

Bellona N.V.

V 1.0

**Manual for the combating
Money Laundering, Financing of
Terrorism and Proliferation of weapons
and mass destruction**

Content

I.	INTRODUCTION	2
A.	KEY RESPONSIBILITIES	4
B.	TARGETED FINANCIAL SANCTIONS	5
C.	DEALING WITH SANCTIONED PERSONS	6
D.	PROCEDURES	7
II.	RISK ASSESSMENT	7
A.	POLITICALLY EXPOSED PERSONS AND SANCTIONS	7
B.	GEOGRAPHIC RISK	9
C.	PAYMENT RISK AND THRESHOLDS	9
D.	NATURE AND FREQUENCY OF TRANSACTIONS	9
E.	SOURCE OF FUNDS BEING TRANSACTED	10
F.	PLAYER RISK MATRIX	10
III.	POLICY AND PROCEDURES	12
A.	IDENTIFICATION	12
B.	ANONYMOUS ACCOUNTS	12
C.	EVIDENCE OF IDENTITY FOR PARTICIPANTS	13
D.	ENHANCED DUE DILIGENCE	15
E.	SOURCE OF FUNDS AND WEALTH	16
F.	KYC MATRIX	17
IV.	ONGOING MONITORING	18
A.	ONGOING MONITORING OF TRANSACTIONS	18
B.	ONGOING MONITORING OF IDENTITY	19
V.	RECORDKEEPING	19
VI.	REPORTING OF AN UNUSUAL/SUSPICIOUS TRANSACTION	20
A.	FILING A STR	20
B.	HANDLING AND MAINTENANCE OF STR RECORDS	21
C.	INTERNAL REPORTING	21
D.	CONFIDENTIALITY AND TIPPING OFF	21
VII.	STAFF EDUCATION, TRAINING, AND DEVELOPMENT	22
A.	OVERVIEW	22
B.	TRAINING CONTENT	22
C.	RECRUITMENT AND EMPLOYEE SCREENING	23
D.	INTEGRITY	24
E.	INTERNAL CONTROL	24
F.	TECHNOLOGICAL DEVELOPMENTS	25
	VERSION CONTROL	25
	APPENDIX A INTERNAL SUSPICIOUS ACTIVITY REPORTING FORM	26

I. Introduction

The aim of this manual is to set out the policies, procedures, systems and controls necessary to meet the obligations of the Company that operates from Curaçao and is held to compliance with National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT).

With the publication of the National Decree supervisor identification when rendering services gaming sector and the National Decree supervisor unusual transactions gaming, the Curaçao Gaming Control Board (GCB) is tasked with the Anti-Money Laundering (AML)/ Countering Financing of Terrorism (CFT)/ Countering Financing of Proliferation (CFP) of Weapons of Mass Destruction supervision of the gaming sector operating in and from Curaçao.

The procedures that are appropriate for the purpose of forestalling and prevention of money laundering include:

- Identification
- Record keeping
- Staff education, training and development
- Internal procedures including the reporting of suspicious transactions, both internal and external

It is the Company's policy that NOIS and NORUT obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

The Company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Curaçao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curaçao authorities and in accordance with Curaçao custom and practice to avoid any risk of the Company committing a tipping-off offence.

The Company's policies and procedures are based upon the regulations referred below and associated guidance issued by the Curaçao Gaming Control Board.

The laws and Regulations are form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);

- National decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the sanctions National Ordinance, containing implementation of the United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation article 2 of the Sanctions National Decree containing implementation of the of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods like those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary

instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

What is Financing of Proliferation of weapons?

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

A. Key responsibilities

The Company's management is responsible for:

- The day-to-day compliance with AML/CFT/CFP obligations within the areas of the Company for which they are responsible.
- Ensuring that the MLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO and AML/CFT/CFP Compliance Officer with the appropriate resources to fulfil their functions effectively.
- Ensuring that the MLRO has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.
- The Directors and MLRO will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.

MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the Company to all external agencies and any other third- party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.

AML/CFT/CFP Compliance Officer is responsible for:

- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT/CFP legislation.

- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT/CFP including updates to any legislation or regulatory guidance.
 - Any updates to the Company's internal AML/CFT/CFP procedures and policies.
 - Any activities relating to compliance with the NOIS and NORUT.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO all knowledge or suspicions of money laundering.
- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

B. Targeted Financial Sanctions

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take form of economic, trade, financial services, or international movement (travel bans) prohibitions. Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities, and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

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

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar

currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them. The OFAC Sanctions List Search is available at the following link: <https://sanctionsscarch.ofac.trcas.gov/>

OFSI Sanctions

The Office of Financial Sanctions Implementation (OFSI), part of HM Treasury in the United Kingdom, is responsible for implementing and enforcing financial sanctions in the UK. These sanctions are derived from the UK government's own regimes as well as those adopted from the United Nations. UK financial sanctions may apply to individuals, entities, or countries and can include asset freezes, restrictions on financial markets and services, and directions to cease financial activity. All persons within or doing business in the UK must comply with OFSI sanctions. Suspected matches to the UK sanctions list must be reported to OFSI. The UK Sanctions List and related information can be accessed at the following link: <https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>; The UK also maintains a consolidated list of all designated persons: <https://www.gov.uk/government/publications/the-uk-sanctions-list>

ASO-DFAT Sanctions

Australia's sanctions framework is administered by the Australian Sanctions Office (ASO) within the Department of Foreign Affairs and Trade (DFAT). Australia implements two types of sanctions - UN sanctions (as required under international law), and Autonomous sanctions, which are determined independently by Australia to pursue its foreign policy and national security interests. Australian sanctions can target countries, individuals, and entities and typically include restrictions such as asset freezes, travel bans, and prohibitions on providing financial services or goods. It is a criminal offence under Australian law to breach sanctions. The Consolidated List maintained by DFAT includes all persons and entities subject to targeted financial sanctions and travel bans: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-list>

C. Dealing with sanctioned persons

In case when the Employee during Client on-boarding, CDD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and/or entities, he MUST:

- Immediately freeze all the funds / economic resources of the Client available to the Company;
- Not enter into any financial transactions or provide financial assistance or services to the Client;
- Apply Enhanced Due Diligence measures;
- Immediately inform and file the internal report to the MLRO;
- Suspend the account of the Client until further instructions from the MLRO.

It is prohibited to inform the Client or any third party (except a senior manager or MLRO) in advance, that a freezing measure is to be applied.

The MLRO has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU, UN or national Sanctions regimes, the MLRO will cease to conduct any further business and a report will be submitted to the FIU.

D. Procedures

- All persons conducting business with the Company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the Company to 'know its client' and predict the expected pattern of business.
- Potential new business partners that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Money Laundering Reporting Officer (MLRO).
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation.
- All suspicions are reported promptly to the MLRO.
- That the Company's vigilance systems are implemented and regularly monitored.

II. Risk Assessment

Based on the FATF Recommendations, casinos are required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. As part of the companies regulated approach to AML/CFT/CFP risk the following assessment has been conducted to adopt a risk-based approach to compliance with customer due diligence, both at the point of registration and in relation to on-going monitoring of clients.

A. Politically Exposed Persons and Sanctions

A Politically Exposed Person (PEP) is a person in an influential and prominent political position operating within a domestic or foreign capacity. In their role as senior government officials, they have access to resources and power that can influence government, policy, and people. The more senior the role a person holds in government, the more exposure that person has to the people and resources that can influence or corrupt the laws that govern financial actions. Those that are politically exposed are more likely to have the opportunity to manipulate and misuse the financial system for illicit gain and personal advantage.

To identify whether a customer, prospect or associate is a PEP, the Anti-Fraud team conducts a screening of all new members (registered during the last 24 hours) once per day. The screening is achieved through a number of methods ranging from individual searches using a web-based interface or batch screening entire databases, including but not limited to: (i) keyword searches for adverse media and PEP hits in public search engines (e.g., Google) and trusted international and local (to the user) news databases using the player's full name, date of birth, and country of residence and other available details; (ii) checks against government or international organization websites (e.g., relevant Parliament directories, UN resources); (iii) checks against lists and bulletins from regulatory bodies and enforcement agencies like the ASO-DFAT, OFSI, OFAC, INTERPOL, UN, or EU sanctions. The status of a politically exposed person can change overnight; therefore the

Company also revisits PEP status checks for existing users as part of the scheduled and ad hoc due diligence reviews on an ongoing basis to mitigate risk.

These screenings may or may not necessitate additional action, depending on their outcome: (i) If no matches are found the onboarding process/ongoing account activity may proceed as normal; (ii) if the matches found are partial and/or not related to financial activity, ML, TF, or significant political activity (e.g. the user is a low-level municipal clerk with no criminality, but minor delinquency) the findings are presented with priority to the MLRO/senior management for further guidance and investigation; (iii) if PEP/ML/FT/FP/Adverse media hits are found, the account is suspended and the case forwarded with priority to the MLRO/senior management for a decision on whether the relationship with the user should be terminated or if additional due diligence/other actions should be undertaken.

Bellona N.V. has made the decision to not accept PEPs as customers, as they fall outside the Company's risk appetite.

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;
- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State-owned enterprise;
- A senior official of an international entity or organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;

- A person in a position to conduct substantial financial transactions on behalf of a PEP.

B. Geographic Risk

Customers who are suspected to be located in, are found to have significant interests/connections to or otherwise attempt to access the service from Afghanistan, Belarus, Burma/Myanmar, Burundi, Central African Republic, China, Côte d'Ivoire, Democratic Republic of Congo, Eritrea, Guinea, Guinea-Bissau, Haiti, Iran, Iraq, Lebanon, Liberia, Libya, North Korea, Russia, Sierra Leone, Somalia, South Sudan, Sudan, Syria, Tunisia, Ukraine, Yemen, Zimbabwe or generally - jurisdictions subject to relevant international sanctions (e.g., UN, OFAC, OFSI, EU, ASO-DFAT) or identified by the FATF as blacklisted/non-cooperative are not eligible for onboarding and are prohibited from using the service. These jurisdictions are excluded from our platform in accordance with regulatory compliance and risk management policies and recommendations.

C. Payment Risk and Thresholds

To ensure compliance with applicable AML/CFT/CFP regulations, the Company applies risk-based thresholds to customer financial activity. These thresholds are designed to elicit appropriate due diligence measures based on transaction size, frequency, and customer behavior.

Events which necessitate a review and the application of Customer or Enhanced Due Diligence measures, as appropriate:

- A single deposit or withdrawal equal to or exceeding EUR 2,000 (or the currency equivalent);
- Aggregate deposits exceeding EUR 2,000 within any rolling 30-day period;
- A suspicion of money laundering or terrorist financing or similar illicit activity; or
- Doubts regarding the accuracy or adequacy of previously obtained customer identification data

The following maximum thresholds and controls for transaction management are established:

- Maximum amount per deposit before requiring Source of Funds (SoF) documentation: EUR 2,000 (or equivalent);
- Maximum cumulative deposits allowed without Source of Funds documentation: Below EUR 2,000 over a rolling 30-day period;
- Maximum singular deposit permitted: EUR 5,000 (or equivalent);
- Enhanced Due Diligence (EDD) threshold: Any individual or cumulative deposit exceeding EUR 5,000 (or equivalent).

When a customer reaches the threshold, the transaction that they are attempting (either a deposit or withdrawal) will not be permitted until they have satisfied their customer or enhanced due diligence requirements accordingly.

D. Nature and frequency of transactions

Regular customer transactions—such as consistent deposits and betting activity using a single payment method—are generally considered low risk. The Company's risk assessment framework places these users in the low risk category when they lack apparent connections to problematic

jurisdictions, they provide valid identification, and exhibit stable financial behavior. In contrast, irregular activity, such as frequent changes in payment methods, large or rapid transactions, or use of tools intended to mask the user's true identity or location (e.g., VPNs), elevates a customer's risk level and may trigger investigation or enhanced due diligence checks.

Transactions and account behaviors are monitored continuously through the company's internal systems, including checks on IP addresses, cookies, and payment method similarities to detect anomalies, fraud, or potential multi-accounting. When unusual behavior is detected, it prompts a deeper review, potentially escalating the customer's risk classification or resulting in account suspension pending further verification.

The Company's procedures aim not only to identify and verify customers during onboarding but also to monitor ongoing activities for shifts in risk profile. If there is a substantial change in behavior or transactional pattern, further checks are initiated, including verification of source of wealth and identity documentation.

Customers attempting to manage their activity to avoid qualifying thresholds, especially through structuring smaller transactions or switching payment methods, are subject to enhanced scrutiny. Where deemed necessary, the Compliance Officer/MLRO will be engaged for further review or suspension of services.

E. Source of funds being transacted

The legitimacy and ownership of customer funds must be established and traceable. The Company mandates that all withdrawals must be made back to the original deposit method. If this is not feasible (e.g., bank account closure), the customer must provide documentation showing that they are the legitimate owner of the new payment method.

Frequent changes in payment sources are subject to a further detailed review. Supporting documents such as employment contracts, bank statements, or employer letters may be requested to verify the source of funds or wealth. If a customer fails to satisfactorily justify the origin or ownership of funds, their account may be suspended indefinitely, and a Suspicious Transaction Report (STR) filed with the relevant authorities.

All such investigations and documentation are securely stored in read-only format and maintained for at least five years in accordance with regulatory requirements.

F. Player Risk Matrix

Risk rating	Nature	Location	Source of funds/ Wealth	Transaction size
Prohibited	Entity (i.e – not a natural person)	Closed jurisdictions	Undetermined, unverifiable or supposedly cash	A customer that has breached any of the below thresholds but does not
	Sanctioned individual	A customer that has triggered any of the below qualifiers to become high or medium risk but	A customer that has triggered any of the below qualifiers to	comply with the Company's CDD/ EDD requirements

	A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements Anyone deemed to be linked with the financing of terrorism Business participant PEP	does not comply with the Company's CDD/ EDD requirements Named on FATF's Blacklist or otherwise heavily sanctioned jurisdictions	become high or medium risk but does not comply with the Company's CDD/EDD requirements Funds appear to be generated or linked to the proceeds of crime	
High	Any individual subject to warnings Suspected professional gambler Customers that are suspected sporting professionals betting on sports High net worth individuals	Generally cooperative countries with some AML/CFT/CFP strategic difficulties, under increased FATF monitoring	Attempts at using over 5 different payment methods Inconsistent transaction velocity and volume patterns	Cumulative deposit of EUR 10,000 in any period
Medium	Public profile raises some minor form of concern e.g. adverse media, social media activity	Countries which in the opinion of the MLRO represents heightened risk	Use of voucher or pre-paid card Attempts of withdrawal to a method which differs from that of original deposit Use of over 3 different payment methods	Single instance deposit or withdrawal of over EUR 2,000 (or currency equivalent) or cumulative deposit of more than EUR 2,000 (or currency equivalent) in any 30-day period
Low	Regular Individual	Fully compliant with FATF No AML/CFT/CFP concerns	Single payment method used	Under any of the qualifying payment thresholds

Following the risk assessment, customers will be identified as either low, medium, high or will not be able to open an account. The relevant level of customer due diligence will then be applied to each participant's account and reviewed on an on-going basis as part of the monitoring procedure.

The Company will undertake a review of the relevance of its risk assessment as part of the AML/CFT/CFP Compliance Officer's annual report to senior management or as and when significant changes in business operations dictate.

III. Policy and Procedures

A. Identification

In accordance with regulatory obligations, the Company conducts identity verification (Customer Due Diligence or CDD) upon withdrawal attempt or when financial transactions equal to or exceeding EUR 2,000 are performed. However, CDD procedures begin at the point of registration, where the customer must provide essential personal information including:

- Full name;
- Country of residence and full address;
- Date of birth;
- Phone number;
- Email address;

The system automatically rejects registrations where the customer is under the legal minimum age of 18. Age is validated during the registration process, and any attempt to register with an invalid birthdate will result in the denial of access.

Upon completion of the registration form and agreement to the Terms of Use, the customer receives an email to the address provided. To activate the account, the customer must follow the verification link and re-log into the platform. Only after account activation can financial transactions be performed—no deposits or bonuses are permitted before this stage.

The Company maintains a complete log of all registration attempts, successful registrations, and inactive or failed attempts as part of its ongoing monitoring and compliance procedures.

B. Anonymous Accounts

The Company does not allow the creation of anonymous, fictitious, or duplicate accounts. During registration, all submitted details are screened by automated systems, which include checks for:

- Identical or suspicious personal information;
- Matching IP addresses or device identifiers;
- Payment method duplication;
- Use of VPNs or proxy servers;

If clearly fictitious names or suspicious data patterns are detected—whether at registration, during the first financial transaction or at any point thereafter—the account is flagged for review and may be suspended or terminated. Obvious misuse, such as attempting to mask identity or creating

multiple accounts to bypass controls, is handled by the internal anti-fraud team and may be escalated to the MLRO.

In cases where account termination is not linked to an STR or regulatory referral, customers will be informed via email. However, if an STR is submitted to the Financial Intelligence Unit (FIU), the matter will be managed confidentially under the guidance of the MLRO, and the customer may not be notified, until a time when such a notification would not constitute a tipping-off incident.

C. Evidence of identity for participants

In compliance with AML obligations, the Company requires full Customer Due Diligence (CDD) to be performed when a payment to a participant exceeds EUR 2,000 (or currency equivalent). However, the Company begins collecting identity evidence at the point of registration and enhances its verification requirements as transactional thresholds are approached or crossed.

CDD measures taken include:

- Identifying the player and verifying that customer's identity using reliable, independent documents, data, or information;
- Understanding the purpose and intended nature of the business relationship as part of a broader risk assessment;
- Conducting ongoing due diligence, including the scrutiny of transactional behavior, to ensure consistency with the customer's profile and known source of funds;

1. Verification of identity:

Customer identity verification starts at registration and becomes expands upon transactions reaching EUR 2,000 or more. Beginning verification involves an initial screening that analyzes the customer's KYC data (name, DOB, address), IP address, and device fingerprint. If the check confirms all data is consistent and credible, the standard procedure is applied. However, in cases of suspicion—such as potential underage use or fabricated identities—enhanced checks are triggered.

As part of standard CDD, the following information is required:

- Full name
- Identification document (passport or national ID)
- Permanent residential address
- Date of birth
- Personal Identity number

Identity documents must meet these criteria:

- Clear, High-Resolution, Color Copy
 - Color images, captured in color, not black and white or grayscale.
 - Images must be clear, legible and of reasonable quality - blurred, dark, pixelated, or cropped images will not be accepted.
 - All four corners of the document must be visible, and there should be no obstructions, such as fingers, glare, or shadows.

- Not expired at the time of submission
 - The document must be valid at the time of review. Expired documents will be immediately rejected, even if recently expired.
- Bear a visible photograph of the holder
 - The document must contain a clear photo of the customer that accurately matches their appearance.
 - The image must not be obscured, faded, or altered in any way.
- Signed by the holder
 - The document must contain the holder's signature. This is typically found on the ID page of passports and national IDs.
 - Unsigned documents (where a signature is expected) may trigger a request for supplementary verification, such as a selfie with ID or a signature sample.

All newly registered customers are screened against PEP (Politically Exposed Person), sanction, and adverse media databases as part of the onboarding process.

2. Verification of address:

Proof of address is requested either upon a withdrawal attempt, upon reaching the EUR 2,000 threshold or earlier if suspicion is raised. Acceptable documents include:

- Bank or Credit Card Statement
 - Must be issued by a recognized financial institution
 - Must include the customer's full name and complete residential address
- Utility Bill (Electricity, Gas, Water, Landline Telephone)
 - Must be issued by a trusted provider
 - Must show both billing and service address if applicable
- Government-Issued Correspondence
 - May include letters from tax authorities, social welfare departments, or other official state agencies
 - Must be addressed directly to the customer
- Residential Lease or Property Ownership Agreement
 - Must be legally binding and issued by a verified landlord, property manager, or government authority
 - Should clearly specify the full address, rental period, and parties involved
- Insurance Policies or Statements
 - Only if issued by a licensed provider and stating the insured party's full personal details and address

To be accepted, documents submitted for address verification must meet the following criteria:

- Must clearly state the customer's full legal name and current residential address
- Must be dated within the last 6 months (unless otherwise specified)
- Must be issued by a reputable and verifiable organization
- Must be submitted in high-resolution color format (scan, photograph or digital, when the document is originally issued in such a manner)
- No screenshots, mobile phone photos with glare, partial scans, or tampered files will be accepted

Unacceptable documents include, but are not limited to:

- Envelopes or mail packaging
- Documents referring to P.O. Boxes, care-of ("c/o") addresses, or virtual mailboxes
- Handwritten letters or notes
- Outdated documents
- Documents issued in a third party's name, even if family members or spouses

Triggers for address verification or reverification may include:

- Apparent discrepancies between declared and document-provided address
- Attempted/suspected multiple account usage with overlapping or altered addresses
- Attempted use of VPNs, proxies, or access from flagged IP ranges inconsistent with registered location
- Inconsistencies in declared identity (e.g. use of identity documents from one jurisdiction while logging in from another)
- Suspicions of transactions or other associations with jurisdictions considered high-risk
- Suspicions of linkage to criminal activity, adverse media, or sanctioned individuals

Consequences of Incomplete or Invalid Verification:

- The customer account may be temporarily restricted, preventing deposits, withdrawals, or gameplay
- The account may be permanently suspended if fraudulent activity or intentional misrepresentation is identified
- Where legally required, a report may be filed with the Financial Intelligence Unit (FIU)

D. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is a critical layer of the Company's AML/CFT/CFP compliance program, applied when a customer is identified as presenting a higher risk of money laundering, terrorist financing, or fraudulent behavior. These determinations are made through ongoing monitoring, transactional analysis, and the Company's risk assessment framework.

Customers identified as High Risk are subject to additional controls, monitoring protocols, and information-gathering requirements. Until these requirements are fulfilled and approved, the customer's ability to transact on the platform may be restricted.

The following events necessitate EDD initiation:

- Transactions exceeding established financial thresholds, particularly when inconsistent with prior behavior or declared occupation

- Attempted logins from or transactions involving higher risk jurisdictions
- Frequent or structured changes in deposit and withdrawal patterns, especially when involving multiple payment methods or attempts to avoid threshold-based monitoring
- Unusual or complex financial behavior, including disproportionately high deposits, use of prepaid instruments, or betting strategies inconsistent with recreational gaming
- Submission of incomplete or inconsistent personal documentation, frequent attempts/requests to change to registered details, or use of anonymizing tools (e.g., VPNs) without valid justification
- Negative media coverage, public records or open-source information linking the customer to known PEPs, illicit activity, fraud, or financial crime

To create a clearer customer profile and detect inconsistencies or identity concealment attempts the Enhanced Due Diligence process includes:

- Collection of additional identity details (middle names, former names and aliases, previous residential address data)
- Collection of additional tax ID confirmations, occupation and employer details
- Additional and alternative verification items, such as:
 - Alternative identity document sample
 - Customer 'selfie' holding ID to confirm facial match
 - Notarized or certified true copies of documentation
- Establishing the source of funds (e.g., employment records, payslips, bank statements)
- Establishing the source of wealth (e.g., asset sale documentation, inheritance letters, business ownership)
- Additional Open-source research and media checks for further insight

E. Source of Funds and Wealth

1. Source of Funds

Source of funds refers to the method by which a customer deposits money into their account. This is typically identifiable at the point of transaction, as the system logs the deposit type—e.g., debit/credit card, e-wallet, bank transfer, or voucher.

While most payment methods are recognized, certain edge cases may occur:

- If the payment method used does not align with the customer's registered details,
- If the method raises concern due to unusual usage patterns, or
- If there is insufficient information to verify ownership of the method

then the account will be immediately suspended, and the incident will be escalated to the MLRO for review.

Only funding methods that are registered under the customer's verified name are permitted. Third-party payments or anonymous payment services are not allowed under any circumstances.

Withdrawals are permitted only to the same payment method used for deposit. If this is not possible (e.g., due to a closed bank account), the customer must provide evidence explaining the change and prove ownership of the new payment method.

2. Source of Wealth

Source of wealth refers to how a customer has acquired the funds they are using on the service, and their overall financial standing. This is typically assessed during Enhanced Due Diligence (EDD) or when a customer's activity appears inconsistent with their expected profile.

To verify source of wealth, the Company may request supporting documents such as:

- Recent pay slips or an employment contract
- Tax returns or official income declarations
- Bank statements showing regular income
- Inheritance documentation, property sale agreements, or investment records
- Letters from a customer's employer or independent recognized financial advisor

Open-source checks (e.g., LinkedIn, company websites, press releases) may also be used to confirm the customer's employment or financial background.

Each case is unique, and the Company will take a risk-based approach, applying different levels of scrutiny depending on the customer's risk profile and transaction behavior.

When assessing source of wealth documentation, staff shall consider:

- The independence and reliability of the document or source
- The plausibility of the information in relation to the customer's age, occupation, and location
- Whether the customer's betting and deposit behavior aligns with the declared source of wealth

If doubts remain after review, further clarification or additional documentation may be requested. Failure to provide satisfactory evidence may result in the customer being restricted or suspended, and a Suspicious Transaction Report (STR) being filed if appropriate.

F. KYC Matrix

The following matrix details the customer due diligence requirements:

Due Diligence Check	Low Risk	Medium Risk	High Risk
PEP, Sanction, and Adverse Media Screening	✓	✓	✓
Identity Verification Screening	✓	✓	✓

Supplementary Documents		✓	✓
Additional Open-Source Checks		✓	✓
Source of Funds	✓	✓	✓
Source of Wealth			✓
Additional/advanced Identity & Address Documents			✓

IV. Ongoing Monitoring

The Company is committed to conducting ongoing due diligence throughout the duration of each customer relationship. This includes regular reviews of transactions and account behavior to ensure consistency with the customer's verified identity, expected activity, and assigned risk level.

A. Ongoing Monitoring of Transactions

All financial and gaming transactions are automatically recorded and stored securely. These transactions can be filtered and reviewed on a daily, weekly, monthly, or annual basis through the system.

Significant or unusual changes in behavior may indicate suspicious activity and will trigger an internal review. Such changes may include, but are not limited to:

- Unusually large deposits compared to historical patterns
- Gaming behavior that deviates significantly from prior activity
- A pattern of large deposits followed by attempted large withdrawals with minimal gameplay
- Frequent attempts at changing deposit or withdrawal methods
- Activity inconsistent with previously verified source of funds

Transaction monitoring is conducted continuously, and any customer behavior that suggests a change in risk profile will prompt immediate reassessment and may be escalated to the MLRO/Compliance Officer.

If a risk level change is identified (e.g., from Low to Medium or High), a review of the customer's existing due diligence file is conducted to ensure it meets the standards for their new risk category. If any documents are outdated or missing, the customer will be contacted and required to submit updated information in a timely manner.

Where transactions are deemed unusual but not clearly suspicious, the customer may be asked to explain the activity and/or provide additional documentation such as source of funds or source of wealth. Where activity cannot be reasonably explained or raises further concern, an internal report will be generated, and an STR may be filed. .

B. Ongoing Monitoring of Identity

The system does not permit users to update personal or identity details directly. Any request for changes to key information—such as name, address, date of birth, nationality, etc.—must be submitted via Customer Support and will be escalated to Compliance for review.

In these cases:

- The request will be reviewed manually by Compliance
- The customer's existing identity documents on file will be cross-checked
- The customer must provide a valid reason for the change and supporting documentation (e.g. legal name change certificate, updated ID, proof of new address)

If the request is approved:

- The relevant KYC verification steps will be re-applied as needed
- The customer's risk profile will be reassessed, and their CDD/EDD file updated accordingly
- If the customer is reclassified at a higher risk level than previously, additional documentation may be requested

If the existing identity documentation is found to be no longer sufficient or otherwise unfit for purpose, the customer will be required to provide updated documents before any changes are made.

All CDD (Customer Due Diligence) and EDD (Enhanced Due Diligence) records are fully reviewed semi-annually, even if there has been no change to the customer's status.

If a customer fails to provide updated or required verification documents:

- Their account will be suspended
- All gameplay and financial activity will be blocked
- The matter may be escalated to the MLRO, and an STR may be submitted to the Financial Intelligence Unit (FIU) if appropriate

V. Recordkeeping

The Company will log all details related to the verification process, including all identifying information provided by a customer, methods used as well as verification results, and the resolution of any discrepancy in the identifying data. The Company will maintain highly confidential records, containing a description of any document that is being relied on to verify customer's identity, describing the type of document, any identification number contained in the document, the place of issuance, the date of issuance, if any, the expiration date, etc.

All customers' money transactions and gaming activity are automatically recorded in Company's database in accordance with the set limitation periods, outlined in the relevant data protection and AML regimes. There is neither data-cleaning process nor data deleting actions that might delete those records in deviation from the Company's regulatory commitments. Transaction records are maintained for a minimum of five (5) years from the date of executing the respective transactions. The retention period for these records may be extended, subject to an according mandate by the Financial Intelligence Unit.

All customers' documents and additional customer information which has been provided during identification and verification procedures are saved on dedicated servers within the Company's infrastructure. The data is stored as protected "read-only" files which cannot be deleted by regular employees. In addition, it is regularly and automatically backed. Information and intelligence obtained through the Due Diligence process, including the client's profile, contact details, copies or records of official identity documents (e.g., passports, identity cards), bank statements, and business correspondence is securely kept on record for a minimum of five (5) years following the termination of the business relationship.

All reports generated by the MLRO/Compliance Officer, regarding money-laundering activities and any internal or external STR reports are kept in a dedicated place on the server, as protected "read-only" files, with access granted only to the MLRO/Compliance Officer and senior management.

Transactional and DD data are retained in a secure, yet accessible manner, ensuring timely compliance with information, data retrieval and inspection requests from the authorized governmental and regulatory entities.

VI. Reporting of an unusual/suspicious Transaction

An unusual transaction is defined as one that is inconsistent with a customer's established profile. Recognizing suspicious behavior depends on maintaining sufficient knowledge of the customer's identity, deposit and withdrawal patterns, and gameplay behavior.

All suspicions or knowledge of potential money laundering or terrorist financing must be reported to the Money Laundering Reporting Officer (MLRO) as soon as reasonably practical.

A. Filing a STR

The MLRO will file Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIU) for any transaction or attempted transaction involving €2,000 or more, where the Company suspects or has reasonable grounds to suspect that:

- The transaction involves funds derived from illegal activity, or is intended to hide, disguise, or convert the proceeds of crime in an attempt to evade regulatory requirements or reporting obligations.
- The transaction has no clear or lawful purpose and is not consistent with the customer's known profile or expected activity. After reviewing the background and context, no reasonable explanation can be identified.
- The Company's platform is being used to facilitate or enable criminal activity, including money laundering, terrorist financing, or fraud.

As part of its risk management and transaction monitoring framework, the system generates alerts that are triaged manually, flagged transactions are reviewed in detail, focusing on the player's historical activity and overall risk profile. If reasonable suspicion arises, cases are escalated for further investigation by the MLRO, and if deemed necessary, a STR is prepared and submitted to the Financial Intelligence Unit (FIU). This approach ensures compliance with regulatory requirements while leveraging internal solutions for effective monitoring and risk management.

B. Handling and maintenance of STR records

All Suspicious Transaction Reports (STRs), along with any supporting documentation or internal analysis, must be handled with the highest level of confidentiality and security.

To ensure regulatory compliance and protect the integrity of investigations:

- All STRs are maintained separately from other Company records to prevent unauthorized access, internal leaks, or accidental disclosure.
- STRs are stored in a secure, access-controlled digital environment, with permissions restricted to authorized personnel only.
- Records are managed by the MLRO/Compliance Officer, who are responsible for the proper filing, storage, and retrieval of STRs in accordance with regulatory and recordkeeping requirements

C. Internal Reporting

Any employee who suspects that a customer (or another employee) may be engaging in money laundering or suspicious activity must complete an Internal Suspicious Activity Reporting Form and submit it directly to the MLRO.

- The report must clearly outline the reasons for suspicion and include any supporting details or observations.
- Upon receipt, the MLRO will assess the report, initiate further investigation if required, and determine whether a formal STR to the FIU is warranted.

All employees are trained on the process for identifying and reporting suspicious activity, and clear reporting lines to the MLRO must always be followed.

A template for the above-mentioned reporting form can be found in 'Appendix A' of this document.

D. Confidentiality and Tipping Off

All Suspicious Transaction Reports (STRs) and related investigations must be treated with the strictest confidentiality by all Company staff.

It is strictly prohibited for any employee, officer, or agent of the Company to:

- Disclose that an STR has been filed with the Financial Intelligence Unit (FIU)
- Reveal that an investigation into money laundering, terrorist financing, or the proceeds of crime is underway, proposed, or pending
- Inform any customer, third party, or colleague that they are the subject of suspicion or that a report has been submitted concerning their activity

Any person who knows or suspects that a suspicious transaction report has been made, or that an investigation is ongoing or intended, must not communicate this information to any unauthorized individual. This applies to:

- Casual conversation with colleagues
- Direct communication with the customer
- Disclosure to external parties or third parties (including friends or family of the subject)

Any breach of this obligation—commonly referred to as "tipping off"—is considered a criminal offense and may constitute a breach of internal policy, subjecting the offender to disciplinary action and legal consequences.

VII. Staff education, training, and development

A. Overview

All members of management and staff receive initial training during their onboarding and routine on-going training thereafter.

Each person employed within the Company is assigned a supervisor who instructs them in relation to all policies, procedures, customer documentation forms, regulatory requirements, etc. There is a training plan for each new employee and further examinations during the following 3 months.

The AML training program is aimed to ensure that every employee receives appropriate training level with regards to any possible AML/CFT/CFP risks.

All employees are required:

- At a time specified by the MLRO/Compliance Officer, to undertake training programs on anti-money laundering policies and procedures.
- To get trained in how to recognize and deal with transactions which may be related to money laundering.
- To timely escalate and report the matter to the MLRO/Compliance Officer
- To get themselves acquainted with AML/CFT/CFP Rules & Regulations.
- To comply with the requirements of said Rules & Regulations.

B. Training Content

The Company's AML and risk awareness training includes the following content:

- The Company's commitment to the prevention, detection and reporting of ML and TF crimes.
- The consequences of ML/FT/FP for the Company, including potential legal liability.
- The responsibilities of the Company under the AML/CFT/CFP Acts and Regulations.
- Examples of ML/FT/FP that have been detected in similar organizations, to create an awareness of the potential ML/FT/FP risks which may be encountered by the Company's employees.
- Well known or recognized typologies, especially where made available by the FATF, Central Banks, other relevant bodies/institutions or AML Supervisors.
- Those particular responsibilities of employees as identified in this manual, and how employees are expected to follow the Company's internal AML/CFT/CFP procedures.
- Identification and reporting of activity that may unusual, suspicious, or otherwise concerning or noteworthy.

- The rules that apply against unlawful disclosure of suspicious transactions, activities or investigative efforts thereof (“tipping off”).

C. Recruitment and Employee screening

To maintain a trustworthy, compliant, and low-risk operational environment, the Company is committed to rigorous staff recruitment and vetting procedures. The integrity of employees – particularly those in roles exposed to sensitive customer data, transactions, or compliance decision-making – is a foundational element of the Company’s AML/CFT/CFP framework.

All prospective employees undergo a structured and documented recruitment process that includes:

- Standard Screening Measures
 - Identity verification and work eligibility checks
 - Employment history verification: The Company verifies an applicant’s past employment, cross-checking references, dates, and positions to assess reliability, continuity, and honesty.
 - Reference checks: Professional references are contacted to assess the applicant’s integrity, performance, and conduct in previous roles.
 - Criminal background checks: Where legally permitted, a check is conducted for prior convictions or involvement in criminal activity, especially in relation to fraud, financial crime, or misconduct.

Any discrepancies or red flags uncovered during this process are escalated to the Compliance or HR department for further review before any hiring decision is finalized.

- Assessment of Compliance Awareness

For roles directly or indirectly linked to financial transactions, customer verification, or risk monitoring, applicants are asked to demonstrate:

- A fundamental understanding of compliance and ethical obligations
- A willingness to follow procedures and uphold confidentiality
- An ability to recognize potential red flags or unusual behavior in interactions

This may be assessed through interview questions, practical tests, or scenario-based assessments where appropriate.

- Enhanced Vetting for Sensitive Roles

Applicants for roles with heightened exposure to risk – such as in AML compliance, payment operations, fraud prevention, or customer due diligence (CDD)—are subject to enhanced background screening. This may include:

- More detailed reference checks across multiple prior roles
- Deep-dive verification of qualifications and licensing (where relevant)
- Expanded criminal history or regulatory disciplinary record searches
- Additional screenings against watchlists, sanctions, or adverse media (especially for compliance-related roles)

Only candidates who pass all stages of vetting satisfactorily will be cleared for onboarding.

- Ongoing and Periodic Re-Screening

The Company reserves the right to re-screen existing employees, particularly when:

- An employee transfers into a new role with increased access or responsibility
- Red flags or misconduct concerns arise during employment
- Internal audits or external regulators recommend refreshed checks

Periodic re-screening may include re-confirmation of identity, updated criminal background checks, or renewed conflict of interest declarations, depending on the role and level of exposure to risk.

D. Integrity

The effectiveness of the AML/CFT/CFP framework is built on the integrity and professionalism of the Company's management and staff. Integrity forms the first line of defense against the risks of criminal exploitation of the operation.

While direct involvement in money laundering schemes represents the most severe breach, a more likely risk is a lack of proactive engagement—where staff:

- Fail to remain alert or recognize issue indicators
- Ignore or avoid reporting obligations
- Do not engage seriously with AML training
- Fail to create or support a reporting culture among their peers and/or subordinates

To mitigate these risks:

- Staff are vetted during recruitment for ethical standards, reliability, and alignment with company values
- A clear, zero-tolerance policy exists for internal misconduct related to AML/CFT/CFP failures
- Managers are expected to lead by example and actively foster a culture of vigilance, transparency, and accountability
- Whistleblowing channels are in place to support internal reporting without fear of retaliation

Failure to uphold AML responsibilities may result in disciplinary action, including termination of employment and reporting to external authorities where applicable.

E. Internal Control

As part of its framework, the Company employs an internal system of checks and controls:

- Each operator has their own credentials hence every operation carried out by one of the operators can be automatically tracked and linked to its originator. This will allow the MLRO and senior management to identify cases where one of the operators takes part or collaborates with customers who are engaged in a financial crime.
- Daily checks are carried out by the finance department, in order to assure there is a perfect match between backend transaction records appearing on Company's side and the payment supplier records. This procedure will prevent any attempt at concealing a money transfer by an employee to one of the customers without being noticed.

- The Company deploys integrated computer and communication channel monitoring solutions, which help control data leaks, investigate fraud and collect evidence in a non-disruptive way. The monitoring system tracks employee internet usage and online activity.
- In any case where it comes to any of the managers' attention that one of the operators is acting in an illegal way or a reasonable suspicion of such action is present, a swift internal investigation will be carried out by the MLRO/Compliance Officer.

F. Technological Developments

The Company recognizes the emerging risks posed by technological developments, particularly their potential misuse for money laundering, terrorist financing, fraud, and identity-related crime.

In response, the Company maintains a proactive stance to safeguard its operations, systems, and users by:

- Ensuring that senior management closely monitors technological developments, especially those related to phishing, identity fraud, unauthorized access, and new money laundering methodologies.
- Conducting internal security reviews to identify vulnerabilities in systems, software, or customer-facing channels.
- Committing to the ongoing development and enhancement of internal IT infrastructure.
- Applying layered security protocols across all digital assets to protect against data breaches, unauthorized access, and misuse.
- Running testing to evaluate the robustness of cybersecurity defenses and make necessary improvements where necessary.

The Company is committed to staying ahead of evolving threats by continuously improving its technology stack, aligning internal capabilities with global AML/CFT/CFP risk management standards, and ensuring that its systems remain resilient, secure, and effective in combating financial crime.

Appendix A | Internal Suspicious Activity Reporting Form

Account ID	
Name	
Address	
Email	
Phone Number	
Amount(s)	
Date(s)	
Due Diligence	(Please list checks done and items KYC items available. Continue on a separate sheet if necessary.)
Description of activity	(Please continue on a separate sheet if necessary.)
Payment Method(s)	
Evidence	(Please list and attach if possible)
Reasons for suspicion of money laundering activity	(Please continue on a separate sheet if necessary.)
Has any investigation been undertaken (as far as you are aware)?	☐ Yes ☐ No
Have you discussed your suspicions with anyone else?	☐ Yes ☐ No
If yes, with whom and why were discussions necessary?	
Please set out below any other information you feel is relevant	(Please continue on a separate sheet if necessary.)
Date of Report	
Submitted by	
Important Notice: Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity, directly or indirectly, or with anyone else who could alert the suspect(s) that they are under investigation. To do so may constitute a 'tipping off' offence and violation of internal policies and legal obligations.	

Receipt of report acknowledgement	
Signed MLRO	
Date	