

STARFISH MEDIA N.V.
ANTI-MONEY LAUNDERING, COUNTER-
TERRORISM FINANCING Policy
Business to Business

OGI/2024/363/0741

AML-KYC Business to Business:

“AML” Anti-Money Laundering

“CDD” Customer Due Diligence

“CRA” Customer Risk Assessment

“CTF” Counter-Terrorist Financing

“EDD” Enhanced Due Diligence

“FIU” Financial Intelligence Unit

“FS” Financial Sanction

“FT” Funding of Terrorism

“KYB” Know your Business

“KYC” Know Your Customer

“ML” Money Laundering

“PMLA” Prevention of Money Laundering Act

“SAR” Suspicious Activity Report

“SDD” Simplified Due Diligence

“SN&P” Sanctions negative media and political exposure

“STR” Suspicious Transaction Report

1. **Starfish Media N.V.** hereinafter referred to as “the Company” has chosen to instigate best practice policies, procedures and structures to improve its’ handling of Money Laundering Issues and Know Your Customer (hereinafter within this policy and procedure referred to as “**KYC & KYB**”) Practices.

These KYC & KYB Practices have been drawn-up to reflect the best practice principles and guidelines, reflecting the major international standards, directives and acts, including but not limited to:

- FATF Recommendations (Financial Action Task Force, European Inter-governmental body)
- 6th Anti-Money laundering directive

The specified policies and reporting procedures, along with the implied quality standards, apply across the board, in the Company’s activity.

The purpose of these KYC & KYB Practices is to inform employees, banking partners, regulatory authorities and foreign correspondents as to the Anti Money Laundering (AML) and Counter-Terrorist Finance (CTF) procedures adopted by the Company.

This document explains:

- What is money laundering?
- Anti-Money laundering procedures within the Company: What is the process of Money Laundering and Funding of terrorism
- Penalties

The main legislation used to compile this document includes, but is not limited to:

- 849/2015 The 4th Anti-Money Laundering and Funding of Terrorism Directive and subsequently 2018/843 5th AMLD and 2018/1673 AMLD which will be replacing the 859/2015.;
- The Money Laundering and Terrorist Financing Prevention Act.
- AML/CFT/CFP Provisions and Guidelines: In 2023, the Centrale Bank van Curaçao en Sint Maarten (CBCS)
- National Strategy and Action Plan

The present policy, and the procedures contained herein, have been drafted in order to document and support the efforts of the Company in the prevention and detection of financial fraud, money-laundering and the financing of terrorist activities, whilst conducting its business.

Scope:

The policy has been created to cover:

- Awareness and remaining alert to the possibility of money laundering or terrorist financing;
- Reporting all suspicions to the Management email address in accordance with the AML/CTF policy and SAR procedures;
- Complying fully with all anti-money laundering procedures including player identification, monitoring, record keeping, awareness and reporting in accordance with their respective roles and responsibilities within the Company
- Complete the mandatory AML/CFT Training periodically to ensure compliance and adherence to the policy

Note: All employees are obliged to read this policy, and to confirm in writing that they understand their personal responsibilities arising from the policies and procedures which are set down, along with The Company's corporate responsibilities under the Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations.

2. Purpose and Objective

The Company AML/CFT Policy is designed to prevent and mitigate any occurrence of money laundering arising from Client misuse of the Company's services. This objective is met by diligently enforcing international standards of due diligence obligations during the Company's operations, including but not limited to: the need to have adequate systems and controls to mitigate the risk of having the Company's services being used to promote financial crime.

The Company reserves the right to refuse registration, and/or provision of its services to Clients hailing from jurisdictions which fall foul of international AML/CFT standards.

The objective of this policy is to ensure regulatory compliance throughout the Company's activities, and, to establish an internal framework which aims to minimise the risk of the Company's products and services being used for money laundering and terrorist financing purposes.

In order to ensure compliance with national and international AML/CFT standards, the Company has therefore developed its Anti-Money Laundering and Know Your Client "AML/KYC" procedures. Knowledge and strict compliance to the Company's AML/KYC procedures is mandatory for all Company employees. The Company's employees will enforce AML/KYC policies with persons who use the Company's services - ie: the Company's Clients.

3. Definition of Money Laundering

Money Laundering is a term given to the various methods by which criminals attempt to make funds originating from illicit activity appear legitimate.

Therefore, and for the purposes of this present policy, “**Money laundering**” means:

- 1) concealment or maintenance of the true nature, origin, location, manner of disposal, relocation or right of ownership or other property-related acquired because of a criminal activity or property acquired instead of such property;
- 2) conversion, transfer, acquisition, possession or use of property acquired as a result of a criminal activity or property acquired instead of such property with the purpose of concealing the illicit origin of the property or assisting a person who participated in the criminal activity so that the person could escape the legal consequences of his or her actions.

Money laundering is a criminal offence, by which money derived from criminal activity is passed through a series of processes (“the laundering process”), which is used to disguise the ownership and management of such revenue, aiming to render the funds untraceable to the underlying crime. The process of money laundering makes such funds appear to have been derived from legitimate sources of business.

Money laundering also means a situation whereby a criminal activity, as a result of which the property used in money laundering was acquired, occurred in the territory of another state.

Money laundering is no longer simply the act of ‘cleaning’ or making the proceeds of crime appear as having originated from a respectable source. The process of money laundering is now widely understood to cover any and all proceeds arising from any and all criminal activity.

Therefore, the goal of anti-money laundering activities is to eradicate the laundering of profit which arises from criminal activity (such as narcotics trafficking, fraud, embezzlement, corruption, trafficking in human beings and ‘cyber crime’ etc.), as well as to provide a deterrent to criminals seeking to launder funds obtained from criminal activity by establishing sufficient safeguards and deterring measures.

These joint efforts would thereafter act to stultify the efforts of criminals who attempt to use legitimate businesses to launder their ill-gotten means

The stages of money laundering are as follows:

- Placement
- Layering
- Integration

Placement

Placement is the stage where the illicit funds are introduced into the financial system. At this stage, the funds in question are still illegitimate. The launderer will incorporate and place the money derived from illicit activity into banking and financial systems, to start the process of money laundering.

Therefore, it is very important to understand where the money is being derived from, as the person with the intention of committing such an act will need to dispose of the money derived from criminal activity, without attracting much or any attention.

Methods known to be used by launderers during the placement stage include: cash deposits, cheques, traveller's cheques, gambling, loan repayments, insurances on life policies, deposits in amounts of less than Euro 10,000, mixing legitimate with illegitimate funds, and asset purchasing.

Layering

During the layering stage, the funds would have managed to be deposited into the financial system. At this point, layering is the means used to further conceal the origin and ownership of the funds in question. Launderers often use complex structures aimed at losing all traces of the origins of the funds, and disguising ownership. Layering may happen through conducting transactions across different jurisdictions. The process is also directed to confuse investigators, and mislead the traceability of funds.

Prevention and detection of money laundering at this stage can occur by randomly questioning transactions, whilst taking care to avoid alerting the customer of any wrongdoing; vigilant monitoring of transactions and related amounts; verification of salary amounts; monitoring use of gambling chips; requesting invoices and comparing the quoted prices to the market price; and ensuring that any loan repayments are supported with relevant documentation. These are amongst some of the methods which can be used to monitor transactions, and prevent a legitimate business in being used for money laundering purposes.

Integration

At the integration stage, the money derived from criminal activity has been rendered legitimate, and has managed to be placed on the financial system, disguised as legitimate funds.

3. Terrorist financing

"Terrorist financing" loosely means the act of financing acts of terrorism

Terrorist financing is a very serious threat to financial services and businesses and is as much of a threat as is money laundering.

However, in terrorist financing, the funds in question are not necessarily derived from criminal activity. Funding of terrorism can adopt a similar methodology to that used for money laundering, however it is important to note that the intent and scope of either act vary from one another.

The main distinguishing factor between money laundering and terrorist financing, is that the source of funding for terrorist activity can be lawful, and unlike money laundering, a relatively small amount of money is required to fund the attacks. This makes it easier for criminals to bypass the legitimate financial system.

Many of the techniques used to disguise the destination of terrorist funds are identical to those used to disguise the source of illicit funds.

The company is not a subject person although the Company recognizes the importance of KYC and KYB and has practices in place to ensure compliance to the standards in place. One of the means through which the Company enforces its efforts to ensure that it or its business is not utilised by criminals in order to avoid and mitigate the risks of being utilised by criminals in this effect is that of keeping records of beneficial owners of business entities, and business applicants. The lists of individuals and entities are then uploaded and compared daily on software which is designed to automatically detect any such designated individuals or entities that have been listed on the international sanctions list.

The software is also programmed to notify the Company's employees in case of any changes or updates on sanctioned individuals, newly sanctioned individuals, or entities included on such a list. The list of active clients is scanned daily. Apart from daily monitoring, these controls are also carried out prior to the onboarding of a new customer.

The software in question is a tool used by the Company as part of its ongoing monitoring of business relationships, such as when the Company is notified of any change to beneficial ownership pertaining to the Client account. The Company's employees physically compare beneficial owners, and where suspicion is raised through any intermediary or known controlling party against sanction searches, they are checked against the following sanctions lists.

If such searches reveal a positive match, and the match has met several criteria, such match will be reported accordingly to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number

If a match has been found, the Company's employees will also investigate through open sources to obtain further information and immediately inform the Company's Head of Legal, by following internal reporting procedures. The Head of Legal will thereafter investigate any suspicion, knowledge or reason to believe and report where necessary. The Head of Legal also has the responsibility of ensuring that the screening is being carried out as instructed.

4. Terrorism Financing (TF) and Proliferation Financing (PF).

One of the issues of terrorist financing is the difficulty in identifying which dual use goods can be used for terrorism. These dual use goods evolve over time, as terrorists seek to develop new techniques in order to conduct their ventures. Dual Use items are products and technologies normally used for civilian purposes but which may have military applications.

Proliferation financing (PF) is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes) in contravention of national laws, or where applicable international obligations.

PF involves both trading in goods and the provision of services. One cannot exist without the other. United Nations (UN) Sanctions cover not only the treatment of PF but also Dual Use Goods. There is often a link between Terrorism Financing (TF) and Dual Use Products.

However, whilst in TF, one will look at the movement of funds, and a reasonably large possibility of distribution of materials to the end-point of the targeted jurisdiction, in PF one will look at the movement of goods across jurisdictions, whether or not they have been listed for export control. Moreover, PF transactions may be conducted through formal financial channels.

Dual Use Items are normally associated with proliferation and proliferation financing (there may be links between these activities and TF). As regards Dual Use Items, the Company will refer to the up-to-date list of items that the UN and European Union (EU) have identified as Dual Use Goods. The list is continuously updated to reflect new developments whenever necessary, available under Commission Delegated Regulation (EU) 2018/1922 of 10 October 2018. [See Annex 1 of this Manual].

5. Offences Relating to Money Laundering

The primary offences relating to the funding of terrorism and money laundering. The law deals with suspicion of terrorist financing and attempts of recycling funds derived from criminal activities - and these require those companies within the regulated sectors to report to the appropriate authorities, where there are grounds to know or suspect offences relating to terrorist financing and/or money laundering.

These offences include:

- Raising funds with the intent that same be used for terrorism or funding of terrorism purposes;
- Using or possessing money for the purposes of terrorism or derived from criminal activities.
- Involvement in funding arrangements and
- Money laundering (facilitating the retention or control of money which is derived and/or destined for terrorism).
- Tax evasion
- Fraud

A further list of predicate offences as per the 6th Anti-Money Laundering directive the list of criminal activities below should funds be derived shall be deemed as predicate offences”

- participation in an organised criminal group and racketeering, including any offence set out in Framework Decision 2008/841/JHA;
- terrorism, including any offence set out in Directive (EU) 2017/541 of the European Parliament and of the Council (9);
- trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU of the European Parliament and of the Council (10) and Council Framework Decision 2002/946/JHA (11);
- sexual exploitation, including any offence set out in Directive 2011/93/EU of the European Parliament and of the Council (12);
- illicit trafficking in narcotic drugs and psychotropic substances, including any offence set out in Council Framework Decision 2004/757/JHA (13);
- illicit arms trafficking;
- illicit trafficking in stolen goods and other goods;
- corruption, including any offence set out in the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union (14) and in Council Framework Decision 2003/568/JHA (15);
- fraud, including any offence set out in Council Framework Decision 2001/413/JHA (16);
- counterfeiting of currency, including any offence set out in Directive 2014/62/EU of the European Parliament and of the Council (17);
- counterfeiting and piracy of products;
- environmental crime, including any offence set out in Directive 2008/99/EC of the European Parliament and of the Council (18) or in Directive 2009/123/EC of the European Parliament and of the Council (19);
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- tax crimes relating to direct and indirect taxes, as laid down in national law;
- extortion;
- forgery;
- piracy;

- insider trading and market manipulation, including any offence set out in Directive 2014/57/EU of the European Parliament and of the Council

This obligation is significantly different, as it does not just cover "proceeds" of crime, but all funds, regardless of their origin.

There are three principal money laundering offences covering criminal activity and two related to money-laundering offences as follows:

- An offence is committed under the law when a person conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the proceeds of crime which the person knows, or suspects represents the proceeds of crime.
- Enters into an arrangement which he knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person acquires, uses or has possession of property which he knows, or suspects represents the proceeds of crime.
- Fails to disclose to the Head of Legal, whilst knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to any individual at whatever level (employee, manager, director).
- Fails to disclose when knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to the Head of Legal or sole proprietor of a business.
- ‘Tips-off’ any person that a disclosure has been made, knowing or suspecting that doing so is likely to prejudice an inquiry, makes a disclosure which is likely to prejudice a money laundering investigation or falsifies, conceals, destroys or otherwise disposes of documents which are relevant to the investigation.

6. Information required for reporting.

- Reporter Information: Reporter name, Department & today's Date
- Client information: Name, Date of Birth (DoB), Address/es, Telephone, Email, ID Number, Source of Funds (SOF), Identity of the Client (or Clients) accounts relevant to the request;
- Analyse the Client's information, including, amongst others, due diligence, transactions and ongoing monitoring information;
- Account Information: Account ID, and any associated accounts
- Suspicious Activity/Transaction: Reason for Suspicion, Timeline, Predicate Offence, Individuals Involved, Date and Time of Transaction, Amount, Transaction Number;
- List of Attached Supporting Documents

- Identify the information which is relevant following a due assessment of the information, prepare and provide the information to the the Company's Head of Legal
- Update the Company records in respect of such a request and where appropriate, notify the relevant regulators or authorities or any ML/FT suspicion

7. Risk Appetite

The Company continuously assesses the risk level of the Customer seeking its services and products. In the case of customer acceptance, only Customers who fall within the scope of the Company's Customer acceptance policy are accepted. To that end, the Company has rigorous controls in place to residually decrease risk of Customers who may pose a higher than average risk - this is done through the application of enhanced due diligence, and further checks as required on a case by case basis.

As regards business risk which the Company is ready to absorb, the Company has a medium risk appetite, in relation to products or services. The Company has sufficient controls in place by which it mitigates the risk posed, to be within controllable and acceptable boundaries, and for which the Company has control over the behavioural pattern throughout its relationship with the Client.

The established policies and procedures, as further discussed hereunder, reflect the Company's practices in relation to risk management. These procedures and policies are in place to further ensure that the desired result in achieving proper risk management and risk mitigation targets of the Company are achieved. .

8. Customer Acceptance Policy

The Customer Acceptance Policy (CAP) defines the criteria which the Company follows, in accepting new Clients. It defines the Client categorisation criteria, which are followed by the Company, and the Company employees involved in the Client acceptance and processing procedure for the provision of the services.

The Company will ensure that acceptance of new Customers will be subject to satisfactory assessment in line with the control measures in place. The Company therefore adheres to international and municipal legislation, in assessing whether an individual is seeking to partake in activities which the Company offers, in line with the risk acceptable to the Company.

9. Not Acceptable Clients

The following list establishes the category or criteria of individuals who are not deemed to be acceptable as Clients, as well as those Clients with whom the Company will not engage in a business relationship, or occasional transaction.

The list has been compiled throughout the Company's course of business, and is continuously updated, in instances such as where the Company's Board of Directors deem new and evolving lines of business as posing a high and unacceptable risk towards the Company. The risk concern is raised with senior management, where the risk declines, and an analysis is conducted in the case where a SAR is raised.

- Clients who fail or refuse to submit the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification.
- Clients who have been convicted of criminal acts either by the relevant courts of or in any other part of the world.
- Clients who are sanctioned
- Clients who have not reached the legal age of 18+
- Clients who attempt to open account with fraudulent information, fictitious names or identity theft matters
- Clients attempting to register from Non- Reputable jurisdictions (as per internal jurisdiction scoring)
- Clients who are PEP's
- Client with intent to coming ML/FT
- Clients who are involved in business activities which are illegal, unethical or involve actions which are contrary to public order or moral standards
- Clients who are sanctioned by international or governmental organisations
- Individuals involved in business structures that make it impossible to verify the ultimate beneficial owner/s
- Individuals/business structures that make it impossible to verify the legitimacy of their activities or the source of funds
- Applicants for business who refuse to provide the required information or documentation;
- Sanctioned individuals and entities
- Applicants for business involved in child pornography
- Applicants for business involved in illegal drug paraphernalia
- Applicants for business involved in pyramid sales
- Applicants for business involved in the production or trade in radioactive materials and or arms of mass destruction
- Applicants for business involved in the production or trade in weapons and munitions or spare parts of war related vehicles
- Applicants for business involved in production or activities involving harmful or explosive forms
- Applicants for business involved in forced/harmful child labour activities

- Applicants for business involved in any form of counterfeit goods
- Applicants who use Service provider which are registered in non-reputable jurisdictions and which are not licensed or authorised to operate in the EU
- Individuals or entities linked to pseudo-chivalric orders or self-styled orders which are not officially recognised
- Verification or reason to believe that funds were obtained illegally or are derived from illicit purposes
- Client for whom an SAR/STR has been raised
- Any client who activates fraud or transactional triggers and upon analysis are found to be in a serious violation of the said account
- Customers who refuse to explain unusual or suspicious access or who do not sufficiently explain unusual or suspicious activity on the remote gaming system
- Customers flagged by payment providers, verification providers, law enforcement bodies or other industry collaborative platforms as potentially suspect customers or engaging in fraud, money laundering, terrorist financing etc

Clients who fall foul of due diligence procedures, or are deemed to bypass due diligence procedures shall fall outside the acceptable limits established in the CAP. Clients engaging in illegal activity, deceiving the Company and/or acting fraudulently shall be reviewed for malicious practice. If intent is established, such Companies and individuals representing the Client, whatever the case may be, are thereafter considered to be outside the acceptable limits of the Company.

The scope of the CAP is therefore to:

- Manage any risk that the Company may be exposed to through the provision of its services to customers;
- To prevent the Company from being used, intentionally or unintentionally, for ML and/or FT purposes; and
- To identify Clients who are likely to pose a higher than average risk

10. Definition of 'Know Your Client' & Know Your Business (KYC/KYB)

KYC consists of two distinct elements:

- Verification of the identity of the Client.
- The requirement to gather enough information about the Client to be able to ascertain deviation from the 'norm' that indicates suspicious activity.

KYB is an exercise which consists of :

- Identifying and verification of the business

- Obtaining information and a company profile
- Verification of all directors and beneficial owners
- Analysis of good standing including also negative media, sanctions and political exposure

11. Internal process: Client Onboarding

The Company conducts Client onboarding through several stages. Each stage is elaborated upon below.

- Introduction: A potential Client requests to engage in a business relationship or occasional transaction with the Company.
- Onboarding Package Sent: The potential Client is sent an onboarding pack containing the relevant information and documentation required. The package contents will depend on the type of business and the entity's corporate structure.

(NB: The below lists are not exhaustive, for a full list of the information and documentation required by the Company, the reader is invited to peruse the below sections).

- Types of Entity includes: Financial Institution, Non Financial Institution, Non-Licensed Entity, Gaming Provider, VFA Licensed Entity, Partnerships, Listed Companies, Trusts & Foundations/Charities.
- Information and documentation to be requested relating to the potential Client entity includes: Certificate of Incorporation, Memorandum and Articles, Certificate of Incumbency (where applicable), Certificate of Good Standing (where applicable), Official Extract from Registry (where applicable), Organisational Chart including ownership and control structure chart, Professional Reference & SOW/F.
- Individuals & entities within the Company structure are required to provide information and documentation. These individuals and entities include: Representatives (introducer & intermediaries), Directors, Beneficial Owners (individuals and entities), Partners, Company Secretaries, Individuals with Executive Authority, Trustees, Settlers, Beneficiaries & Protectors.
- Individuals will have Financial Sanctions (FS), Politically Exposed Person (PEP) & Negative Media (NM) checks conducted on them and will be requested to provide information and documentation such as: Full Name-ID, Home and/or Work Address- PoA, Mobile Number, Curriculum Vitae (CV), Authorisation letter (as contained in Annex 2) (if required by and agent or individual representing the company) & Police Conduct Report.

- Beneficial owners (holding 10% share capital) and Representative Intermediaries will be asked to provide Source of Wealth/Source of Funds (SOW/F). Beneficial Owners who are entities will have to provide company information such as Certificate of Incorporation, Memorandum and Articles, Certificate of Incumbency & Certificate of Good Standing.
- Customer feedback and completion: Once all the required information and documentation has been received the risk score/ due diligence level is completed and signed off by the relevant officer.

12. Simplified due diligence

Simplified due diligence ('SDD'), the application of which is not an exemption from carrying out CDD measures, but rather a variant to the timing of the CDD measure to be

The measures applied may be

- The level of information and documentation obtained for verification of the identity and other CDD measures;
- The frequency and intensity of the ongoing monitoring in the case of a business relationship. Ongoing monitoring shall also determine if the level of due diligence should remain at an SDD level should there be any suspicion or any alerts raised during such monitoring.

Should it be the case where information is found to be of a suspicious nature SDD shall no longer subsist and EDD shall be applied accordingly or should any scenario within the review of the client risk assessment warrant CDD or EDD accordingly. In the onboarding of B2B simplified due diligence is not applied.

13. Customer Due Diligence

The Company's Customer Due Diligence ("CDD"), or Business Partner Due Diligence (both meaning the same thing), process is the main practice used by the Company to obtain sufficient information on its Prospective Clients and existing Clients.

By utilizing its CDD process the Company will be able to determine the customer profile through which it is to:

determine and verify whether a Prospective Client is the person s/he purports to be;

- determine whether such person is acting on behalf of another;
- establish the purpose and intended nature of the business relationship.
- monitor such business relationships on an ongoing basis.
- establish the nature of the source of wealth and funds
- establish the activity and turnover
- understand the organisational structure
- understand the reputation should the be company be already incorporated and hold a level of maturity

- identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identify, where there is a beneficial owner who is not the customer, the beneficial owner and take adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement.

In terms of timing, the Company applies its CDD process in line with the applicable laws on the Prevention of Money Laundering and Funding of Terrorism which require entities to apply CDD measures to new clients and to existing clients at appropriate times on a risk sensitive basis.

In line with the above, CDD is to be applied:

- To all Prospective Clients for business prior to establishing a business relationship;
- To all existing Clients in the event that the Company becomes aware that changes have occurred; and
- To existing high risk Clients on a periodic basis where it is deemed necessary to reconcompany identification, nature of business and any other information previously obtained.

14. Internal process: Client Onboarding

The Company conducts Client onboarding through several stages. Each stage is elaborated upon below.

- Introduction: A potential Client requests to engage in a business relationship or occasional transaction with the Company.
- Onboarding Package Sent: The potential Client is sent an onboarding pack containing the relevant information and documentation required. The package contents will depend on the type of business and the entity's corporate structure.
- (NB: The below lists are not exhaustive, for a full list of the information and documentation required by the Company, the reader is invited to peruse the below sections).
- Types of Entity includes: Financial Institution, Non Financial Institution, Non-Licensed Entity, Gaming Provider, VFA Licensed Entity, Partnerships, Listed Companies, Trusts & Foundations/Charities.
- Information and documentation to be requested relating to the potential Client entity includes: Certificate of Incorporation, Memorandum and Articles, Certificate of Incumbency (where applicable), Certificate of Good Standing (where applicable), Official Extract from Registry (where applicable), Organisational Chart including ownership and control structure chart, Professional Reference & SOW/F.

Individuals & entities within the Company structure are required to provide information and documentation.

These individuals and entities include: Representatives (introducer & intermediaries), Directors, Beneficial Owners (individuals and entities), Partners, Company Secretaries, Individuals with Executive Authority, Trustees, Settlers, Beneficiaries & Protectors.

Individuals will have Financial Sanctions (FS), Politically Exposed Person (PEP) & Negative Media (NM) checks conducted on them and will be requested to provide information and documentation such as: Full Name- ID, Home and/or Work Address- PoA, Mobile Number, Curriculum Vitae (CV), Authorisation letter (as contained in Annex 2) (if required by and agent or individual representing the company) & Police Conduct Report.

Beneficial owners (holding 10% share capital) and Representative Intermediaries will be asked to provide Source of Wealth/Source of Funds (SOW/F). Beneficial Owners who are entities will have to provide company information such as Certificate of Incorporation, Memorandum and Articles, Certificate of Incumbency & Certificate of Good Standing.

Customer feedback and completion: Once all the required information and documentation has been received the risk score/ due diligence level is completed and signed off by the relevant officer.

15.Organisational structure

It is pertinent to identify and verify the organisational structure, such may be obtained via the following steps:

Step 1: The onboarding forms state that an organizational structure is to be obtained. An internal structure and corporate structure is to be obtained

Step 2: The corporate structure is to be verified with documentation obtained from reliable sources or requested directly from the customer. Such documentation may also be required to be certified or apostille as necessary.

Step 3: If the corporate structure does not match the structure stated by the client, or it is evident that the structure has changed, this information is to be reported to the responsible person who will further contact the registry of companies

Step 4: If the structure is a PLC or does not hold relevant beneficial ownership, be it shares or voting right, a report of the steps taken to ensure there is no beneficial ownership is to be in place, and identification and verification should be undertaken on those who hold relevant control of the organization or those deemed to be the decision makers.

Step 5: If there are concerns over the structure and the information at hand, such shall be raised with the responsible person .

If it has been verified that beneficial owners are not fully in line with what is listed on the business registry, such are to be duly informed accordingly

16. Timing of Customer/Business Partner Due Diligence

The verification of the identity of the Client and the Beneficial Owner shall be performed before the establishment of a Business Relationship or the carrying out of a transaction.

By way of derogation from point (1) above, the verification of the identity of the Client and the Beneficial Owner shall be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted or the client engaging with the practitioner.

In cases where the Company is unable to comply the company shall not carry out any transaction or commence the business relationship and shall be outrightly refused until such documentation is made available.

Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing

17. Enhanced due diligence

Enhanced due diligence is the highest form of due diligence to be obtained on an entity or an individual. When business is being conducted from high risk jurisdictions, it is important to be able to access or ask the company to provide the AML/CFT controls and obtain appropriate approval from senior management, one needs to be satisfied with the respondent institution has verified the identity and ongoing performing due diligence on those customer (directors, shareholders, signatories).

The client should be able to provide relevant due diligence upon request. Enhanced due diligence is to be conducted when Politically Exposed Persons are involved or when a client has been identified to have a higher risk of being involved in ML/FT or when there has not been face-to-face contact with the client. When a PEP has been identified in the company structure, the following are to be implemented

- Approval from senior management.
- The source of wealth and the source of funds need to be established (including also transactions to such persons).
- Ongoing enhanced due diligence (every 6 months) needs to be conducted to monitor the business relationship.
- Although the term of a PEP is 12 months after one is no longer serving in public office. It would be beneficial that after the term enhanced due diligence should still be conducted for a minimum established 12 months or longer until the individual is deemed to pose no further risk.

In some situations, The Company conducts Enhanced Customer Due Diligence. These situations include:

(a) upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents;

(b) the customer is a politically exposed person, except for a local politically exposed person, their family member or a close associate;

(c) the customer is from a high-risk third country or its place of residence

(d) Customer has links to any high risk on non-reputable jurisdiction

(e) The origin of wealth and/or source of funds cannot be easily verified or the audit trail has been deliberately broken and/or unnecessarily layered or deemed complex as per the customer risk assessment;

(f) The nature of the company's business, or makes it difficult to identify the true beneficial owner;

(g) Any other situation where there is a higher risk of money laundering as defined by applicable laws and regulations according to the internally held customer risk assessment.

Enhanced due diligence measures may include (but not be limited to):

- (a) Verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
- (b) Gathering additional information on the purpose and nature of the relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source.
- (c) Gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;
- (d) Gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;
- (e) application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

The enhanced due diligence measures for customers in a high-risk third country may include one or several of the following:

- Obtaining information on the source of funds and source of wealth of the customer obtaining information on the reasons for the intended or performed transactions;
- Obtaining the approval of senior management for establishing or continuing the client relationship;

Conducting enhanced monitoring of the client relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. Where applicable, requiring the customer to carry out the first payment through an account in the customer's name with a credit institution subject to customer due diligence standards that are not less robust than those laid down in the 5th Anti-Money Laundering EU Directive.

The enhanced due diligence measures when dealing with a politically exposed person are to:

- (a) obtain senior management approval for establishing or continuing business relationships with such persons;
- (b) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
- (c) conduct enhanced, ongoing monitoring of those business relationships.

18. Client screening

Client Screening: Politically Exposed, Financial Sanctions and Negative Media

This document sets out the Company's policy to screen new and existing Clients for FS, Negative Media and PEP status.

Negative media is information or intelligence, whether proven or alleged, relating to serious financial crime, terrorism, fraud, narcotics dealings, or any crime which has an element or can lead to ML/FT.

Negative Media Screening is conducted when establishing a business relationship with a Client. In those instances where a Client has Negative Media, said Client will be evaluated prior to the Company entering into a business relationship with said Client.

When analysing Negative Media hits, the Company looks at individuals who are both convicted, and those not fully convicted, meaning; allegations, cases under investigation pending legal proceedings, wanted individuals, and any intelligence which gives rise to knowledge or suspicion that the Client is involved with ML/TF.

Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, are reported, due to the sensitivity of the crime and the possible involvement of the Client in financial crime. Should any predicate offence raise concerns, they shall be raised with the Head of Legal or the Deputy Head of Legal, accordingly.

Negative Media is categorised as follows:

i) Financial Crime

Financial crime covers a wide range of activities, including ML and the FT. It may also include fraud, bribery, or insider trading. Financial crime is a broad and

complex criminal field which may be covered in both traditional and emerging media.

ii) Violence

Violence involving Clients directly, or carried out on their behalf, may generate significantly different types of adverse media, especially when forming part of a criminal enterprise. Violent crimes may be associated with political and workforce disputes, or wider patterns of human rights abuse.

iii) Terrorism

The financing of terrorism, any terror-related activities are liable to generate significant adverse media across a range of media outlets. Terror-related types of adverse media may range from the distribution of terrorist literature and encouragement to radicalization, to the direct perpetration of terrorist acts.

iv) Fraud

Fraud can be perpetrated in numerous ways, such as: fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offence and, while the majority of cases involve improper financial gain, it may also involve property or immigration fraud.

v) Narcotics

Narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offences and associated news stories are often related to financial crimes, including ML and FT.

vi) Cybercrime

Any criminal activity involving a computer or networked device like a phone or tablet may be considered cybercrime and reported as such. Cybercrime is an umbrella-term describing activities used to facilitate other offences like digital financial crime, ML, fraud, and terrorism.

vii) Regulatory

Regulatory misconduct or non-compliance may constitute a crime in itself, or be an indication that clients are involved in other types of criminal activity. The types of adverse media stories relating to regulatory offences frequently cross-over with financial crime.

viii) Property

Adverse media stories on property may involve activities such as burglary, theft, larceny, and arson, and constitute both civil or criminal misconduct. Property offences may vary greatly in scope and be reported in a wide variety of news media formats.

ix) Trafficking

Trafficking involves the transport of humans for the purposes of forced labour or sexual exploitation. A serious criminal offence, trafficking is often related to other offences, including terrorism and various financial crimes.

x) Sexual Crimes

Sexual crimes include a wide range of activity, from violence, abuse, and rape to the transmission or possession of illegal imagery. Sexual crimes are often in proximity to other offences, including ML and cybercrime.

Any of the offences indicated above, whether convicted or alleged, shall be evaluated and the Client relationship terminated accordingly, if the adverse media is deemed to be a positive match with the Client profile.

19. Financial Sanctions

If a Client is listed under any sanction, even those not enforceable under EU legislation such as OFAC, or in the case of Clients directly or indirectly involved, or the provenance of funds used by the Client is from ownership, involvement or controlled by a sanctioned individual seeking a business relationship with the Company, the following course of action is adopted:

- All funds are to be frozen, including financial assets and economic resources, whether owned directly or indirectly by a person or an entity.
- All those assets being financial or economic resources, are not to be made available to or for the benefit of the designated persons or entities.
- If one suspects that a transaction, whether completed or attempted, is related to FT, he/she should immediately inform the Head of Legal by following internal reporting procedures.
- If the Head of Legal knows, rather than suspects, that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, he/she should not complete the transaction and report it to the relevant authority immediately.

20. Politically Exposed Persons (PEPs)

A PEP is an individual who has been entrusted with a prominent public function, such as a senior political figure, as indicated *supra*. Individuals closely related to the PEP would consist in, for instance: immediate family members and close associates. PEPs are classified as a ML/FT risk since they may be exposed to property or funds that has been generated by corruption and bribery, purely because of their position.

If a Client results as a PEP or a PEP associate, the Client profile is escalated to the Head of Legal, and the Client account is terminated. The Company does not offer its services to PEP's. Upon a Client becoming a PEP, the Client account is terminated.

21. Client Screening

An overview of the Client screening is provided in this section. The reader is kindly invited to refer to the PEP, Sanctions and Negative Media Policy section for further information.

The Company recognizes the importance of maintaining an up-to-date customer profile, and has practices in place to comply with the laws and regulations concerning identification, verification and screening of the Client for sanctions, political exposure and negative media .

Upon initiation of the account registration, the Client will be immediately screened using a third party provider (The Company currently utilises the services of Dilisense) and block any Clients who are flagged as positive for a PEP, Sanction or negative media match. Following Client registration, the Company's list of Clients is automatically scanned by the software Dilisense, on an annual basis.

Positive matches and those Clients on whom doubt remains, on the information provided by Anima Ltd. shall be investigated through open sources to obtain further information about the match. Any positive match will be immediately communicated to the Head of Legal by following internal reporting procedures. The Head of Legal may appoint any employee working within the Company Legal department to investigate such matters.

The Company reserves the right to request further documentation concerning any possible match in order to verify or discount the suspicion. If a positive match is confirmed due to the match meeting several criteria, the Company will report this to the relevant local authority.

The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Nationality

The Head of Legal is responsible to ensure that screening is being carried out as instructed. For this to be achieved, sampling of the data shall be carried out and recorded accordingly.

22. Training and Awareness Program

The Company seeks to ensure that all efforts are made to identify customers who:

- Reach substantial transaction levels – deposit and withdrawal
- Behave in a fashion that deviates from the 'norm' and therefore arouses suspicion.

Therefore all Company staff who are in any way involved with Clients and Client accounts and transactions must undergo a training program, which will ensure that they are fully aware of issues and the reporting structure available within the Company.

The training programme involves providing employees with a comprehensive understanding of the “normal” patterns of Client activity and onboarding behaviour, as well as those triggers which constitute suspicious or questionable activity, ie: deviating from Client patterns or Client behaviour deemed acceptable.

Customer Service Representatives will not be required to deal with investigation of Clients, but will be trained to assess relevant red flags, and will thereafter report the Client in question to the Head of Legal.

Yearly updates and refresher courses are made mandatory for all existing staff. This enables staff to be made aware of any issues that have arisen and how they were dealt with.

23. Recruitment

All new employees are recruited from reputable and known agencies, via local contacts or promoted from within the Company structure. The agencies utilised by the Company to conduct recruitment of new employees are required to in turn request all prospective employees to have suitable character references. The Company further requires that all new employees who are offered a permanent or temporary contract with the Company provide two sources of independent referees.

These independent referees are then sent a letter (and/or are contacted telephonically) to ensure that the prospective employee’s character reference is correct and reflects the employee’s character.

24. Whistle blowing

The Company’s Whistle-blower Policy exemplifies the standards the Company expects its employees to uphold, as representatives and ambassadors of the Company. The Company’s reputation for honesty and integrity is reflected in the way it conducts business, including but not limited to, in the integrity of its financial reporting.

The Company has cultivated a culture where employees feel empowered to report, without fear of retaliation, where they suspect or note any wrongdoing or misconduct whilst conducting their duties in the Company.

Where employees suspect any wrongdoing or misconduct, they are obliged to report it immediately. Doing so enables the Company to inspect, mitigate and remove

reputational risks. This also enables the employees to manage and absolve themselves of any personal risk.

In order to further attest to the Company's commitment in its efforts to remove, and mitigate ML/FT risks, and as already discussed throughout this policy, the policy is provided to all employees upon engagement with the Company. Employees are further required to review and attest their understanding of this policy on an annual basis.

The Company has appointed a dedicated individual to act as a point of contact for any employee or individual acting as a Whistle-blower under this policy. The Company Head of Legal/designated officer within the Human Resources Department ensures that the identity of any individual who comes forward in order to report a suspected or actual observation of misconduct and/or wrongdoing is duly protected, where the individual reporting shall remain anonymous and their identity protected. Moreover, the Company Head of Legal/designated officer within the Human Resources Department will be responsible for escalating any reports with the pertinent Company management, or local authorities concerned.

24..1 Purpose

The Company's Whistle-blower Policy is designed to ensure, and to provide assurance, that business misconduct or wrongdoing is reported. Employees and external parties are guaranteed confidentiality when such concerns are raised. The policy also protects the Whistle-blower from retaliation.

The policy is intended to encourage Board members, staff, and other individuals who may have a relationship with the Company to report suspected or actual occurrence(s) consisting of illegal, unethical, or inappropriate events (behaviours or practices) without fear of retribution.

- The Whistle-blower should promptly report the suspected or actual event to his/her supervisor.
- If the Whistle-blower would be uncomfortable or otherwise reluctant to report to his/her supervisor, then the Whistle-blower can report the event to the next highest or another level of management, including to an appropriate Board committee or member.
- The Whistle-blower can report the event with his/her identity, or anonymously.
- The Whistle blower shall receive no retaliation or retribution for a report that was provided in good faith.
- A Whistle-blower who makes a report that is not done in good faith is subject to discipline, including termination of the Board or employee relationship, or other legal means to protect the reputation of the organisation and members of its Board and staff.
- Anyone who retaliates against the Whistle-blower(who reported an event in good faith) will be subject to discipline, including termination of Board or employee status.
- Crimes against person or property, such as assault, rape, burglary, etc., should

immediately be reported to local law enforcement personnel.

- Supervisors, managers and/or Board members who receive the reports must promptly act to investigate and/or resolve the issue.
- The Whistle-blower shall receive a report within five business days of the initial report, regarding the investigation, disposition or resolution of the issue.
- If the investigation of a report, that was done in good faith and investigated by internal personnel, is not to the Whistle-blower's satisfaction, then he/she has the right to report the event to the appropriate legal or investigative agency.
- The identity of the Whistle-blower, if known, shall remain confidential to those persons directly involved in applying this policy, unless the issue requires investigation by law enforcement, in which case members of the organisation would possibly be subject to a subpoena, in accordance to the extant laws of Lithuania.

24.2 All Employees have an obligation to report real or perceived concerns.

Employees have an obligation to report all and any concerns, as soon as they become aware of the situation in question, which raises concern. The employees have the obligation to furnish as much detailed information and facts as are known to them.

If an allegation is made in good faith, but it is not validated through a review, no disciplinary action will be taken against the Employee reporting the concern. If, however, an allegation is made frivolously, maliciously or for personal gain, disciplinary action may be taken against the Employee. Intentionally or recklessly accusing an individual of wrongdoing, which the Employee knows, or reasonably ought to know, is false, is a serious matter and is subject to disciplinary action.

24.3 Anonymous Reports

This Policy encourages Employees to come forward in person wherever possible. Concerns expressed anonymously hold less water, but will be considered based on a number of factors including the seriousness of the issues raised, the credibility of the concern, and the likelihood of confirming the allegation through credible sources and/or documentary evidence.

24.4 Acknowledgement of Report

Every reported incident will be acknowledged within twenty-four hours of receipt (factoring in weekends and public holidays) with the exception of anonymous reports.

24.5 Review & Investigation of Concerns

The Company will commence a review/investigation of all concerns received, regardless of the channel through which said concern was received. All concerns received will be documented and tracked until such time as the investigation is closed.

At a minimum, the reporting Employee will be advised of the status of the review/investigation, that the review/investigation has been concluded and, where possible, the steps that were taken to resolve or prevent future occurrences, while respecting the privacy of all those involved.

13.6 Confidentiality

Unless compelled by judicial or other legal process to reveal the identity of the Employee making an allegation under this Policy, the identity of the individual utilising the Whistle-blower policy will remain confidential. No attempt to ascertain the identity of any person or group who makes a report anonymously will be tolerated.

24.7 Protection from Retaliation

The Company will not tolerate any retaliation by management or any other person or group, whether done directly or indirectly, against any person who, in good faith, makes an allegation or files a report as per this Policy, and who provides assistance to management or any other person or group, including any governmental, regulatory or law enforcement body, investigating a report.

Any individual who retaliates in any way against a person who has made a good faith allegation will be subject to disciplinary action, which may include termination of employment, and being reported to the authorities.

24.8 Methods for Reporting Concerns

Employees can use any of the following methods to report a concern:

- Either by posting an anonymous letter of concern to the HR
- Via e-mail to the Human Resources
- Verbally, to the Head of Legal/Human Resources department.

25. Record Keeping

The Company shall retain the following documents and information for a period of five (5) years following termination of the Business Relationship.

Upon expiry of the retention periods stipulated above, the Company shall delete all personal data unless otherwise instructed by any local investigative or regulatory authority. It may be necessary that any documents and/or information are retained for an additional five (5) year period. Said documents and/or information may additionally be retained if the Company is ordered to do so, or if it shall be considered necessary not to jeopardise any investigation or ongoing investigation, by any investigative or regulatory authority. In the latter case, said documents and/or information shall be retained for the duration communicated by any relevant or investigative authority.

A list of documentation to be kept for the minimum period of five (5) years are:

- Policies and documentation:
 - Copies of all policies and procedures, internal controls and compliance management;
- CDD:

- A copy of all documentation received by the Client;
- A copy of any correspondence received by the Client;
- Information on the purpose, nature and expected activity;
- All transactions;
- All training delivered and attendees;
- Employee screening records;

All Information and documentation collected for Client Due Diligence purposes shall be kept in a language that is understood by officers and employees responsible for AML/CFT within the Company. Where information and documentation is obtained in a language that is not understood, a translation (certifying that it is a correct and accurate translation) is to be made, and a copy of the translation kept on file for ease of reference.

26. Conclusion

The procedures and policies discussed in this document lay down the Company's AML and CFT policies, as well as the information which the Company requires in relation to its KYB/KYC services.

The policy in part or in its entirety is a continuously evolving document, and will be subject to change, according to the Company's business practices, in keeping in line with evolving laws, and best practices as may be stipulated, from time to time, by the pertinent national or regional regulatory authorities.

Annex 1

The subjoined list implements internationally agreed and mandated Dual-Use controls. Said items are “flagged” accordingly, when they are observed, whether during the Client on-boarding procedure, and/or during on-going monitoring, as described *supra*.

Any flagging of Dual Use products is immediately communicated to the Company’s Head of Legal, for further guidance and direction on the course of action to be adopted.

Category 0 Nuclear materials, facilities and equipment

Category 1 Special materials and related equipment

Category 2 Materials processing

Category 3 Electronics

Category 4 Computers

Category 5 Telecommunications and information security;

Category 6 Sensors and lasers

Category 7 Navigation and avionics

Category 8 Marine

Category 9 Aerospace and propulsion

Annex 2

AUTHORISATION LETTER

I/WE _____, holding passport number/s _____ hereby
duly authorise **<<list individual/s authorised> >** holding passport number **<<list their
passport/s number** to act on my behalf of the above said individuals execution of the
following services:

<<List service>>

Signature

Name & Surname:

Date _____

Authorization is valid for <<insert validation timeframe>>

Version Control

Version	Description of Changes	Release Date
1.0	Initial Version - New document created as part of AML/CFT Program review	18.01.2021
1.2	Policy updated	10.10.2023
1.3	Policy updated	15.01.2025
1.4	Policy updated : B2B version	06/02/2026

Distribution

Company	Role	Name
STARFISH MEDIA N.V.	All Employees	

Contact Information

Name	Pierric Galtier
Position	MLRO
E-mail	pierric.galtier@premiergaming.eu
Phone	(+356) 79843965
Address	Office 1/3327 Level G Quantum Hse, 75 Abate Rigord Str, Ta Xbiex XBX, XBX 1120, Malta