documented onboarding process to ensure that only customers meeting the company's acceptance standards gain access to the platform. No account is activated until the customer has successfully completed all required identification, verification, and sanctions screening steps.

During registration, customers are required to provide their full legal name, date and place of birth, nationality, residential address, and an official identification number such as a passport or national ID.

Every applicant is screened against international sanctions and Politically Exposed Person (PEP) databases using automated tools to ensure comprehensive coverage. Any potential matches or alerts are reviewed manually by trained compliance officers to confirm accuracy and rule out false positives.

If a customer is identified as high risk during the initial assessment, additional verification is required. This includes providing documentation to confirm the legitimacy of their funds and, where relevant, the source of their wealth. Acceptable documents may include recent bank statements showing income deposits, business account records or financial statements, tax returns, contracts of property or asset sales, and investment account statements. These enhanced measures ensure that the company meets regulatory expectations and maintains a strong control framework to protect the platform from misuse.

Client **Identification requirements and verification procedures**

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

Document verification is intended to prevent the following issues:

Forgery
Data tampering
Photo replacement
Fraud
Using document printouts
Other manipulation

The ID document must contain as minimum the following information:

Owner full name
Owner full date of birth
Document number
Validity data (issue date or validity period)
Owner photo
Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.

If the document has data on the front and back, both sides should be uploaded.

The size of the uploaded file is no less than 100 KB or 300 DPI.

The photo is in color.

The information in the document is readable.

All corners of the document are visible and no foreign objects or graphic elements are present.

The uploaded photo has not been edited with any software or converted to PDF.

The document is not digital (in most cases).

Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

1. Proof of address verification

a. Face-to-face procedures

For the purpose of face-face Client identification, the MLCO shall inspect the person's original Proof of Address (PoA) documentation and make a certified true copy to be maintained as evidence of verification.

b. Non-face to face procedures

The process of Proof of Address (PoA) document verification for non-face to face Clients consists of the following steps:

- **Uploading a PoA photo.**

By default, the system accepts PoA documents that have been issued within the last 3 months.

- **Checking the image for authenticity.**

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- **Checking the integrity of the image.**

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.
- **Data extraction** (full name, home address, issue date).
- **Data validation** (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the MLCO to see the applicant's geolocation in the Dashboard.

Supported PoA Documents

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.
- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.
- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).
- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.
- Letter from a recognized public authority or public servant (any government-issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases). Both paper documents and electronic documents (in PDF) are accepted.

Alternative proof of residency examples

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card

- Driving license
- Residence permit (EU samples containing address)

**** The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

Documents which are not acceptable as Proof of Address, include:

- Old government-issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills
- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address
- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies
- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

Source of Funds (SoF) and Source of Wealth (SoW)

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Examples of SoW and SoF and supporting documentation that can be provided, include:

Income category	Documents required
Income from salary	• Pay slips for the past 3 months and bank statement showing the salary being paid into this bank account; • Audited personal tax statement.
Inheritance	• Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance and a bank statement showing these funds being deposited into the account; • Signed letter from a licensed solicitor or estate trustees on letter-headed paper clearly indicating the amount of inheritance, accompanied by updated proof of the solicitor's regulated status and a bank statement showing these funds being deposited into the account.
Gift/donation	• Notarized gift/ donation letter and a bank statement showing these funds being deposited into the account; • Gift agreement and a bank statement showing these funds being deposited into the account.
Savings/deposits	• Savings statement; • Bank statement.
Government grants (retirement income, grants for veterans, research grant, etc.)	• Type of received grant and a bank statement showing these funds being deposited into the account; • Documents confirming/ proving received grant and a bank statement showing these funds being deposited into the account.
Company profit / dividends	• Dividend contract note or equivalent and a bank statement showing these funds being deposited into the account; • Copy of latest audited financial statements; • Tax declaration form.
Loan or investment	• Loan/Investment agreement or other documents confirming the agreement and a bank statement showing these funds being deposited into the account.

Sales (of property, goods, shares, etc.)	• Copy of contract of buy/sale/production and a bank statement showing these funds being deposited into the account; • Prove of e-shop sale report (screenshot) with the list of items sold and a bank statement showing these funds being deposited into the account; • Shipping documents and a bank statement showing these funds being deposited into the account; • Proof of delivery and a bank statement showing these funds being deposited into the account; • Customs declaration; • Audited financial report; • Tax report; • Statement evidencing the money and a bank statement showing these funds being deposited into the account.
--	---

6. Ongoing Monitoring

Luckyroo N.V. recognises that customer acceptance is an ongoing process rather than a one-time activity. Continuous monitoring is essential to ensure that customer behaviour remains consistent with the profile established during onboarding and that any irregularities or deviations are promptly identified and addressed.

The company uses automated transaction monitoring systems to detect patterns of unusual or suspicious behaviour. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without meaningful gameplay, the use of multiple or unusual payment methods, or patterns that may suggest collusion, chip-dumping, or other prohibited activities.

Each alert is reviewed by trained compliance officers, who assess the circumstances and determine whether further investigation or escalation is needed.

In addition to real-time monitoring, the company conducts periodic reviews of customer profiles on a risk-based schedule to ensure risk ratings remain accurate. If there are material changes in a customer's situation, such as relocation to a high-risk jurisdiction, significant increases in transaction values, or changes in funding methods, the customer's risk profile is immediately reassessed. Where necessary, enhanced monitoring and other controls are applied to maintain compliance and mitigate potential risks.

7. Prohibited clients and transactions

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- c. Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.
- d. Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (Appendix II).
- e. Conclude or implement any business relationship with a credit institution or other financial institution or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions or legal person that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful management and which is unaffiliated with a regulated financial group (i.e. shell company) or is known to permit accounts to be held by a shell bank.
- f. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity including (but not exhaustive)
 - Terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out on Titles II and III of Directive (EU) 2017/541 (replacing Framework Decision 2002/475/JHA on combating terrorism)
 - Any of the offences referred in article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
 - The activities of criminal organizations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA on the fight against organized crime;
 - Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU;
 - Sexual exploitation, including any offence set out in Directive 2011/93/EU;
 - Fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1 (1) and Article 291) of the Convention on the protection of the European Community's financial interests;
 - Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the EU Communities or officials of Member States of the EU;
 - All offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national Laws of Lithuania and which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, if there is a legal threshold by Law for such offences, all offences punishable as above for a minimum of more than six months;
 - Counterfeiting of currency, including any offence set out in Directive 2008/99/EC;
 - Cybercrime, including any offence set out in the Directive 2013/40/EU;
- g. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:

- Legal entities are owned through bearer instruments;
 - Legal entities are involved in the adult industry;
 - Legal entities are involved drugs industry;
 - Legal entities are involved in arms industry;
 - Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;
 - Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
 - Purchase or sale of virtual assets ultimately owned or controlled, directly or indirectly, by sanctioned parties;
 - Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- h. Establish a business relationship and/or conduct transactions with natural or legal persons residing in a jurisdiction/country where it is prohibited by Company policy to offer its services to. Prohibited jurisdictions / countries shall include:

Unrecognised / Disputed Territories

Crimea	Republic of Abkhazia
Donetsk	Republic of China (Taiwan)
Luhansk	Republic of Kosovo
Nagorno Karabakh Republic	Republic of Somaliland
Palestine	Republic of South Osetia
Pridnestrovian Moldavian Republic	Turkish Republic of Northern Cyprus

Prohibited Jurisdictions / Countries

Australia	Libya
Belarus	Mali
Belize	Netherlands
Central African Republic	North Korea
Cuba	Russia
Curaçao	Somalia
Democratic Republic of Congo	Sudan
Dutch West Indies (Aruba, Bonaire)	Syria
France	Turkish Republic of Northern Cyprus
Germany	UK
Iran	USA
Iraq	Yemen
Lebanon	Libya

8. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) procedures are applied to customers who present an elevated risk profile. This includes Politically Exposed Persons (PEPs), their family members, and close associates; customers based in or funding their accounts from high-risk jurisdictions; those conducting unusually large, complex, or unexplained transactions; and customers whose financial behaviour is inconsistent with their declared income or business activities.

EDD involves a more detailed and rigorous verification process than standard due diligence. This includes a full analysis of the customer's source of funds and source of wealth, supported by credible and independent documentation. Additional steps include corporate registry and public record searches to verify legal and beneficial ownership, confirmation of employment or business ownership, reviews of audited financial statements or other reliable financial documents, and thorough adverse media and reputational checks.

Senior management approval is required before onboarding any high-risk customer, and in complex or sensitive cases, formal approval from the Board of Directors may be necessary.

Once these customers are onboarded, they are subject to ongoing enhanced monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of their transaction patterns, and more frequent reassessments of their risk profiles. These measures ensure that higher-risk relationships are managed appropriately, in full alignment with both regulatory obligations and the company's internal risk appetite.

Prohibited Customer Categories

Luckyroo N.V. will not onboard or will immediately terminate relationships with customers who meet any of the following criteria:

- Anonymous or unverifiable customers, including those who fail or refuse identity verification within 30 days.
- Shell companies, fictitious entities, or customers with unclear beneficial ownership.
- Sanctioned individuals or entities, including those appearing on UN, EU, OFAC, OFSI, SNO, or Kingdom Sanction Act lists.
- Residents of or transacting from prohibited or sanctioned jurisdictions, as defined in Section 4 (Geographic Risk).
- Customers below the legal age for gambling.
- Customers involved in fraud, bonus abuse, identity theft, or other illicit behaviour.
- Third-party transactors or users of anonymous payment channels without valid justification or verification.
- Customers whose source of funds or source of wealth cannot be verified or is linked to crime.

Acceptance and Rejection Triggers

Customer applications will be immediately rejected or suspended when any of the following triggers

occur:

a. Documentation and Verification Failures

- Refusal to provide KYC, proof of address, or EDD documentation.
- Submission of false, altered, or misleading information.
- Failure to complete mandatory verification within 30 days.

b. AML/CTF/CPF Risk Triggers

- Positive sanctions match or verified PEP hit without manageable risk.
- Suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.
- Inability to verify SOF/SOW after reasonable attempts.

c. Behavioural and Transactional Triggers

- Highly unusual deposit/withdrawal activity inconsistent with profile.
- Multiple accounts, third-party payments, or misuse of payment instruments.
- Attempts to circumvent controls or operate through intermediaries.
- Evidence of collusion, chip dumping, or non-genuine gameplay.

9. Termination

Luckyroo N.V. reserves the right to suspend or terminate any customer relationship when required by regulations, internal policies, or risk considerations. This action may be taken if a customer fails to provide the requested identification or supporting documentation within 30 calendar days, if there is reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in activities that violate applicable laws, regulations, or the company's Responsible Gambling Policy.

When a relationship is terminated due to suspected criminal activity, the company promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds pending investigation. Detailed records of all termination actions, including the rationale and supporting evidence, are maintained for at least five years.

Luckyroo N.V. will refuse to onboard or will terminate an existing relationship in cases where:

- The customer is a resident of, located in, or conducting transactions from a prohibited or sanctioned jurisdiction.

- The customer fails to provide required information or documentation within the specified timeframe.
- False, misleading, or incomplete information is provided during registration or verification.
- The source of funds or source of wealth cannot be confirmed as legitimate.
- The customer is involved in, or suspected of, money laundering, terrorist financing, or other criminal activity.
- The customer is a Politically Exposed Person (PEP) whose risk profile cannot be mitigated to an acceptable level.
- Fraudulent activities, bonus abuse, collusion, or prohibited gambling behaviour are detected.
- The customer attempts to use third parties to transact without proper disclosure and verification.
- The customer has self-excluded or been excluded for responsible gambling reasons.
- Large chip redemptions or withdrawals are requested without verifiable linked gambling activity.
- The customer is a minor or below the legal gambling age in their jurisdiction.

10. Curaçao's Legislative Framework

Luckyroo N.V. acknowledges that its Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to fully comply with Curaçao's legal and regulatory requirements, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is treated as a priority in daily operations. The customer acceptance procedures are embedded within the company's compliance processes to ensure due diligence is continuous and extends beyond onboarding. This approach ensures that any significant changes in a customer's risk profile, transactional behaviour, or jurisdiction are identified and addressed promptly.

All employees involved in onboarding and verification activities receive dedicated training to help them understand the legislative framework and the company's internal standards. The training focuses on effectively applying the Risk-Based Approach, identifying and escalating high-risk indicators, and following escalation protocols to the Compliance Officer or senior management.

Independent audits are conducted at least annually to evaluate how effectively the Risk-Based Approach and the Customer Acceptance Policy are being implemented. These audits review critical processes, such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD) procedures, and the ongoing monitoring of customer activities. The findings are reported to the Board of Directors, and any gaps or deficiencies are addressed promptly through corrective measures implemented within defined timeframes.

11. Responsible Gambling Integration

Luckyroo N.V. ensures that its Customer Acceptance Policy is fully aligned with its Responsible Gambling Policy, recognising that protecting customers from gambling-related harm is a key part of

its compliance and operational framework.

If a customer shows behaviour that indicates potential harm, such as frequent deposits that exceed their apparent financial capacity or excessively long gaming sessions, the company takes immediate action. Depending on the situation, this may include setting deposit or wagering limits, temporarily suspending the account, or, in severe cases, refusing further access to services to protect the customer.

Self-exclusion requests are handled promptly and applied to all accounts linked to the customer to ensure these measures cannot be bypassed. These restrictions remain active for the period specified by the customer or as required by regulatory standards.

Employees in customer-facing roles receive targeted training to help them identify early signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring activities, enabling timely intervention when risk indicators are observed.

12. Review and Governance of CAP

This Customer Acceptance Policy (CAP) is reviewed at least once every twelve months to ensure that it remains effective, compliant with legislative and regulatory requirements, and consistent with industry best practices. The review process also takes into account any changes to the company's risk profile, emerging patterns in customer behaviour, and technological advancements that could create new risks or vulnerabilities.

Proposed revisions or updates are prepared by the Compliance Officer and submitted to the Board of Directors for approval prior to implementation. All updates are thoroughly documented, and relevant staff are informed and trained to ensure that the revised policy is applied consistently and accurately throughout the company's operations.

13. Record Keeping

Luckyroo N.V. keeps detailed records of all customer acceptance activities for at least five years after the end of the business relationship, in accordance with regulatory requirements. These records include identification and verification documents, proof of address, evidence of the source of funds and source of wealth, transaction monitoring alerts and investigation reports, Enhanced Due Diligence (EDD) files, internal compliance reviews, and documentation of any account suspensions or terminations.

All records are stored securely in encrypted formats with strict access controls to ensure confidentiality and data protection. Only authorised personnel have access to these records, and all access activity is logged and periodically reviewed to verify compliance with internal policies and applicable data protection regulations.