

ASPRO N.V.**Dr. H. Fergusonweg 1, Curacao****Anti-Money Laundering and
Counter-Terrorist Financing Policy****Approved by the Board of Directors**

Company Name	Aspro N.V.	Aspro N.V.	Aspro N.V.
Version	2024/V.1	2024/V.2	2025/V.3
Date of Approval	January 2024	November 2024	May 2025
Changes implemented	New version	Amendments as per new AML/CFT/CPF regulations (effective as of 15.05.2024)	New AML/CFT/CPF applicable January 2025

Authorized signatory 29 May, 2025	 (SMES) Solutions for Management and Employment Support N.V.
Compliance officer	Rebecca Taiwo Owolabi compliance@aspro-nv.com

This Policy is subject to copyright law and any reproduction of all or part of the contents in any form is prohibited.

Contents

- 1. Policy Statement**
- 2. Key Definitions & Abbreviations**
- 3. Abbreviations**
- 4. Online Casino / Betting Environment**
- 5. Senior Management Responsibility**
- 6. Money Laundering**
- 7. Terrorism Financing**
- 8. Proliferation Financing (PF)**
- 9. ML, TF & PF Risk Assessment**
- 10. Technological Developments Risk Assessment**
- 11. Compliance Officer**
- 12. Customer Due Diligence (CDD)**
- 13. Customer Acceptance Policy (CAP)**
- 14. Enhanced Due Diligence (EDD)**
- 15. Politically Exposed Persons (PEPs)**
- 16. Ongoing Monitoring**
- 17. Termination of Business Relationships**
- 18. Third-Party Reliance on CDD**
- 19. Sanctions Management, License Restrictions, FATF Blacklist –**
- 20. Record-Keeping**
- 21. Suspicious Activity Reporting Guidelines**
- 22. Unusual Transactions**
- 23. Employee Training Policy**
- 24. Audit Function**

POLICY STATEMENT

The purpose of the **Anti-Money-Laundering Policy (the AML Policy)** is to promote company-wide compliance with the local and international Anti-Money Laundering/ Counter Terrorism Funding (AML/CFT/CPF) legislation, implement best AML/CFT/CPF industry standards internally, and uphold all relevant laws in all the jurisdictions Astro N.V. operates in. The AML Policy's framework is based on robust AML/CFT/CPF measures, including the identification and mitigation of the inherent risks associated with customers, products and services, payment methods, countries, and delivery channels.

The AML Policy has been approved by the Board of Directors (BoD) of Aspro N.V. and is subject to an annual review. In addition to the annual review process, periodic amendments of the policy are submitted to the BoD for approval when alterations in AML/CFT/CPF operator practices are advisable and/or a request to implement urgent internal and third-party AML audit recommendations as regards risk probability and risk impact is put forward by a nominated officer.

The AML Policy is a reflection of the main international objectives highlighted by the current 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 (NORUT0), and the National Ordinance on Identification of clients when Rendering Services (NOIS). It also relies on 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.

The Company's directors, officers and personnel are committed to upholding a set of standards set in the Policy in line with the recommendations of the AML/CFT/CPF supervisor in Curacao, namely the Curacao Gaming Control Board.

The Policy applies to all persons at all levels working for the Company and third-party consultants whose services are enlisted from time to time for audit purposes.

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/CPF 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 customers' 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.

Blacklist- 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.

The FATF blacklist is a list of countries that FATF has determined are noncooperative in the international fight against money laundering and terrorist financing.

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. **Customer-** a person that opens an account and transacts with the Company.

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

Customer Due Diligence- a set of internal controls that internet gambling operator establish a customer's identity, predict with relative certainty the types of transactions in which the customer is likely to engage, and assess the extent to which the customer exposes it to a range of risks (i.e., money laundering and sanctions). Organizations also need to know their customers 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/CPF 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 an individual customer or a legal entity, conducted in the process of preparing for a business transaction. Due diligence should be completed before initiating any 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.

Egmont Group of Financial Intelligence Units-The Egmont Group consists of a numerous national of financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the field of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

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 Customer Due Diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer.

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. Its Recommendations do not have the force of law. 35 countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods.

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

First Line of Defense- within the governance structure of a sanction's compliance program, the first line of defense (also referred to as the "front line") includes relationship managers and other customer-facing employees who are closest to the customers and counterparties during the onboarding and contracting phase of relationships. The first-line defense is responsible for ensuring that adequate information is obtained so that effective screening of customers and their owners and controllers can be performed. In general, the first-line defense 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.

Inherent Risk- The level of sanctions risks that exist before controls are applied to mitigate them. There are four main inherent risk categories: customers, 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, customer outreach, and possible escalation to the compliance function.

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

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.

Minor – under the 18 years of age.

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.

Money Laundering Reporting Officer (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 customer 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 customer.

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.

Proliferation Financing (PF): Aspro N.V. is committed to identifying and mitigating the risk of proliferation financing (PF), defined as the provision of funds or financial services used for the manufacture, acquisition, or transfer of nuclear, chemical, or biological weapons and related materials. The Company incorporates PF risk indicators into its risk assessments and customer due diligence procedures in accordance with the FATF Recommendations and Curaçao's legal obligations. PF risks are assessed alongside AML/CFT/CPF risks and subject to ongoing monitoring, reporting, and escalation to the FIU where necessary.

Red Flag (like 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.

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.

"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 customers 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 Customer (KYC) / Customer Due Diligence (CDD) that focuses on the risks specific to sanctions, considering 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.

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 Customer (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 customer 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 customer'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 Defense - The third-line defense within the governance structure of a sanction's compliance program is the internal audit, which involves independent reviews of the controls applied by the first two lines of defense. 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.

Wolfsberg Group- an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global anti-money laundering guidelines for international private banks.

ABBREVIATIONS

AML – Anti-Money Laundering

Compliance Officer. A senior officer at management level and independent from the game's operations, responsible for the detection and deterrence of money laundering and terrorist financing.

BoD – Board of Directors of the Company

CDD - Customer 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 buitengaatsse hazardspelen, P.B. 1993, no. 63)

PEP- Politically Exposed Person

UN- United Nations

ONLINE CASINO/BETTING ENVIROMENT

Aspro N.V. is a Curacao-based legal entity which currently runs the following websites:

www.astrobet.com
www.betingsite.com
www.xparibet.com
www.linebet.com

Aspro N.V., a legal entity established in Curaçao. Company is licensed under Curaçao Gaming Control Board with license number OGL/2024/565/0553 issued 12/11/2024. This license mandates compliance with Curaçao's regulatory requirements and imposes strict restrictions on service provision in specific jurisdictions. As such, Aspro N.V., refrains from offering remote gaming services in the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. The company strictly adheres to this policy, operating exclusively in regions where online gambling is legally permitted, without targeting markets where such activities are prohibited.

E-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 customers or the external payment providers to help them bypass internal safeguards.

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/CPF 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 at least every 6 months based on monthly risk assessments' results and the AML/CFT/CPF Officer may request the approval of the Board of Directors for any changes in its AML/CFT/CPF policy to remedy any identified weaknesses in the internal controls and risk management practices, should they arise.

In alignment with international best practices, senior management oversees the development and implementation of robust employee training programs. These initiatives are designed to enhance staff awareness and understanding of AML/CTF/CPF risks, equipping them—especially those in key roles—to identify and respond effectively to suspicious activities.

Management also ensures the company's internal control systems are comprehensive and include clear segregation of duties, defined authorization processes, consistent monitoring, and thorough documentation. To reinforce regulatory compliance and optimize the effectiveness of the AML/CTF/CPF program, regular independent audits and evaluations are conducted to provide impartial insights and identify opportunities for improvement.

MONEY-LAUNDERING

Money-Laundering is an integral part of any financially motivated crime, often on an international scale, such as tax evasion, violations of sanctions, fraud, corruption, illegal arms trade, drug trafficking, extortion, kidnapping etc. Disguising the illegal origin of the criminal proceeds during its processing, including their identity, source and the destination, defines money-laundering in broad terms. 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). Online gambling sites may therefore constitute just one stage of the money-laundering process, and this is why it is imperative that casino operators do not offer anonymous services to potential customers and/or facilitate transactions of suspicious nature. Terrorism financing is another “amber alert” for the online operators as the money may move through the system in a similar fashion as the laundered money, despite the fact it often comes from legitimate sources whereas the act is committed for religious or other reasons. Broadly speaking, this refers to the funds that are possessed, used, or received with the purpose of financing acts of terrorism. 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.

Key Stages of Money Laundering

Placement:

The initial stage involves introducing illicit funds into the financial system. Common methods include depositing funds into bank accounts, purchasing high-value goods, or conducting other financial transactions. This phase aims to start blending illegal funds into the legitimate economy.

Layering:

In this stage, funds are subjected to a series of complex transactions designed to obscure their origin. Techniques include transferring money across multiple accounts, converting currencies, or investing in financial instruments. The objective is to create a convoluted transaction trail that hinders efforts to trace the funds back to their source.

Integration:

The final stage involves reintroducing the laundered money into the legitimate economy. This is achieved by purchasing luxury assets, investing in cash-intensive businesses, or conducting other legal transactions. By this point, the funds appear legitimate, making them more challenging to link to their illicit origins.

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

- Verification fraud and identity theft (customer due diligence covering documentation verification, age verification and location verification)
- Operation of multiple accounts and high transaction volumes
- 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.
- Using the online platform as a player-to-player transfer route to funnel funds between sellers and buyers and cashing out when necessary.

This list is not exhaustive and whereas additional risks may materialize from time to time, the Company undertakes to carry out systematic risk assessments tailored to the particular areas of concerns and regular training to its employees with the view of strengthening internal AML compliance programs.

TERRORISM FINANCING

Terrorism-financing is another phenomenon, which covers methods and the means used by terrorist organizations to finance their activities as defined by the United Nations, Office on Drugs and Crime. 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 and individuals through charitable organizations or accounts set up at various payment providers. Overall, the FATF (The Financial Action Task Force) Recommendations 2012-2023 identify customer 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/CPF 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/CPF 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/CPF 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/CPF concern due to “the non-face-to face element, huge and complex volumes of transactions and financial flows” involving cryptocurrencies among other payment instruments.

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.

Indicators of Terrorist Financing

Detecting terrorist financing often involves identifying irregular financial behaviors. Key indicators include:

- Unusual transaction patterns that deviate from established business or personal norms.

- Frequent or large fund transfers linked to high-risk regions or known terrorist affiliates.
- Suspicious activities in high-risk industries or financial actions that appear designed to obscure terrorist operations.

Combating Terrorist Financing

To counter the risks associated with terrorist financing, Aspro N.V implements robust Anti-Money Laundering (AML) measures, including:

- Customer Due Diligence (CDD): Ensuring thorough verification of customer identities and financial activities.
- Transaction Monitoring: Actively tracking and analyzing financial activities for unusual patterns.
- Sanctions Compliance: Adhering to established sanctions lists to prevent transactions that might inadvertently support terrorism.

Sanctions lists observed by the company include the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), the Kingdom Sanction Act (N.G. 2016, no. 54), and announcements from the Curaçao Gaming Control Board (GCB). Additionally, lists from the Office of Foreign Assets Control (OFAC), United Nations Security Council, European Union, and U.S. List of Foreign Terrorist Organizations are incorporated to ensure comprehensive compliance.

International Guidelines and Enforcement

Global efforts to combat terrorist financing are supported by:

- Financial Action Task Force (FATF): Setting international standards for identifying and reporting suspicious transactions related to money laundering and terrorist financing.
- Office of Foreign Assets Control (OFAC): Enforcing U.S. economic sanctions and managing the Specially Designated Nationals (SDN) list, which identifies entities involved in terrorism.
- European Union (EU): Mandating member states to implement AML measures and enforce international sanctions to prevent the financial system's misuse.
- United Nations (UN): Imposing sanctions and maintaining lists of individuals and entities linked to terrorism, contributing to global disruption of terrorist funding networks.

PROLIFERATION FINANCING

Proliferation financing refers to the financial support provided for the development, acquisition, or production of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons, as well as their delivery systems. Such financing poses significant risks to global security, and Aspro N.V is fully committed to preventing its involvement in any activities related to proliferation financing. As a licensed casino operator in Curaçao, Aspro N.V adheres to both local regulations established by the Curaçao Gaming Control Board (GCB) and international standards to mitigate risks associated with proliferation financing.

Sources of proliferation financing

1. **Legal Sources:** Proliferation financing may originate from legitimate business activities, such as trade, investments, or charitable donations, which can be exploited by proliferators to funnel money towards the development of WMDs. Aspro N.V ensures that all transactions, particularly those involving international trade or high-risk regions, are subject to thorough scrutiny to prevent misuse in the financing of WMDs.
2. **Illegal Sources:** Similar to other forms of illicit financing, proliferation financing can stem from criminal activities such as smuggling, fraud, and money laundering. Aspro N.V works diligently to identify and prevent any illicit financial activity that may be used to support proliferation-related objectives. By maintaining a robust monitoring system, the company aims to detect and disrupt illicit funding sources early in the process.

Funds used for proliferation financing may be transferred through both formal and informal financial channels:

- **Formal Channels:** Financial institutions, including banks and payment processors, are frequently used for proliferation financing. These funds may be layered through complex transactions designed to obscure their origin and destination. Aspro N.V employs advanced transaction monitoring systems to detect suspicious activities, especially when funds are routed through formal banking systems in a manner that appears designed to conceal the purpose of the transaction.
- **Informal Channels:** Informal financial systems, such as trade-based financing or alternative remittance networks, can also be exploited for proliferation financing. These systems, operating outside of regulated financial institutions, present a significant challenge to detection. Aspro N.V actively monitors for transactions that may involve high-risk jurisdictions or goods that could potentially be used in the development of WMDs, ensuring that all transactions comply with both Curaçao regulations and international sanctions.

Aspro N.V. has implemented comprehensive monitoring to detect potential proliferation financing, including the following indicators:

- **Unusual Trade Transactions:** Transactions involving dual-use goods—items that can be used for both civilian and military purposes—are closely monitored. Aspro N.V. identifies transactions involving countries or entities linked to proliferation activities, ensuring that trade through the platform does not inadvertently support WMD development.
- **Inconsistent Business Practices:** Aspro N.V. remains alert to transactions that appear to lack legitimate business purposes or that are structured in ways designed to evade detection. Suspicious patterns, such as frequent or large transactions that are inconsistent with a customer's normal business activities, are flagged for further review.
- **Suspicious Patterns in Financing:** The company monitors transactions for signs of money laundering or the misdirection of funds intended for legitimate purposes. Transactions involving high-risk regions or known proliferators are flagged and investigated for potential involvement in WMD financing.

Aspro N.V. employs a robust set of measures to combat proliferation financing:

- **Enhanced Customer Due Diligence (CDD):** Aspro N.V. conducts comprehensive customer due diligence (CDD) to verify the identities of its customers, particularly those engaged in international trade or operating in high-risk industries. The company ensures that customers and transactions are legitimate, and that there are no links to proliferation financing or activities involving WMDs.
- **Transaction Monitoring:** The company uses state-of-the-art transaction monitoring systems to detect irregular patterns, particularly in high-risk transactions. Unusual or suspicious activities, such as large cross-border payments, will trigger further scrutiny to ensure that the funds are not being used for illicit purposes, including the financing of WMDs.
- **Sanctions Compliance:** Aspro N.V. adheres to both local and international sanctions programs, including those enforced by the United Nations, the European Union, and the U.S. Office of Foreign Assets Control (OFAC). The company ensures that no transactions are conducted with entities or individuals listed on sanctions lists related to the development or proliferation of WMDs.

Aspro N.V. follows both local Curaçao regulations and global standards aimed at preventing proliferation financing, including:

- **Curaçao Regulations:** As a licensed casino operator in Curaçao, Aspro N.V. adheres to the regulations set forth by the Curaçao Gaming Control Board (GCB) and complies with the relevant national ordinances, including the National Ordinance Penalization of Money Laundering (NOPML) and the National Ordinance on the Reporting of Unusual Transactions (NORUT). These regulations require operators to implement strict anti-money laundering (AML) measures to detect and prevent illegal financing, including that related to WMD proliferation.
- **Financial Action Task Force (FATF):** Aspro N.V. follows FATF recommendations, which include guidelines for identifying and preventing the misuse of financial systems for proliferation financing. By adopting FATF's recommendations, the company ensures that its compliance program is in line with international best practices.
- **United Nations (UN) and European Union (EU) Sanctions:** Aspro N.V. adheres to sanctions lists and regulations issued by the UN, EU, and U.S. OFAC. These sanctions are critical in preventing financial resources from flowing into the hands of entities or individuals involved in the development of WMDs. The company carefully monitors transactions to ensure compliance with these global efforts to curb the proliferation of dangerous weapons.

Through its adherence to local Curaçao regulations and international standards, Aspro N.V. ensures that its operations are free from any involvement in the financing of weapons of mass destruction. By employing rigorous monitoring systems, conducting enhanced customer due diligence, and complying with global sanctions, the company actively contributes to global efforts to prevent the spread of WMDs and enhance international security.

ML & TF, PF RISK ASSESSMENT

Company applies a risk -based approach in combating exploitation of its online platform for the purposes of ML and TF & CPF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/TF/PF 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. Specifically, AML/CFT/CPF risk assessment categories center around the risks associated.

The range of products and services the Company offers

Online platforms may attract a global clientele, increasing the risk of transactions involving jurisdictions with weak AML controls. Factors that Company considering evaluating Product or Services Risk:

- The complexity of the product, service, or transaction
- The value or size of the product, service, or transaction
- Services provided through third-party providers or affiliates (e.g., payment processors, game providers) add an additional layer of risk.

Low to Medium Risk

- EEA countries.
- Third countries with effective mechanisms to combat money laundering and financing of terrorism.
- Third countries, which credible sources have identified as countries with a limited extent of corruption or other criminal activity.
- Third countries which, based on credible sources such as mutual evaluations, reports on detailed assessment or publicly available follow-up reports, have requirements to combat money laundering and financing of terrorism which are consistent with the FATF recommendations of 2012, and which implement these requirements in an efficient manner.

High to Ultra-High Risk

- Countries which do not have effective mechanisms to combat money laundering and financing of terrorism.
- Countries, which credible sources have identified as countries with a significant level of corruption or other criminal activity.
- Countries subject to sanctions, embargoes, or similar measures taken by, for example, the EU or UN; o Countries that finance or support terrorist activities, or which house known terrorist organizations.

Adherence to Curaçao's Updated Legislative Framework

Aspro N.V aligns its practices with the revised LOK framework, ensuring compliance with all AML/CTF/CPF requirements. The company's compliance program incorporates a robust risk-based approach tailored to its operational scope and complexity. Regular training sessions are provided to staff, ensuring that they understand their AML/CTF/CPF obligations and how to manage risks effectively. Independent audits are carried out periodically to assess the performance and effectiveness of the company's AML/CTF/CPF strategies and the application of the risk-based approach.

Aspro N.V recognizes the unique risks posed by the gambling sector, particularly in relation to money laundering and terrorist financing. The company identifies and mitigates customer risks by conducting comprehensive customer due diligence (CDD) and enhanced due diligence (EDD) for high-risk individuals. Key customer risk factors include irregular income sources, high spenders, and PEPs. Continuous monitoring and profile updates, along with stringent identity verification, are employed to mitigate these risks.

Customer Risk

The company evaluates customer risk by examining factors that could indicate a heightened likelihood of involvement in financial crime. This includes assessing the customer's financial behavior, the transparency of income sources, and potential affiliations with politically exposed persons (PEPs). Customers with multiple or opaque income streams, or those demonstrating inconsistent or high-volume financial activity that is not aligned with their declared profile, are considered higher risk and subjected to enhanced due diligence (EDD).

Clients who maintain multiple accounts or who exhibit spending patterns that significantly exceed their known financial means may attempt to obscure transaction trails, which complicates compliance efforts. Aspro N.V sets clear transaction thresholds based on typical user behavior to trigger investigative reviews. Low-risk customers generally have a single, documented source of income and a consistent transactional footprint, while higher-risk individuals are flagged for closer scrutiny, including more rigorous KYC documentation and monitoring protocols.

Product, Service, and Transactional Risk Exposure

Certain products and transaction types within the iGaming and digital services sector are more prone to misuse for illicit purposes. Services that allow rapid, high-volume transactions or offer anonymity—such as the use of cryptocurrencies or prepaid instruments—can be exploited to introduce, layer, and integrate proceeds from criminal activities into the legitimate financial system.

Examples of heightened product and transaction risks include:

- Use of gaming or wallet accounts primarily as pass-through mechanisms without active service usage.
- Peer-to-peer fund transfers that bypass conventional financial monitoring systems.
- Deposits or withdrawals made using third-party financial tools, including bank accounts or cards not registered to the account holder.

To counter these risks, Aspro N.V. monitors all platform-based transactions in real time and uses automated detection systems to flag atypical behavior. Where red flags are identified, the company initiates investigative protocols and applies EDD measures to assess potential threats.

Geographical Risk Considerations

Geographic risk is assessed by evaluating the customer's country of residence or the origin of their financial resources. Certain jurisdictions are associated with weak AML/CTF enforcement, high levels of public corruption, or a history of non-cooperation with international regulatory bodies. Engagement with clients or transactions linked to these jurisdictions poses an elevated compliance concern.

Aspro N.V. relies on guidance from internationally recognized bodies to evaluate and respond to geographic risks, including:

- FATF list of jurisdictions under increased monitoring or subject to countermeasures.
- Regional reports from the Caribbean Financial Action Task Force (CFATF).
- U.S. State Department International Narcotics Control Strategy Reports (INCSR).
- The European Commission's list of high-risk third countries.
- OFAC sanctions databases and the Transparency International Corruption Perceptions Index (CPI).

Based on these sources, the company categorizes countries into varying levels of risk. Clients from high-risk jurisdictions are subjected to strict onboarding controls and enhanced monitoring, while transactions involving sanctioned countries are blocked or escalated for additional review. Geographical risk profiles are revisited regularly to ensure the company's controls remain responsive to global developments.

Distribution Channel Risk and Authentication Controls

The methods through which Aspro N.V. establishes and manages customer relationships also influence its exposure to financial crime. Channels that permit remote or anonymous access, especially without sufficient verification layers, are inherently more susceptible to misuse. This is particularly relevant in digital environments where face-to-face interaction is absent.

To reduce this risk, the company employs secure identity verification protocols for all customers. These include biometric checks, multi-factor authentication, and identity validation tools that interface with global databases. By ensuring that access to services is tightly controlled and all interactions are traceable, Aspro N.V. maintains operational integrity and regulatory compliance.

Technological Developments Risk Assessment

Aspro N.V. recognizes that continuous technological evolution presents both opportunities and risks within the digital services and iGaming ecosystem. In line with its commitment to regulatory integrity, the company proactively safeguards its operations against the misuse of emerging technologies for illicit financial activities, including money laundering (ML) and terrorist financing (TF). A forward-looking risk management framework ensures that innovation does not come at the expense of security or regulatory compliance.

Risk Identification and Evaluation Procedures

To prevent the exploitation of new technologies, Aspro N.V. conducts structured and comprehensive risk assessments prior to the introduction of any digital tool, platform feature, or operational change. These assessments are essential in evaluating the potential for financial crime vulnerabilities and ensuring that regulatory obligations under AML/CTF/CPF regimes are met.

Risk assessments are systematically performed under the following circumstances:

- When launching a new product, feature, or service within the platform.

- When implementing new operational procedures designed to improve efficiency or enhance user engagement.
- When introducing new delivery mechanisms, including digital account access, mobile wallet integrations, or alternative payment solutions.
- When adopting or integrating innovative technologies such as blockchain applications, AI-driven tools, machine learning analytics, or enhanced cybersecurity protocols.

Each assessment involves a detailed analysis of potential risk vectors, with a focus on identifying how the technology may be misused to obscure the origin of funds, circumvent due diligence, or exploit system vulnerabilities. All findings are documented and retained to ensure traceability and transparency in line with domestic and international compliance standards.

Implementation of Mitigation Strategies

Where technological risks are identified, Aspro N.V takes immediate action to integrate targeted controls. These mitigation efforts are designed not only to prevent misuse but also to support continuous compliance with AML/CTF regulations in an evolving threat landscape.

Key mitigation measures include:

- **Strengthening security infrastructure**, such as deploying multi-factor authentication (MFA), biometric identification, advanced data encryption, and AI-based fraud detection technologies.
- **Enhancing monitoring capabilities**, ensuring that transaction surveillance systems can detect and escalate anomalies in real time—especially those reflecting structuring, layering, or uncharacteristic activity patterns.
- **Adapting compliance policies** to reflect the risks posed by digital transformation. The AML/CTF framework is updated regularly to account for emerging crime methodologies and to incorporate new risk indicators tied to technological abuse.

Commitment to Secure Innovation

Aspro N.V is committed to fostering innovation in a manner that reinforces—not undermines—its compliance posture. The company's approach to technological adoption emphasizes anticipation of risk, continuous system evaluation, and robust internal governance. Regular reviews of deployed technologies are conducted to reassess vulnerabilities and to adapt mitigation measures as necessary.

By incorporating these risk-based strategies into its AML/CTF/CPF policy, Aspro N.V effectively mitigates the risks associated with money laundering, terrorist financing, and proliferation financing. The company is committed to upholding Curaçao's regulatory standards while ensuring the integrity and security of the gaming sector.

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.

COMPLIANCE OFFICER

Compliance officer oversees the AML compliance program, i.e., actively manages money laundering, terrorist financing and proliferation financing risks. It is a crucial role which encompasses being authorized to communicate with the regulatory bodies, supervision of a team of internal 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, and maintaining a watchful eye over all due diligence and anti-fraud procedures with the view of conducting regular risk assessments. The Officer is also responsible for reporting suspicious activity, including suspicious transactions, to the FIU in Curacao.

Internally, the Compliance Officer is requested to report to the Board of Directors to keep the Board members informed of any recommended changes that may be required to manage the AML/CFT/CPF compliance program.

The compliance officer is assigned the following responsibilities (list is not exhaustive)

- To design and implement the AML program.
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing.
- To review compliance with the casino's policy and procedures.
- To organize training sessions for the staff on various compliance-related issues.
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions.
- To review all internally reported unusual transactions for their completeness and accuracy with other sources.
- To keep records of internally and externally reported unusual transactions.
- To execute closer investigation of unusual transactions if necessary.
- To prepare the external report of unusual transactions.
- To make necessary changes to the AML program.
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements.
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

The AML/CFT/CPF Officer acts independently always and his/her decision-making process is not impeded by the operational goals of the Company when investigating internal or external reports of suspicious activity.

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 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 customer risk's rating is deemed to be high due to presence of some behavioral or transactional triggers that point to a potential AML/CFT/CPF breach.

CUSTOMER DUE DILIGENCE GUIDELINES

The Company does not accept or maintain anonymous accounts under fictitious names. Aspro N.V. does identify each player/client, gathering its name and other relevant information to understand the purpose and nature of the business relationship. Without adequate knowledge of the customer, the Company does not establish nor maintain a business relationship, nor process occasional transactions. When establishing a business relationship with customers the Company identifies whether a customer 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. In the context of AML, customer due diligence process is a procedure which includes the identification of the potential customer, 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 behavioral and transactional patterns for any deviations that may be construed as a violation of AML/CFT/CPF legislation and policies. Research into the customers 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 customer data places such applications in a low-risk category, whereas Enhanced Due Diligence is applied to cases that require additional screening due to the system flagging certain data entries.

The integrity of the 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. Activities or type of players that may indicate a higher risk include the following categories:

1. Anonymous customers
2. Economic profile is inconsistent with the increase in gambling activity
3. Requests to withdraw winning via another payment method which differs from the one that was used for the original placement of the bet.
4. Attempts by the same individual to create multiple accounts
5. Drastic changes in the gambling pattern
6. High-value staking/ high transaction volume
7. Unusual requests that do not fall within the recommended guidelines such as to bypass KYC verification process etc.

Anti-Fraud team oversees operating a proprietary system which analyzes players' data based on the automatic checks performed through several third-party databases such as WorldCheck, Dow Jones and Lexis Nexis. In addition, manual checks are 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 Compliance Officer in writing through an internal suspicious activity report (SAR).

Customer Due Diligence is triggered in the following scenarios:

- When identifying the player and verifying that customer's identity using reliable, independent source documents, data or information.
- When identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner. For legal persons and legal arrangements, the Company seeks to understand the ownership and control structure of the customer.
- If suspicions are raised as regards the authenticity of the information and documents obtained during the onboarding process.
- If there is a suspicion of money laundering or terrorist financing as regards the customer's profile and activity.
- If there are any unauthorized changes detected as regards the player's profile.
- When transactions of NAF 4,000 or more appear CDD measures are applied to any single transaction that meets or exceeds this threshold.
- When occasional transactions exceeding NAF 4, 000 CDD measures are applied. This includes infrequent transactions that surpass the specified limit.
- When to either a single transaction or multiple transactions that collectively exceed NAF 4,000 appear CDD measures are applied. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD.
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

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.

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 customer gets terminated due to the failure to satisfy AML/ CFT legislative requirements and the funds are refunded back to the customer through the same payment channel and account used to deposit the funds.

Player Identity Establishment

To establish a player's identity, Company collects the following information:

- 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 reserves the right to terminate relationships with players engaged in suspicious activities or those who fail to provide sufficient information. Such decisions must be documented and approved by senior management. Upon termination, all activities will be reviewed, and any suspicious transactions will be reported to the FIU. Records related to terminated relationships will be securely stored for a minimum of five years.

Timing of Customer Due Diligence Measures

Aspro N.V applies Customer Due Diligence (CDD) measures in a timely and systematic manner, in line with its regulatory obligations under Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) frameworks. These procedures are designed to ensure that customer identification, verification, and risk assessment occur at the appropriate stages of the business relationship and in response to specific financial thresholds or behavioral indicators.

CDD Triggers Based on Transaction Thresholds

Upon account registration, the company collects the following minimum customer data:

- Full legal name
- Permanent residential address
- Date of birth
- Politically Exposed Person (PEP) status screening
- Sanctions screening against relevant domestic and international lists

As part of its risk-based methodology, Aspro N.V ensures that identity verification is completed before the execution of any transaction (or linked series of transactions) equal to or exceeding NAF 4,000.

This threshold-based verification applies to:

- A single transaction that reaches or surpasses the NAF 4,000 limit.
- Multiple linked transactions—including deposits, withdrawals, and peer-to-peer transfers—that cumulatively meet or exceed this value.

To ensure full regulatory compliance, the company monitors transaction activity on a daily rolling basis, calculating total exposure from the start of the customer relationship.

Once the NAF 4,000 threshold is triggered, Aspro N.V immediately conducts a full risk assessment and completes any outstanding due diligence requirements before allowing further financial activity.

Customer Acceptance Policy (CAP)

Aspro N.V. implements a formal **Customer Acceptance Policy (CAP)** to establish clear guidelines for the acceptance, onboarding, and continued engagement of customers, in alignment with its risk-based approach to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance obligations.

This policy defines **which customer types are acceptable, under what conditions** they may be onboarded, and **when service must be refused or terminated**.

Principles of Customer Acceptance

The acceptance of a customer must be based on:

- A clear understanding of the customer's identity, source of funds, and transactional behavior.
- Risk scoring and profile categorization (low, medium, high).
- Completion of required Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) based on risk level.
- Screening against sanctions, PEP, watchlists, and adverse media.

The Company reserves the right to reject or terminate any customer relationship that presents excessive risk or fails to meet verification standards.

Categories of Customers Not Accepted

Aspro N.V. does **not establish or maintain** business relationships with the following categories:

- Individuals providing false, forged, or unverifiable documentation.
- Persons under the age of 18 or otherwise considered minors.
- Individuals from jurisdictions subject to sanctions, embargoes, or identified by FATF as high-risk or non-cooperative.
- Politically Exposed Persons (PEPs), or their close associates/family, who are assessed to pose a high residual risk after EDD.
- Customers with known links to criminal activity, terrorism, or proliferation financing.
- Customers who refuse to complete KYC/CDD processes or are uncooperative.
- Persons using third-party payment methods not registered in their own name.
- Anonymous users or users attempting to bypass geo-blocking or IP detection systems.

Onboarding Thresholds and Risk Tiers

Customers are accepted based on a **tiered risk model**:

- **Tier 1 (Low Risk):** EEA residents with a single funding source and standard wagering behavior.
- **Tier 2 (Medium Risk):** Users with moderate transaction volume or from regions with partial AML risks.
- **Tier 3 (High Risk):** PEPs, offshore clients, cryptocurrency users, or customers with complex ownership structures. Require EDD and managerial approval.
- **Tier 4 (Unacceptable Risk):** Customers that fall under banned categories listed above.

The Compliance Team reviews all high-risk applications before activation.

4 Review and Approval

- All high-risk customer onboarding requires **pre-approval by the Compliance Officer or designated senior personnel**.
- The CAP is reviewed at least annually, or upon any regulatory change, and approved by the Board of Directors.

Termination Based on Risk Profile

If a customer's profile changes or exhibits high-risk behavior post-onboarding (e.g., unusual transactions, fraud indicators), the relationship may be suspended or terminated following internal review. All such cases are documented and, where appropriate, reported to the FIU.

ENHANCED DUE DILIGENCE

Enhanced Customer Due Diligence and Ongoing Monitoring are applicable to cases that receive a high-risk rating. Such examples may include doubts as to the authenticity of the documents, a high-risk third country location of the customer, a Politically Exposed Person (PEP) status of a potential customer, unusual behavioral patterns and therefore require additional investigations in the form of additional verification checks, adverse media screening or requests to provide additional documentation as regards the source of wealth, source of funds, utility bills, etc.

Company undertakes a list of Enhanced Due Diligence measures that may include:

- Obtaining additional information on the intended nature and purpose of the business relationship.
- Obtaining information of the source of funds or source of wealth of a customer.

- Obtaining additional information on the intended purpose of a transaction.
- Obtaining, and where appropriate verifying, additional information on the customer and beneficial owner.
- Searching the Internet for corroborating activity information consistent with the customer's transaction profile
- Obtaining, where possible, negative information about the customer and his/her business activities through adverse media searches.
- Increasing the frequency of reviews on a customer.
- Performing a credit search on a customer
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requesting data relating to transaction and trading history
- Request business documents, financial statements, or KYC documents to be certified or notarized by an independent third party (e.g. accountant or solicitor or public notary)
- Request a meeting in person with the customer or a video call to verify the customer's identity
- Corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources.
- Tracing the customer's IP address
- All high-risk customers are reviewed by the Compliance team prior to onboarding.

PEPs (Politically Exposed Persons)

A Politically Exposed Person (PEP) is defined by the FIU s 'Individuals entrusted with prominent public functions. The definition of a 'prominent public function' will vary according to the nature of the function held by a person. The Firm is required to understand the nature of each position held and whether the function gives rise to the risk of large-scale abuse of position.

The Politically Exposed Persons (PEPs) applications are handled by the senior management team whose approval is necessary to transact with such individuals and an internal register of such cases is kept by the Compliance officer office.

A PEP is an individual who recently held (in the last 12 months) 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.

If the Compliance Team identifies a PEP as a beneficial owner of a merchant entity, the Company will not automatically treat the legal entity as a PEP only because a PEP is a beneficial owner. However, the Compliance Team will apply a risk-based approach to the entity to assess the risk posed by the involvement of that PEP and, after making this risk assessment, the Company will apply appropriate measures in accordance with this procedure. These could range from applying Standard Due Diligence measures in cases where the PEP is just a figurehead for an organization (this will vary according to the circumstances of each entity but could be the case even if PEP sits on the board, including as a non-executive director). However, if it becomes apparent the PEP has significant control or the ability to use their own funds in relation to the entity, the Firm will apply Enhanced Due Diligence measures.

PEP Risk Factors and Assessment

PEPs may pose various levels of Money Laundering and Terrorist Financing risk dependent on strength of certain risk factors. The Company also considers a PEP, family member, or close associate.

The Compliance Team is required to manually handle this process and not rely on third-party service providers. The Team is required to diligently assess these risk factors for each identified PEP or known close associate or family member of a PEP. After doing so, they must determine if the PEP represents a high risk or a low risk, escalate it to Higher Manager for the final decision and this decision must be recorded in the customers' file.

Identification of PEP and Mitigation Measures

Compliance Team required to undertake certain measures when they identify and verify a proposed customer PEP, or family member, or known close associate of a PEP's status.

Upon verification of the PEP, or family member or known close associate of a PEP's status. The following measures should be applied:

- Obtain sign-off, as a minimum, from Higher Management before proceeding with the relationship.

- Take “adequate measures” to establish the customer’s source of wealth and source of funds relevant to the proposed business relationship or transaction.
 - Conducted enhanced ongoing monitoring of the business relationship.
 - Review PEPs on an annual basis to ensure information is still accurate and up to date
- PEP due diligence measures

If the Firm determines that a PEP represents an elevated risk of Money Laundering and Terrorist Financing, Compliance Team conducts EDD measures on them. EDD measures that the Company’s employees may apply to high-risk PEPs include:

- Immediate escalation to the Higher Management for review, the decision whether the business relationship should be established.
- If Higher Management will determine if the risks posed by a PEP are higher than the Company can effectively mitigate, the Company will not enter into or continue a business relationship with a PEP.
- Examine whether the Company knows a PEP face-to-face.
- Intrusive steps to establish the source of wealth and funds
- Examine nature of the proposed business relationship with a PEP.
- The potential for the Company’s products and services to be misused for the purposes of corruption.
- Undertake frequent and thorough monitoring of the relationship to ascertain whether it should be maintained.
- Reference public domain information such as websites of parliaments and governments, reliable news sources, and work by reputable pressure groups focused on corruption risks such as Transparency International or Global Witness to understand the nature of position PEP holds

ONGOING MONITORING

The Firm conducts ongoing monitoring on two levels:

1. Account monitoring
2. Transaction monitoring

The Company conducts manual review of fiat activities and a retrospective analysis of customer behavior. It considers previous checks and data related to the customer. It allocates a specific risk rate, and all high-risk customers are regularly reviewed.

Risk score is assigned to each transaction, based on the following information:

- Higher than average Transaction Value:

The total historical transactional average of a customer will be assessed. Where a transaction exceeds the customer's typical behaviors, these transactions will receive additional weighting.

Activities in a customer's account are being monitored as well analyzing Deposit/withdrawals trends. The Company subjects all accounts for review on a regular basis to determine if account activities are in keeping with the customer's standard and ongoing profile.

When conducting deposit monitoring Company analyze the following:

- The customer profile and risk score history
- Due diligence documents
- The customer incoming funds history
- All transactions made by the customer since the beginning of the relationship such as deposits, betting, losses and winnings
- Number of accounts held by the customer and their transaction history

Termination of Business Relationships

Aspro N.V upholds a strict and transparent procedure for terminating customer relationships that pose an elevated risk of financial crime or fail to meet Customer Due Diligence (CDD) obligations. These measures ensure ongoing compliance with applicable AML, CTF, and CPF regulations while protecting the integrity of the platform.

Grounds for Termination

The company may terminate a customer relationship under the following conditions:
The individual is found to be engaging in activity suggestive of money laundering (ML), terrorist financing (TF), or other suspicious financial behavior.

The customer fails to provide the required CDD documentation or refuses to cooperate with verification procedures within a specified timeframe.

The individual is assessed as posing a high ML/TF risk based on updated risk profiling, behavioral indicators, or jurisdictional exposure.

Termination Procedure

Aspro N.V follows a controlled and documented process when discontinuing a business relationship:

Senior management reviews and formally approves all termination decisions. A final risk-based review of the customer's account activity is conducted prior to closure.

If the review identifies unusual or potentially illicit transactions, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU).

All customer records, including identification details and transactional history, are securely retained for at least five years in accordance with legal and regulatory requirements.

Third-Party Reliance for Customer Due Diligence

Aspro N.V may utilize third-party service providers to perform specific components of its Customer Due Diligence (CDD) obligations. However, such reliance is governed by a strict regulatory framework to ensure that all processes remain fully aligned with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. Regardless of any delegation, the company retains full accountability for the proper execution of CDD measures and overall compliance outcomes.

Oversight and Accountability

To ensure transparency and regulatory integrity in third-party collaborations, Aspro N.V enforces the following controls:

- Formal written agreements are established with all CDD service providers, clearly defining their duties, compliance standards, and data-sharing obligations.
- The company guarantees immediate access to all customer identification records collected by third parties when required.
- Periodic audits and performance reviews are conducted to verify adherence to AML/CTF/CPF protocols.
- Despite any delegation, Aspro N.V independently determines key compliance factors, such as:

The customer's Politically Exposed Person (PEP) status

Ongoing risk classification and updates

Transaction monitoring and red flag detection

Conditions for Acceptable Third-Party Reliance

To qualify for CDD reliance, the third-party entity must meet specific regulatory standards:

- Must be a regulated institution, supervised under a recognized AML/CFT/CPF legal regime.

- Must maintain an independent business relationship with the customer (i.e., not acting solely as an intermediary for Aspro N.V).
- Must operate in a jurisdiction with equivalent AML/CTF/CPF standards, subject to favorable evaluation through the company's jurisdictional risk assessment process.

Aspro N.V. evaluates third-party jurisdictions using internationally recognized intelligence sources, such as FATF mutual evaluations and global AML risk indices, to ensure that outsourcing does not introduce compliance vulnerabilities.

Outsourcing vs. Third-Party Reliance: Key Distinction

Aspro N.V. recognizes the difference between outsourcing and third-party reliance:

- In third-party reliance, the external party conducts specific CDD tasks independently, but the regulatory liability remains with Aspro N.V.
- In outsourcing arrangements, the third party acts under the company's direct instructions, adhering strictly to internal procedures and controls.

Regardless of the structure, Aspro N.V. maintains full oversight and control over customer risk assessments, onboarding decisions, and relationship management.

SANCTIONS MANAGEMENT, FATF BLACKLIST, LICENSE RESTRICTIONS

• License Restrictions:

Aspro N.V. operates under the Curacao online gaming license and is therefore banned from offering its online services in Aruba, Bonaire, Curacao, France, the Netherlands, Saba, Statia, St. Maarten, Singapore and the USA. It does not operate in countries where there is a total ban on gambling such as China, Turkey, Brunei, Cambodia, Japan, Qatar, Lebanon, Poland inter alia or where the Company is required to obtain a local gambling license in order to operate locally (USA, UK, EU countries for instance).

• Sanctions Management:

In light of the fact that the Curacao belongs to the Dutch Caribbean, under article 1(1) of the Kingdom Sanctions Law (Rijkssanctiewet) provisions of binding EU legal acts are effective from the date of their entry into force in Curaçao in the same way as in the Member States of the European Union. Consequently, the Regulations are also directly implemented in Curacao.

The Company, being a Curacao-based entity which transacts with the EU and the EU-based payment partners, complies with the following regional sanctions lists:

European Union Sanctions List: [EU Sanctions Website](#)

UK Sanctions List (OFSI): [UK Sanctions Search](#)

UK Consolidated Sanctions List: [Gov.uk Sanctions Collection](#)

United Nations Security Council Consolidated List: [UN Consolidated List](#)

U.S. State Department List of Foreign Terrorist Organizations: [State.gov FTO List](#)

U.S. Department of Treasury OFAC SDN List: [OFAC Sanctions Search](#)

- **FATF blacklist:**

The Company's primary goal in this regard is to prevent making payments to designated persons and sanctioned entities and/or serve customers from FATF black-listed countries such as Democratic People's Republic of Korea, Iran, Sudan and and countries that are on the State Sponsors of Terrorism list by the U.S. Department of State i.e. Cuba, North Korea, Iran and Syria (<https://www.state.gov/state-sponsors-of-terrorism/>). In unlikely circumstances where a payee or a customer are identified as a designated person, payments will not be processed and an internal SAR/STR report will be submitted to the Compliance officer office for further regulatory processing if necessary.

Aspro N.V. ensures that all customers, counterparties, and transactions are screened against updated sanctions lists on an ongoing basis, using automated screening tools. Upon identification of a potential or confirmed match, the account is immediately **frozen**, and all transactions are **halted** pending internal investigation and potential reporting to the Financial Intelligence Unit (FIU).

The **Compliance Officer** is responsible for reviewing all sanctions alerts. Confirmed designations result in **asset blocking** and the filing of a **Suspicious Transaction Report (STR)**.

Third-party payment processors and affiliated service providers are contractually required to conduct sanctions screening and block transactions involving designated individuals or jurisdictions.

Sanctions procedures are tested quarterly, and screening databases are updated daily to ensure full regulatory compliance.

RECORD-KEEPING

The Company is maintaining all necessary records related to transactions (both domestic and international) for a minimum of five years to ensure compliance with information requests from competent authorities. All records are detailed enough to allow for the reconstruction of individual transactions (including amounts and types of currency involved, if applicable), to provide, when necessary, evidence for the prosecution of criminal activity. Additionally, all records obtained through Customer Due Diligence (CDD) measures, such as copies or records of official identification documents (e.g., passports, identity cards, driving licenses, or similar), account files, and business correspondence, are retained for at least five years following the termination of the business relationship or the date of an occasional transaction. CDD information and transaction records are readily accessible to domestic competent authorities upon proper legal request.

The company adheres to rigorous record-keeping practices to ensure compliance with AML/CTF/CPF regulations. We prioritize maintaining secure, accurate, and accessible documentation to support regulatory compliance, internal audits, and the integrity of the gaming industry.

To meet legal requirements, the company retains key documentation for a minimum of five years. These records include all customer identification details collected during the onboarding process, transaction data, suspicious activity reports (SARs) submitted to the Financial Intelligence Unit (FIU), training records for employees, and audit logs. These documents are critical for demonstrating compliance with the company's AML/CTF/CPF procedures and for assisting in any potential regulatory review or investigation.

SUSPICIOUS ACTIVITY REPORTING

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. 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 (National Ordinance on the Reporting of Unusual Transactions) it is an internet gambling entity's duty to report unusual transactions (A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.) 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/CPF

reporting obligations and then determines whether the business relationship with the suspected customer should be paused or terminated.

Aspro N.V maintains a proactive and structured approach to identifying and reporting suspicious activity that may indicate money laundering (ML), terrorist financing (TF), or proliferation financing (PF). This includes behavioral anomalies, significant or unexplained financial movements, and any interaction involving jurisdictions or individuals known to present elevated risk.

All employees are required to remain vigilant and immediately escalate any concerns to the appointed Compliance Officer. Once notified, the Compliance Officer performs a detailed assessment to determine whether further internal action or an external report to the appropriate authority is necessary.

Identifying Unusual Transactions

Transactions are considered unusual if they significantly deviate from a customer's typical financial behavior or profile. Common red flags include:

- Large, unexpected transactions that are inconsistent with known income or gambling activity
- Transfers involving unidentified third parties or high-risk jurisdictions
- Financial operations that lack a lawful or logical purpose

Monitoring tools are used to flag these transactions automatically, with each flagged case escalated to the Compliance Officer for deeper investigation.

Categories of Transactions Warranting Review

In accordance with Curaçao's AML/CTF regulatory framework, Aspro N.V treats the following types of transactions as unusual and subject to further scrutiny:

- Previously reported transactions: Any transaction already submitted to law enforcement or regulatory bodies due to ML/TF suspicion is immediately categorized as unusual.
- Transactions with sanctioned individuals or entities: Dealings involving any party listed under the Sanctions National Ordinance (N.G. 2014 no. 55) are automatically escalated for further review.
- Transactions at or above NAF 5,000: This applies regardless of payment method—whether via cash, check, electronic transfer, or other digital means. Examples include:
 - Deposits or withdrawals meeting or exceeding the threshold
 - Purchases of gaming tokens, credits, or chips above NAF 5,000
 - Payouts or redemptions reaching this benchmark

Note: Transactions may be considered collectively if they form part of a linked pattern or series that meets or exceeds the NAF 5,000 threshold in a single gaming day.

Presumptive Suspicion and Escalation

If a transaction shows signs indicative of money laundering or terrorist financing—even without conclusive proof—it must be treated as suspicious and documented accordingly. The Compliance Officer then evaluates whether it meets the criteria for submission to the Financial Intelligence Unit (FIU).

Maintaining Confidentiality

To safeguard the integrity of the investigation and comply with legal standards, Aspro N.V enforces strict confidentiality in all matters related to suspicious activity reporting (SAR). Employees are explicitly prohibited from:

- Disclosing SAR-related information to the customer(s) involved
- Discussing the matter with unauthorized colleagues or external parties

Access to SAR documentation and discussions is restricted solely to the Compliance Officer and designated compliance personnel. All employees receive training to reinforce the importance of confidentiality, particularly regarding the risks of “tipping off” and the consequences of non-compliance.

Violations of this policy are treated as serious disciplinary offenses and may lead to termination of employment or other corrective measures.

By cultivating a culture of alertness and discretion, Aspro N.V reinforces its commitment to regulatory compliance, protects the integrity of its operations, and plays an active role in detecting and disrupting financial crime.

UNUSUAL TRANSACTIONS

An unusual transaction is identified as any transaction that deviates from the expected behavior based on the player's profile. The foundational step in recognizing such transactions is to ensure sufficient knowledge about the player. In compliance with the NORUT legislation, the company has established objective and subjective indicators to assess whether a customer's transaction should be classified as unusual. Management is responsible for ensuring that all staff members receive specific training and clear guidance on recognizing and properly documenting such transactions. All unusual transactions must be reported to the compliance officer.

To report unusual transactions to the Financial Intelligence Unit (FIU) of Curaçao Company must through the goAML portal

https://portal.fiucuracao.cw/goAMLWeb_PRD/Home prior obtaining credentials from FIU. After a report is submitted, a confirmation of receipt will be issued by FIU Curaçao.

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.

EMPLOYEE TRAINING

The Company requires all relevant employees to complete AML/CFT/CPF training covering their area of responsibility at least annually. The focus of the training programs is to make sure that the employees follow the right protocols to verify customer information and can identify suspicious activity both internally and externally. The employees are made aware regularly of their legal obligations to report suspected breaches to their senior manager and who then contacts the Compliance officer office to discuss the internally submitted SAR/STR report as any acts of collusion, manipulating records or bypassing KYC protocols will result in committing a criminal offense for which they will be tried if caught.

The doctrine "wilful blindness" is a recurring theme of the internal training programs due to its massive legal implications for the employees who may have deliberately avoided "the knowledge of the facts" and therefore exposed themselves to being criminally liable for the ML/FT offenses. Furthermore, The Company implements the Know Your Employee (KYE) policy which centers around initiatives which help acquire a better knowledge of the employees' character and behavioral patterns after they successfully passed a background check to be able to detect conflicts of interests or suspicious activity occurring in the workplace.

All personnel, whose duties include the handling of Clients' business, are to be adequately trained with respect to the procedures and the provisions of the Prevention of Money Laundering Act.

The level of training provided to individuals is to be appropriate to their role and seniority within the Company. In any case all Employees must have the proper training on ML/TF prevention prior to the commencement of their duties at the Company which involve the ML/TF risk.

Compliance officer prepares and implements, on an annual basis (or whenever deemed necessary), an educational training program (training plan) for staff depending on the needs of the Company regarding the prevention of using the financial system for money laundering or other illicit purpose, including preventive developments and practical methods and trends used.

Compliance officer shall evaluate the adequacy of the seminars, and the training provided to the staff and maintains detailed data regarding the seminars/ programs carried out, such as:

- contents of the training
- the date, title and duration of the seminar and the names of the trainers,
- names of employees participating in the seminar/training by branch/department and by position (management staff, officers, newcomers etc.),
- the persons who were unable to attend the training accompanied with the reason for non- attendance
- whether the lecture/seminar was organized internally or offered by an external agency or consultants.
- An ongoing training plan.

AUDIT FUNCTION

To comply with Curaçao's updated gaming regulations, Company performs an independent audit focusing on Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) procedures and appoints an independent auditor, either external or an internal team with AML expertise, who must be approved by the Gaming Control Board to prevent conflicts of interest. The audit follows both international standards and specific requirements from the Gaming Control Board, examining policies, risk management effectiveness, transaction monitoring systems, staff training adequacy, reporting mechanisms, and compliance with KYC (Know Your Customer), KYB (Know Your Business), and Customer Due Diligence (CDD) protocols.

After completion, the auditor submits a report detailing findings and recommendations to Company's senior management and the Gaming Control Board, with the company committed to implementing any necessary corrective actions. The Gaming Control Board maintains oversight of the audit process and can request additional documentation or perform inspections as needed to verify compliance. The Company acknowledges that non-compliance identified through audits or Board evaluations could lead to penalties, including fines, operational restrictions, or even suspension or revocation of its gaming license, underscoring its commitment to full cooperation with the Gaming Control Board in implementing corrective actions and maintaining compliance.

Audit Process and Evaluation

The audit process follows both international standards and specific requirements set by the Gaming Control Board. Key steps include:

1. **Evaluation of Policies and Procedures:** Ensuring that the company's AML/CTF/CPF policies are updated and fully compliant with current legal requirements.
2. **Risk Management Assessment:** Reviewing how risks are identified and mitigated, and ensuring effective risk management strategies are in place.
3. **Transaction Monitoring Review:** Assessing the effectiveness of systems used to detect suspicious transactions and ensuring proper reporting.
4. **Staff Training Evaluation:** Verifying that training programs meet regulatory standards and that employees are properly equipped to detect and report suspicious activities.
5. **Reporting Mechanism Audit:** Checking how suspicious transactions and compliance issues are reported, ensuring that all processes are streamlined and accurate.

6. Customer File Review: Auditing the KYC, KYB, and CDD protocols to ensure that customer identification and risk assessment procedures are followed.

Audit Report and Findings

After the audit, the independent auditor provides a detailed report to the company's senior management and the Gaming Control Board. This report outlines the findings, recommendations, and any issues identified during the audit. Aspro N.V will act on the auditor's recommendations, implementing corrective actions within an established timeframe.

Gaming Control Board's Role

The Gaming Control Board, which oversees AML/CTF/CPF compliance for all licensed operators, reviews the audit results to ensure that the company is in full compliance. The Board may:

- Review the Audit Report: Analyzing the auditor's findings to assess compliance and highlight any concerns.
- Conduct Onsite Inspections: Verifying audit findings through visits to the company's premises to evaluate the effectiveness of corrective actions.
- Perform Interviews and Documentation Analysis: Interviewing relevant staff and reviewing supporting documents to better understand the company's AML/CTF/CPF practices.