

Anti-Money Laundering and Counter Financing of Terrorism Policies and Procedures

Supergames N.V.

CONFIDENTIAL

This Document is intended only for the following users:

<u>User Types</u>
General Users (All Employees)

Version Control:

<u>Document Version</u>	<u>Document Author</u>	<u>Approved By</u>	<u>Document Purpose</u>	<u>Release Date</u>
1.0	Mr. Igor Basistii – MLRO	Mr. Aleksandr Kalashnikov– UBO, Attorney	Initial Release	01/09/2024
1.1	Mr. Igor Basistii – MLRO	Mr. Aleksandr Kalashnikov– UBO, Attorney	Updated Release	09/07/2025

Table of Contents

1.	Objectives.....	4
2.	Policy Statement	4
3.	General Definitions	4
4.	Introduction	8
4.1.	Stages of money laundering	8
4.2.	Placement.....	9
4.3.	Layering	9
4.4.	Integration.....	10
4.5.	Terrorist Financing	10
4.6.	Financing of Proliferation.....	10
5.	Responsibilities.....	10
6.	AML Policies and Procedures	11
6.1.	AML Detection	12
6.2.	Implement and clearly communicate policies and procedures to staff.....	12
6.3.	Risk Based Approach.....	12
6.4.	Internal Controls – Implementation of the Risk Based Approach.....	12
6.5.	Dynamic Risk Management	13
6.6.	Client Acceptance Policy	13
6.6.1.	Failure or refusal to submit information	14
6.7.	Third-Party Reliance Supergames N.V. may rely on B2C operators for player CDD, provided:	14
6.8.	Politically Exposed Persons	14
6.9.	Record Keeping and Monitoring.....	15
6.9.1	General	15
6.9.2.	Format of Records	15
6.9.3.	Certification and language of documents	15
6.9.4.	AML/CFT Audits	16
6.10.	On-going Monitoring Process.....	16
6.10.1.	General	16
6.10.2.	Procedures.....	16
	On-going Monitoring Process includes:	16
•	Identifying unusual or suspicious transactions by B2C operators.	16

• Investigating suspicious activities and reporting to the MLRO.....	16
• Verifying the source of funds for high-value transactions.....	16
• Using IT systems to track platform usage.....	16
6.10.3. Timeframes.....	16
6.10.4. Reporting to the CGA.....	17
6.11. Technical Compliance.....	17
6.12. Licensing Compliance.....	17
7. Suspicious Activity Reporting	18
7.1. Knowledge	18
7.2. Suspicious Transactions.....	18
7.3. MLRO's Report to the FIU	19
7.4. Submission of Information to the FIU	19
8. Training	20
8.1. Employees' obligations.....	21
8.2. Employees' Education and Training.....	21
8.3. MLRO Education and Training Program	22
9. Agents/Intermediaries	22
Annex A: List of Prohibited Countries	23
Annex B: EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING	24
A. MONEY LAUNDERING	24
Completed transactions.....	25
Attempted transactions	25
B. TERRORIST FINANCING	27

1. Objectives

The aim of this document is to define the policies and procedures implemented by Supergames N.V., a B2B provider, to prevent its services, including, but not limited to, gaming platforms, software, or related systems, from being used for money laundering, terrorist financing, or proliferation financing, including, without limitation:

- Conducting due diligence on business clients to ensure compliance with AML/CFT regulations.
- Providing tools and systems to B2C operators to facilitate player identification, verification, and transaction monitoring in accordance with the National Ordinance on Games of Chance (LOK) and international AML/CFT standards.
- Monitoring and assessing risks associated with business relationships, services provided, and client jurisdictions to prevent fraudulent activities.
- Ensuring compliance with technical and operational requirements set by the Curaçao Gaming Authority (CGA) for B2B licensees.

2. Policy Statement

Supergames N.V. is committed to preventing its services, including, but not limited to, gaming platforms, software, and related systems, from being used for money laundering, terrorist financing, or proliferation financing. The company ensures full compliance with Curaçao laws, CGA regulations, and international AML/CFT standards, including FATF recommendations and applicable EU Directives. This policy applies to all employees, departments, and operations, with a focus on supporting B2C operators in meeting their AML/CFT obligations through robust systems and due diligence on business clients.

3. General Definitions

For the purposes of this Manual, unless the context shall prescribe otherwise:

- “**Advisory Authority**” means the Advisory Authority for Combating Money Laundering and

Terrorist Financing.

- “**Beneficial Owner**” means the natural person or natural persons, who ultimately owns or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted.
- “**Business Relationship**” means a business, professional or commercial relationship which is connected with the professional services offered by the Company and which was expected, at the time when the contact was established, to have an element of duration.
- “**CDD**” – customer due diligence.
- “**CFATF**” - means the Caribbean Financial Action Task Force.
- “**Client**” means a legal entity, such as a B2C gaming operator, aiming to establish a Business Relationship or conduct a transaction with Supergames N.V.
- “**Company**” means Supergames N.V., a company which is duly incorporated under the Laws of Curaçao, with registered No. 167787, having its registered address at Dr. H. Fergusonweg 1, Curaçao, and its related companies and entities.
- “**Curaçao Gaming Authority (CGA)**” means the authority established under the Compliance Ordinance on Games of Chance, responsible for issuing and managing gaming licenses in Curaçao (including B2B licenses), enforcement, AML/CFT supervision, and operational compliance oversight in the gaming sector in Curaçao, under the National Ordinance on Games of Chance (LOK).
- “**EDD**” – enhanced due diligence.
- “**European Economic Area (EEA)**” means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic

Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

- **“EU Directive”** means the Directive (EU) 2023/1544 of the European Parliament and of the Council of 18 October 2023 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending previous Directive (EU) 2018/1673.
- **“FATF”** – means the Financial Action Task Force.
- **“FIU”** – means the Financial Intelligence Unit of Curaçao.
- **“Law”** means any Laws and Acts legally enacted from time to time in Curaçao, or which are applicable and enforceable in Curaçao.
- **“Manual”** means the Anti-Money Laundering and Counter Financing of Terrorism Policies and Procedures.
- **“Money Laundering and Terrorist Financing”** or **“ML/TF”** means the money laundering offences and terrorist financing offences defined in the Law.
- **“Occasional Transaction”** means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.
- **“Politically Exposed Persons (PEPs)”** means the natural persons who have their place of residence in Curaçao or any other country and who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons (see also section 6.12).
- **“PEP Status Screening”** means the process of identifying and verifying whether individuals involved in transactions or business relationships qualify as Politically

Exposed Persons (PEPs), as defined under Curaçao's anti-money laundering and counter-terrorism financing regulations. This includes screening clients, beneficial owners, and relevant parties against criteria for domestic, foreign, or international organization PEPs, as outlined in the National Ordinance on Identification when Rendering Financial Services and related guidelines. The screening is conducted during onboarding, ongoing monitoring, and transaction reviews to assess heightened risks associated with PEPs, requiring enhanced due diligence measures and, where applicable, reporting to the Financial Intelligence Unit (FIU-Curaçao) in accordance with Curaçao's legal framework.

- **“Sanctions Screening”** means the process of verifying whether individuals, legal entities, or organizations involved in transactions are listed on national or international sanctions lists, as required under Curaçao's anti-money laundering, counter-terrorism financing, and counter-proliferation financing laws. This includes checking consolidated lists issued by the United Nations Security Council, the European Union, and Curaçao authorities, as well as conducting customer and transaction due diligence to identify, freeze, and report any matches or suspicious activities to the Financial Intelligence Unit (FIU-Curaçao) in accordance with the National Ordinance on the Reporting of Unusual Transactions.
- **“Tipping-Off”** refers to the act of informing a client or third party that a suspicious transaction report (STR) has been or will be filed with the FIU, which is prohibited under Curaçao law.
- **“KYC”** for Know Your Customer
- **“Virtual Assets (VAs)”** refer to digital representations of value that can be digitally traded or transferred, such as cryptocurrencies.
- **“Virtual Asset Service Providers (VASPs)”** include entities that facilitate the exchange, transfer, or storage of VAs.
- **“B2B Services”** means gaming platform, software or other services provided by

Supergames N.V. to B2C operators or other business entities.

- **“Third-Party Reliance”** means reliance on a third party (e.g., a B2C operator) for performing CDD, subject to compliance with Curaçao’s AML/CFT regulations.

4. Introduction

The AML/CFT policy document outlines Supergames N.V.’s procedures to prevent its B2B services, including gaming platforms, software, and related systems, from being used for money laundering, terrorist financing, or proliferation financing. This document shall set the standard to be followed by the company, its officers and employees, the measures and controls in place and the internal practices to follow. The AML/CFT manual shall be reviewed at least on a yearly basis to determine if any updates and/or amendments are required. The frequency of such updates can be less should there be any regulatory change or change in the policies and procedures to be applied due to any change in the risks faced by the company or due to any changes in the assessment of certain risk factors arising out of publications made by the FIU, FATF, National Risk-Assessments and/or supra-national Risk Assessments. It shall be the MLRO’s responsibility to ensure that this document is reviewed and updated if and when required. Any updates and/or changes made to this document shall be presented to the board of directors who shall review and approved such changes.

Supergames N.V. is in the process of applying for a B2B licence issued by the Curaçao Gaming Authority (CGA) pursuant to the National Ordinance on Games of Chance (LOK) and affirms its commitment to full compliance with all applicable regulatory obligations.

4.1. Stages of money laundering

Supergames N.V. strives to ensure its B2B services are not used to facilitate money laundering or terrorist financing. The company complies with the EU Sixth Anti-Money Laundering Directive (Directive (EU) 2023/1544), EU Fifth Anti-Money Laundering Directive (Directive (EU) 2018/843) and Funding of Terrorism Regulation SL373.01, Prevention of Money Laundering Act 373, the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification when Rendering Services (NOIS), and any other applicable laws and regulations in Curaçao and the EU.

Money laundering is an offence by which money derived from criminal activity is passed through a series of processes to disguise the ownership and management of such revenue which therefore cannot be traced back to the underlying crime. The process of money laundering makes such funds appear to have been generated from legitimate sources of business.

The stages of money laundering are as follows:

- I. Placement
- II. Layering
- III. Integration

4.2. Placement

Placement is the stage where the money is introduced into the financial system, the funds at this stage are still illegitimate and the launderer will try to incorporate and place the money derived from illicit activity into the system to start the process of money laundering. At this stage it is very important to understand where the money originates from, as the person with the intention of committing such act will need to obfuscate any link of the funds with criminal activity without attracting any attention.

There are a number of methods for a launderer to perform the placement stage including, cash deposit cheques, traveler's cheques, gambling, loan repayments, life insurance policies, deposits in an amount of less than 10,000, mixing legitimate with illegitimate funds and asset purchasing.

4.3. Layering

At this stage the funds have managed to be deposited in the financial institution it is at this point layering is used through complex structures directed to lose all trace of the money and remove any trace of its origination from the proceed of a crime. This may happen by conducting transactions to different jurisdictions. This process is intended to ensure that the funds are as far removed as possible from the proceeds of a crime.

It is important to prevent such an event by transaction by ensuring staff are equipped to ask the right questions whilst avoiding alerting the customer of any suspicion. Tipping of a money launderer can have severe penalties, so all staff are regularly trained in how to detect at which point a transaction is out of their comfort zone and how to interact in a way that

would not alert the individual making the transaction of any suspicion.

4.4. Integration

At this stage, the money derived from criminal activity has been made legitimate and placed once again into the financial system as legitimate funds. At this stage, the launderer has been successful in laundering the funds.

4.5. Terrorist Financing

When dealing with the issue of terrorist financing, an important aspect is that the money does not necessarily have to be derived from criminal activity. The funds may be legitimate. It is not a case of disguising the source of the funds but simply the intentional transfer of funds from A to B with the intention of the receiver using those funds to support terrorist activity.

The intent and the scope of such acts are different and differ from case to case, but the process used for the funding of terrorism can be fairly similar to those methods used for money laundering.

Supergames N.V. ensures its platform enable Clients to monitor transactions and comply with sanctions screening requirements to prevent terrorist financing.

The Firm's AML policies, procedures and internal controls are designed to ensure compliance with all applicable legislations and best practice procedures. Policy is reviewed and updated on a regular basis to ensure all applicable procedures and internal controls are up to date to account for both changes in regulation and internal changes that could present new risk factors.

4.6. Financing of Proliferation

The Company shall take measures to prevent and detect the financing of proliferation of weapons of mass destruction, in line with the relevant UN Security Council Resolutions, Kingdom Sanctions Act, and CGA regulations. Supergames N.V. ensures to support B2C operators in implementing enhanced customer due diligence (CDD) procedures. Additionally, appropriate sanctions screening mechanisms shall be applied, particularly in relation to high-risk jurisdictions and transactions.

5. Responsibilities

The Compliance Department and staff are responsible for conducting due diligence on business clients, monitoring transactions facilitated through Supergames N.V.'s services, and ensuring that B2C operators using the company's platforms comply with AML/CFT requirements.

The following departments are directly targeted by the requirements of this procedure:

- **Board of Directors** – Approval and Signature requirements, especially in high risk scenarios.
- **All Key Functions** – Knowledge of procedure and understanding of requirements.
- **Customer Support** – Understanding reporting requirements.
- **KYC Department** – Conducts CDD and EDD on business clients, monitors compliance of B2C operators, and ensures adherence to CGA regulations.
- **Security** – Understanding DD requirements.
- **Fraud** – Understanding the difference between a fraud case and an ML case.
- **Finance** – Understanding the risks posed by ML/TF.
- **Compliance** – Ensuring all legislation requirements are met
- **MLRO** – Updating Policy and ensuring all relevant employees are aware of AML requirements.

The MLRO/Compliance Officer shall act independently and shall not hold, nor be subordinate to, any role that may present a conflict of interest, including but not limited to the positions of CEO, CFO, COO, UBO, Casino Manager, or internal auditor.

- **Local Representative:** Supergames N.V. has appointed Vivian Victoria Ersilia, Managing Director of SMES Solutions for Management and Employment Support N.V., as its local representative in Curaçao to meet the CGA's requirement for a local presence. The representative can be contacted at vivian@smes.solutions.

For any questions regarding this policy, please contact: office@supergames.cloud

The scope of this procedure may be extended to other departments if the need ever arises and all employees need to be attentive and aware of the information flow regarding PMLTF.

6. AML Policies and Procedures

6.1. AML Detection

Senior Management of Supergames N.V. is aware of the stages of money laundering and ensure to take all preventative measures to combat, prevent and detect money laundering in Supergames N.V.'s B2B services.

Prevention is ensured by carrying out the following measures:

- Implement policies and procedures throughout the group of companies;
- Clearly communicate such policies and procedures to staff;
- Adopt a risk based approach for business clients;
- Internal Controls;
- Conducting due diligence on business clients.
- Record keeping and Monitoring;
- Suspicious activity reporting;
- Training

6.2. Implement and clearly communicate policies and procedures to staff

Management ensures that AML/CFT policies and procedures are implemented and communicated to all employees.

Policies include controls to prevent misuse of gaming platforms and software by B2C operators.

6.3. Risk Based Approach

Supergames N.V. applies a risk-based approach to assess ML/TF risks from business clients, their jurisdictions, and services provided.

The Business Risk Assessment (BRA) is reviewed annually and approved by the Board of Directors, addressing risks such as:

- **Jurisdiction Risk:** Risks from clients in high-risk jurisdictions.
- **Interface Risk:** Risks from service delivery channels.
- **Client Risk:** Risks from business clients' operations or ownership.
 - **Product/Service Risk:** Risks from gaming platforms or software misuse.

6.4. Internal Controls – Implementation of the Risk Based Approach

Following the identification of inherent risk, management is required to implement the respective controls in order to mitigate such risks. The first step to adopting some form of internal control, the company must appoint at least one individual (depending on the size of the company) who is a member of the board of directors responsible for the compliance with these Regulations.

Ensure that independent testing is carried out to ensure that such controls in place are in place and do not impose any risk to the company due to present inefficiencies.

6.5. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. The MLRO conducts regular reviews of business clients, services, and risks, updating controls as needed.

In this respect, it is the duty of the MLRO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented as per the Manual's requirements, as applicable, and form part of the Annual Money Laundering Report.

It is also important for the MLRO to monitor and ensure that the proper procedures are being implemented, and the risk-based approach principle is truly being followed in all areas of the Company. By doing so, one will also be ensuring that although certain products or clients may be of a higher risk, the company may continue providing these services and assisting these clients due to the risk being mitigated through the proper policies being implemented.

6.6. Client Acceptance Policy

The Client Acceptance Policy (CAP) defines criteria for accepting business clients:

- Clients must provide: (a) legal entity name; (b) registered address; (c) incorporation details; (d) beneficial owner information.
- Documents must be collected before establishing a business relationship.
- No services are provided to anonymous clients or those on sanctions lists.
- High-risk clients require MLRO and senior management approval.

6.6.1. Failure or refusal to submit information

Clients who fail or refuse to submit and provide the company with the requisite data, information and/or documentation for their identification and verification and the creation of their profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities, although this cannot be taken as an absolute and more investigation may be required before coming to such conclusion. In such an event, the company shall suspend the relationships with such clients while at the same time the MLRO must also consider whether it is justified under the circumstances at hand to submit a report to the FIU.

If, during the Business Relationship, the Client fails or refuses to submit, within a reasonable timeframe (30 days from the date upon which the relevant threshold or circumstances have become effective), the required verification data and information in accordance with this document, the company may inform the Client of their intention to terminate the Business Relationship, in which case guidance shall be sought from the FIU on how best to proceed, while at the same time examine whether it is justified under the circumstances to submit a report to FIU (STR).

6.7. Third-Party Reliance

Supergames N.V. may rely on B2C operators for player CDD, provided:

- The operator is subject to equivalent AML/CFT regulations.
- Reliance agreements are documented and approved by the MLRO.
- The operator provides CDD data upon request.

6.8. Politically Exposed Persons

Supergames N.V. acknowledges its obligations concerning the identification and due diligence of Politically Exposed Persons (PEPs). Given the current scale of operations and the profile of its client base, no PEPs have been identified or established any business relationship with the company to date.

Supergames N.V. screens beneficial owners and key personnel of business clients for PEP status using internet searches, Transparency International Corruption Perceptions Index, www.knowyourcountry.com, and the PEP Caribbean list. Identified PEPs are subject to enhanced due diligence, including source of funds verification, and require MLRO and

senior management approval for business relationships.

6.9. Record Keeping and Monitoring

6.9.1 General

The KYC Department of the Company shall maintain records of:

- a) Business client identification and due diligence documents.
- b) Details of services provided and transactions facilitated.

Records are retained for at least five years from the termination of a business relationship or transaction, or longer if required for investigations.

The documents/data mentioned above shall be kept for a period of at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed.

It is provided that the documents/data mentioned in points (a) and (b) above which may be relevant to ongoing investigations shall be kept by the Company until the FIU confirms that the investigation has been completed and the case has been closed. Furthermore, should the firm require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, than such records will be kept until such time as the claim is extinguished or such prescriptive period has elapsed.

6.9.2. Format of Records

The Administration Department shall retain the documents/data mentioned in this Policy, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Administration Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

In case the company will establish a documents/data retention policy, the MLRO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

The Internal Auditor shall review the adherence of the company to the above, at least annually.

6.9.3. Certification and language of documents

The documents/data obtained, shall be in their original form or as a copy of the original. In high-risk cases or if deemed appropriate, the company may request documents to be

certified as true copies of the original and/or be apostilled. In the case that the documents/data are certified as true copies by a different person than the company itself or by the third party with whom a reliance and or intermediary agreement has been reached, the documents/data must be apostilled or notarized or certified by a professional whose identity and professional capacity must be confirmed and verified. In certain high-risk cases, identification and verification of the certifier may also be necessary. A true translation shall be attached in the case that the documents of point (1) above are in a language other than English or a language which is not known by the person reviewing the document.

6.9.4. AML/CFT Audits

Supergames N.V. will undergo regular AML/CFT audits conducted by CGA-approved auditors to ensure compliance with the National Ordinance on Games of Chance (LOK) and other applicable regulations. Audit results will be reported to the Curaçao Gaming Authority (CGA) as required, and any identified deficiencies will be addressed promptly to maintain compliance.

6.10. On-going Monitoring Process

6.10.1. General

The regular monitoring of the business clients and platform usage is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLRO shall be responsible for maintaining, as well as developing the on-going monitoring process of the Company.

6.10.2. Procedures

On-going Monitoring Process includes:

- Identifying unusual or suspicious transactions by B2C operators.
- Investigating suspicious activities and reporting to the MLRO.
- Verifying the source of funds for high-value transactions.
- Using IT systems to track platform usage.

6.10.3. Timeframes

The time frames set below shall act as guidelines for the KYC officer when setting the

dates for the re-review dates. Such time frames may be changed if justified notwithstanding the client has been risked as in a category, provided such justification is recorded. Furthermore, these time frames shall be changed and updated should any of the factors effecting the risk the client poses will change. The below time frames shall be taken as guidance points and not as a mandatory rule.

Risk Classification Time Frames

Low Risk	30 - 36 months
Medium Risk	18 – 30 months
High Risk	12 – 18 months

6.10.4. Reporting to the CGA

Supergames N.V. will report significant operational changes, security violations, system flaws, or fraudulent activities to the Curaçao Gaming Authority (CGA) within one day of detection. Reports will be submitted via email to info@cga.cw or in writing to the Chairman, Curaçao Gaming Control Board, Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao. Additionally, the company will submit monthly operational reports to the CGA, detailing key metrics such as transaction volumes, player activity, and compliance issues, as required under the National Ordinance on Games of Chance (LOK).

6.11. Technical Compliance

Supergames N.V. complies with the technical requirements of the National Ordinance on Games of Chance (LOK) as follows:

- Server Location: The company maintains at least one physical server in Curaçao to host gaming operations, as required by the LOK.
- Before launching new gaming products or clients interfaces, the Company shall assess potential AML/CFT vulnerabilities. Risk assessments for new technologies shall be documented and reviewed by the MLRO.

6.12. Licensing Compliance

Supergames N.V. is applying for a B2B license under the National Ordinance on Games of

Chance (LOK). The company commits to paying the required license fees under the National Ordinance on Games of Chance (LOK) and complying with CGA requirements. All operational reporting and compliance obligations, including sanctions notifications and AML/CFT audits, are managed in coordination with the Curaçao Gaming Authority (CGA) as per regulatory requirements.

7. Suspicious Activity Reporting

Suspicious activities or transactions by business clients or through Supergames N.V.'s services are reported to the FIU via the goAML portal. The MLRO investigates and files STR/SAR reports within 24 hours of suspicion, ensuring all supporting documentation is provided. If a client is identified on sanctions lists, funds are frozen, and the CGA and FIU are notified immediately.

7.1. Knowledge

Knowledge may be deemed to be an objective criterion and therefore it is not difficult to ascertain whether there is ML/FT. If for any reason the MLRO, or any other employee of the Company, is aware or is in possession of information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the MLRO should immediately proceed with filing a report with the FIU.

7.2. Suspicious Transactions

A suspicious transaction is any activity or transaction involving a business client (e.g., a B2C operator) or the use of Supergames N.V.'s services that appears inconsistent with the client's known legitimate business activities, economic profile, or operational patterns. Suspicion of ML/TF is subjective and requires consideration of multiple factors to determine whether a reasonable suspicion exists. The MLRO ensures that Supergames N.V. maintains adequate information about its business clients' activities to promptly recognize unusual or suspicious transactions.

Examples of suspicious transactions/activities related to ML/TF are provided in Annex B of this Manual. This non-exhaustive list assists the MLRO, Compliance Department, and employees in identifying potential ML/TF methods. Detection of any listed activity prompts further investigation, including requests for additional information on the source and origin of funds, the nature and economic purpose of the transactions, and the circumstances surrounding the activity.

The MLRO shall perform the following activities to identify suspicious transactions:

- Continuously monitor changes in a business client's financial status, operational activities, or transaction patterns facilitated through Supergames N.V.'s services.
- Regularly review whether any client engages in practices listed in Annex B as potential indicators of ML/TF.
- Provide training to all relevant staff, including those handling client onboarding, platform operations, or transaction data, to recognize and report suspicious activities.

Additionally, the MLRO shall:

- Receive and investigate reports from employees on suspicious transactions or activities that raise ML/TF concerns, submitted via an Internal Suspicion Report or other appropriate form based on urgency and severity. These reports are archived by the MLRO.
- Evaluate reported information against other available sources, consulting with the reporting employee and, if necessary, their supervisors. The evaluation is documented in an Internal Evaluation Report, which is filed accordingly.
- If the evaluation confirms suspicion, prepare and submit a written Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) to the Financial Intelligence Unit (FIU) via the goAML portal within 24 hours, as outlined in Section 7.3.
- If the MLRO decides not to report to the FIU, document the reasons fully in the Internal Evaluation Report.

7.3. MLRO's Report to the FIU

Upon submitting an STR/SAR, Supergames N.V. may choose to suspend or terminate the business relationship with the client for de-risking purposes, ensuring no tipping-off occurs in accordance with Curaçao law. The MLRO maintains close liaison with the FIU to avoid interfering with investigations. If no further instructions are received from the FIU, the MLRO, in consultation with senior management, determines the appropriate course of action, ensuring compliance with anti-tipping-off regulations.

Accounts or services related to the reported client, as well as any connected accounts, are placed under enhanced monitoring by the MLRO and may be suspended if deemed necessary, without alerting the client.

7.4. Submission of Information to the FIU

In the event of an FIU investigation, the MLRO ensures the following information is provided promptly:

- Identity of the business client for whom services are provided.
- Identity of the beneficial owners of the business client.
- Identity of persons authorized to act on behalf of the client or its beneficial owners.
- Data on the volume of funds or transactions facilitated through Supergames N.V.'s services.
- Details of connected accounts, if any.

For specific transactions:

- Origin of the funds.
- Type and amount of currency involved.
- Form of funds (e.g., wire transfers).
- Identity of the person authorizing the transaction.
- Destination of the funds.
- Form of instructions and authorizations provided.
- Type and identifying number of any account involved.
- Any other information deemed essential to the investigation.

8. Training

The company must ensure that training and updates are provided to staff and key persons involved in the prevention of AML and fraud within the company. Such training may be in-house or from third party providers. All training provided should be in line and in proportion to the roles and duties of the individual employee.

Training should be tailored to the tasks and duties of the employee and the company should not adopt a one size fits all approach. Training should be provided regularly and when needed. However, a yearly refresher course should be provided to ensure that all staff are up to date on recent developments.

Records of such training received must be kept on file as proof of attendance of such training.

Non-compliance with this policy may result in disciplinary actions, legal penalties under Curaçao law, and reputational damage. Violations of AML/CFT obligations may also

expose the company to fine.

8.1. Employees' obligations

- (a) The Company's employees shall be personally liable for failure to report any information relating to knowledge or suspicion, regarding money laundering or terrorist financing;
- (b) the employees must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention in relation to transactions for which there are grounds for suspicion that the person is involved in money laundering or terrorist financing
- (c) according to the applicable Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

8.2. Employees' Education and Training

- (a) The MLRO shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, directives, and implementing procedures by introducing a complete employees' education and training program;
- (b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Firm. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the system of Curaçao;
- (c) the training program aims at educating the Firm's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;
- (d) the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The MLRO shall be responsible to refer to the relevant details and information in his/her Annual Report in respect of the employees' education and training program undertaken

each

year.

8.3. MLRO Education and Training Program

The MLRO shall be responsible for any updates in the Law and attend any external training necessary. Based on his/her training the MLRO will then provide training to the employees of the Firm further to Section 14.2 above.

The main purpose of the MLRO training is to ensure that relevant employee(s) become aware of:

- the Law and the Directive
- the Firm's Anti-Money Laundering Policy
- the statutory obligations of the Firm to report suspicious transactions
- the employees own personal obligation to refrain from activity that would result in money laundering
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

The MLRO shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

The MLRO shall complete a minimum of ten (10) hours of AML/CFT-specific training per calendar year, which may include workshops, webinars, or professional certifications relevant to local and international standards.

9. Agents/Intermediaries

The company shall be responsible to create and maintain its own customer base, and, for the foreseeable future, shall not engage any intermediaries or Agents nor shall it accept customers coming from such individuals or entities. Should the company decided to change its policy on the above, a more detailed policy is to be created and approved by the board of directors, highlighting the manner in which such entities will be handled in line with the applicable legislation and regulation at that time. Introducers, such as affiliates do not fall within such category as their role is to merely introduce the client to the company and will have no further involvement in the business relationship.

Annex A: List of Prohibited Countries

Clients of Supergames N.V. are required to ensure that they do not conduct operations or engage in any form of business activity in jurisdictions designated as prohibited or restricted, including but not limited to the following countries:

- Curaçao
- The Netherlands
- Democratic People's Republic of Korea
- Iran
- Myanmar

Annex B: EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

Under the laws of multiple jurisdictions money laundering is a serious offence. Money laundering involves various acts committed with the intention to conceal or convert property or the proceeds derived from such property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means an offence under the Criminal Law (Penal Code) of Curaçao or any other applicable law or the equivalent law in the jurisdiction within which such offence has or is suspected to have taken place. It includes but is not limited to those offences relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement amongst other.

Suspicious transactions are financial transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a money laundering offence.

Suspicious transactions also include financial transactions that you have reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that you have reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.

“Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within the industry. While the Act and Regulations do not specifically require the firm to implement or use an automated system for detecting suspicious transactions, we do have such a system in place.

In this context, transactions include those that are completed or attempted as previously explained

The Company's compliance regime includes an assessment in the course of our activities, of the risk of money laundering or terrorist financing. According to this assessment, in higher risk situations, we take reasonable measures to conduct ongoing monitoring for the purpose of detecting suspicious transactions

Completed transactions

Transactions processed through Supergames N.V.'s services, such as payments or fund transfers between a B2C operator and its accounts.

Attempted transactions

An attempted transaction is one that a client intended to conduct and took some form of action to do so. An attempted transaction is different from a simple request for information, such as an enquiry as to the fee applicable to a certain transaction. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the client. A formal request by the client to withdraw funds from their account would constitute such an attempt.

The following are examples of attempted transactions:

- A financial entity or casino refuses to accept a deposit because the client refuses to provide identification as requested.
 - A securities dealer or life insurance agent refuses to process a transaction - for which the client insists on using cash - because their business practice is not to accept cash.
 - A client of a real estate agent starts to make an offer on the purchase of a house with a large deposit but will not finalize the offer once asked to provide identification.
 - An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
 - A money services business will not process a request to transfer a large amount of funds because the client requesting the transfer refuses to provide identification requested.
- To report an attempted transaction, it must be one that you have reasonable grounds to suspect that it is related to money laundering or terrorist financing (as explained in section

An attempt to conduct a transaction does not necessarily mean the transaction is suspicious. However, the circumstances surrounding it might contribute to your having reasonable grounds for suspicion.

The following are examples of suspicious transactions/activities related to money laundering:

1. Transactions with no discernible business purpose or that are unnecessarily complex, such as multiple fund transfers through Supergames N.V.'s platforms without clear justification.
2. Use of business client accounts with complex ownership structures (e.g., nested shell companies) that are not justified by the client's operational needs or economic profile.
3. Transaction volumes or sizes requested by a business client that are inconsistent with their known business activities or financial capacity.
4. Large volumes of funds processed through Supergames N.V.'s services that do not align with the business client's stated revenue sources or operational scope.
5. A business client's reluctance to provide complete information when establishing a business relationship, including the nature and purpose of their activities, beneficial ownership details, or source of funds, or provision of misleading or unverifiable information.
6. Frequent high-value transactions by a business client without a clear economic rationale, such as rapid transfers to multiple accounts.
7. Transfers of funds to or from jurisdictions identified as high-risk for ML/TF by FATF or Curaçao authorities, without a legitimate business purpose.
8. A business client introduced by a third party from a high-risk jurisdiction that does not adequately comply with FATF recommendations.
9. Inconsistencies in due diligence documentation, such as discrepancies in beneficial ownership records, corporate registration details, or financial statements.
10. Requests to settle transactions through third parties unrelated to the business client, without a documented intermediary agreement.
11. Delays or difficulties in submitting required due diligence documents, such as certified corporate records or beneficial ownership information.

12. Transactions involving business clients with beneficial owners or key personnel listed on sanctions lists or identified as politically exposed persons (PEPs) without adequate risk mitigation.

B. TERRORIST FINANCING

Terrorist financing may involve funds from legitimate or illicit sources transferred to support terrorist activities. Unlike money laundering, terrorist financing does not always require disguising the source of funds but focuses on their intentional transfer for illicit purposes. Supergames N.V.'s AML/CFT policies, procedures, and internal controls are designed to prevent its services from being used for terrorist financing, ensuring compliance with Curaçao's laws, CGA requirements, and international standards (e.g., FATF, EU Directive 2023/1544). These policies are regularly reviewed to address regulatory changes and emerging risks.

Terrorist financing funds may originate from criminal activities (e.g., kidnapping, extortion, smuggling, robbery, drug trafficking) or legitimate sources, such as:

- Collection of membership dues or subscriptions.
- Sale of publications or media.
- Cultural or social events.
- Donations or community fundraising.

Suspicious transactions related to terrorist financing include those that Supergames N.V. has reasonable grounds to suspect are linked to the commission or attempted commission of a terrorist financing offense. If an employee or officer knows, rather than suspects, that a transaction involves funds owned or controlled by a terrorist or terrorist group, the transaction is suspended, accounts are frozen, and a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is filed immediately with the Financial Intelligence Unit (FIU).

The following are examples of suspicious transactions/activities related to terrorist financing:

1. Transactions by a business client involving entities or individuals listed on national or international sanctions lists, or with known ties to terrorist organizations.
2. Unexplained high-volume fund transfers through Supergames N.V.'s platforms to or from high-risk jurisdictions without a clear business purpose.

3. Business clients with beneficial owners or key personnel identified as PEPs or associated with entities in high-risk jurisdictions, without adequate due diligence.
4. Use of Supergames N.V.'s services to facilitate transactions for organizations claiming charitable or non-profit status but lacking transparency in their operations or funding sources.
5. Frequent transfers to third-party accounts unrelated to the business client's operations, particularly in jurisdictions with inadequate AML/CFT controls.
6. Transactions involving complex corporate structures that obscure beneficial ownership, potentially facilitating the transfer of funds for illicit purposes.
7. Requests for rapid or frequent fund transfers through Supergames N.V.'s platforms with no documented business rationale, particularly to high-risk jurisdictions.

By: **MLRO of Supergames N.V.**

Name: Igor Basistii

Date: 09.07.2025



Signature

By: **UBO, Attorney of
Supergames N.V.**

Name: Aleksandr Kalashnikov

Date: 09.07.2025



Signature



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

Date: 30.07.2025