

Boom Line N.V.
Anti Money Laundering & Combating the Financing of Terrorism Policy
Anti-Money Laundering (AML) Program and Compliance Procedures

I General Definitions

For the purposes of this Manual, and unless the context otherwise requires:

Money Laundering Reporting Officer (also MLRO) means the person appointed by the Company as its AML/CFT compliance and reporting officer under the Regulations;

Beneficial Owner means

a an individual who is an ultimate beneficial owner of the Legal Person, partnership or legal arrangement, whether or not the individual is the only beneficial owner;

and

b an individual who exercises ultimate control over the management of the Legal Person, partnership or legal arrangement, whether alone or jointly with any other person or persons, regardless of whether the ultimate ownership or control is direct or indirect. For the avoidance of doubt, an individual is not deemed to be the Beneficial Owner of a company, the securities of which are listed on a recognized exchange;

Business Relationship means a business, professional or commercial relationship between the Company and a Customer which is expected by the Company, at the time when contact is established, to have an element of duration;

Company means Boom Line B.V., a limited liability company established under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 159576;

Customer means any Legal Person with whom the Company has or expects to establish a Business Relationship or Occasional Transaction;

Customer Due Diligence Information means Identification Information and Relationship Information;

Customer Due Diligence Measures means

(1) the measures for:

a identifying a Customer as well as any Player;

b determining whether the Customer or Player is acting for a third party and, if so, identifying the third party;

c verifying the identity of the Customer or Player and any third party for whom the Customer or Player is acting;

d identifying each Beneficial Owner of the Customer and the third party, where either the Customer or third party, or both are not individuals;

e taking reasonable measures, on a risk-sensitive basis, to verify the identity of each Beneficial Owner of the Customer and third party so that the Company is satisfied that it knows who each Beneficial Owner is, including, in the case of a Legal Person, partnership, Foundation, trust or similar arrangement, taking reasonable measures to understand the ownership and control structure of the Legal Person, partnership, Foundation, trust or similar arrangement;

f obtaining information on the purpose and intended nature of the Business Relationship or Occasional Transaction. Such measures include where the Customer is not an individual, measures

for verifying that any person purporting to act on behalf of the Customer is authorized to do so, identifying that person and verifying the identity of that person.

g Where the Company is required to verify the identity of a person, it shall verify that person's identity using documents, data or information obtained from a reliable and independent source.

Domestic Politically Exposed Person means a person who is or has been entrusted with a prominent public function by the State;

Foreign Politically Exposed Person means a person who is, or has been entrusted with a prominent function by an international organization;

Foundation means a foundation, wherever established;

Identification Information is information used to identify a person required by the regulations to be identified and as specified in this AML/CFT policy;

Introducer means a person who has a Business Relationship with a Legal Person and who introduces that Legal Person to the Company with the intention that the Legal Person will form a Business Relationship or conduct an Occasional Transaction with the Company so that the Legal Person becomes a Customer of the Company;

Legal Person includes a company, a partnership, whether limited or general, an association or any unincorporated body of persons, but does not include a trust;

Occasional Transaction means a transaction that is carried out otherwise than as part of a Business Relationship, and is carried out as:

a a single transaction; or

b two or more linked transactions where it appears at the outset to any person handling any of the transactions that the transactions are linked or at any later stage it comes to the attention of the person handling any of those transactions that the transactions are linked, that amount to EUR 2500 where it is a transaction or linked transaction carried out on the course of a money services business or EUR 10,000 in the case of any other transaction or linked transaction;

Ongoing Monitoring means with regards to a Business Relationship:

a scrutinizing transactions undertaken throughout the course of the relationship, including where necessary the source of funds to ensure that the transactions are consistent with the Company's knowledge of the Customer and the Customer's business and risk profile; and

b keeping the documents, data or information obtained for the purpose of applying Customer Due Diligence measures up-to-date and relevant by undertaking reviews of existing records.

Politically Exposed Person means a Foreign Politically Exposed Person, a Domestic Politically Exposed Person or a person who is, or has been entrusted with a prominent function by an international organization;

Players any person who completes the registration and identification process enabling him to make use of the online gaming services on the Websites;

Regulations means the Anti-Money Laundering and Terrorist Financing Regulations applicable to business activity of the Company and/or any applicable regulatory or governmental obligations;

Relationship Information means information concerning the Business Relationship or proposed Business Relationship between the Company and its Customer;

Websites means all websites authorized under a valid gaming license in the name of the Company, which can be accessed by means of a domain name and where Players can access the online gaming services.

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions in which the Company operates, to prevent the use of the financial system for the purpose of money laundering and terrorist financing.

The Company **Boom Line N.V.** is incorporated in Curacao and is licensed and regulated by GCB to offer remote games over the internet, under the license conditions issued by Curaçao. The Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

The Company has appointed a MLRO.

The MLRO must be appropriately qualified and will be responsible for receiving internal disclosures/ notifications, reviewing and investigating such disclosures/ notifications and deciding whether those disclosures/notifications should be reported to the relevant authorities and preparing any necessary reports.

III Objective of the Policy

1 It is the policy of the Company to comply in all respects with the requirements of the Money Laundering Legislation (including but not limited to the Prevention and Suppression of Money Laundering and Terrorist Financing Law) by ensuring that we have policies and procedures to aid compliance.

2 The main scope of this policy is to establish the essential standards designed to prevent the Company from being used for money laundering and terrorism financing. This AML and CFT policy applies to the Company and all of its staff, whether on a full or part time basis, and to any subcontractor and its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.

3 The Company is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as the risks to its reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

4 The Company will endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

5 The Company's policies, procedures and internal controls are designed to ensure compliance with all applicable laws, rules, directives and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place.

IV Regulatory Framework

National regulations

Pursuant to the National Ordinance Penalization of Money Laundering (1993), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

- a The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c The National Ordinance on Identification when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- f National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting International standards by regularly implementing these standards in its national legislation.

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

V Definition of money laundering

1. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. There are three stages in the process:

- 1) Placement: Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments.
- 2) Layering: How the link between the funds and the criminal is concealed.
- 3) Integration: Investing and/or recovering the funds in a way that looks legitimate.

As it is strictly a Company policy not to accept cash as means of payment, the Company's AML Policy is focused to prevent the use of the Company's activities and resources in the 2nd and in the 3rd stage.

VI Player Identification Process

1 The Company will take reasonable steps to establish the identity of all Players. For this purpose the process for the registration of Players provided for under the General Terms and Conditions of the Company provides for the due diligence process that must be carried out before the opening of a user account.

2 The Company will keep at all times a secure online list of all registered Players and information and documents will be retained in accordance with the applicable data protection obligations.

3 The Company will collect certain minimum Player identification information from each Player who opens an account. The Company will not accept to open anonymous accounts or accounts in fictitious names such that the true beneficial owner is not known. The information required will include at least: a) Player's date of birth (showing that the player is over eighteen (18) years of age);

b) Player's first and last name;

c) Player's place of residence;

d) Player's valid email address; and

e) Player's username and a password.

4 Documents to verify the identity information received will be requested from the Player, as a Standard Due Diligence procedure, if and when there is considered to be risk or uncertainty about the information provided and prior to any payment in excess of ANG 5000 or equivalent to that amount in any other currency per occasion or when payments to the account are made in excess of ANG 5000 or equivalent to that amount in any other currency. These documents shall include, to the extent permitted under the relevant data protection regulations:

a) A copy of a valid identity card or passport;

b) Proof of address; and

c) Source of funds

5 The Company may supplement the use of documentary evidence by using other means, which may include:

a) Independently verifying the Player's identity through the comparison of information provided by the Player with information obtained from a reporting agency, public database or other source;

- b Checking references with financial institutions; or
- c Obtaining a financial statement.

The Company will inform relevant Players that the Company may seek identification information to verify their identity.

- 6 Any employee of the Company who becomes aware of an uncertainty in relation to the accuracy and truthfulness of the Player information provided shall immediately notify the MLRO, who will review the materials and determine whether further identification is required and/ or that it may be determined whether a report is to be sent to the relevant authorities.
- 7 If a potential or existing Player either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, the MLRO will be notified so that it may be determined whether a report is to be sent to the relevant authorities.
- 8 If a Player has been identified as attempting or participating in any criminal or unlawful activity, the Company will take the appropriate steps to immediately freeze the account of the Player.
- 9 If any material personal information of a Player changes, verification documents will be requested.

VII Customer Due Diligence and on-going monitoring

- 1 In accordance with Customer Due Diligence measures it is the policy of the Company to undertake a risk assessment, and ensure that evidence of Customer's identity is obtained and retained as appropriate for all customers. Due to the nature of the online gaming business, the Company conducts an enhanced due diligence process for all of its prospective Customers.
- 2 The Company shall obtain from the Customer full amount of KYC documentation and information – included but not limited to details of Ultimate Beneficial owners (UBO), details of directors, gaming licenses etc. Every Customer shall have to fill out a due diligence form as provided in Appendix 1 (Customer form).
- 3 Once all the information requested is obtained, the Company sends a confirmation email to the Customer on the email inserted by the Customer in the registration form.
- 4 In addition, to the due diligence process performed at the initial acceptance stage, the Customers shall be monitored on an on-going basis.
- 5 The steps concerning Customer Due Diligence and on-going monitoring on Players can be found under section VIII.

VIII Continuous transaction due diligence

- 1 The Company will monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
- 2 Monitoring will be conducted through the following methods -Transactions will be automatically monitored and reviewed daily for all transactions above 1000 EUR along with all the details of the users making those transactions. Documents may be required at the determination of the MLRO.

The MLRO will be responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the relevant authorities.

3 Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

1 Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason.

2 Many small, incoming wire transfers or deposits made using checks and money orders.

3 Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose.

4 When an employee of the Company detects any activity that may be suspicious, he or she will notify the MLRO as per form specified in Appendix 2. MLRO will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

5 The Company will not accept cash or non-electronic payments from Players. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method approved by the Company or respective regulators.

6 The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

7 To the extent the Company utilizes a third party to process and record payments to and from Player and accounts, the Company will use best efforts to ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The MLRO shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

8 Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

9 MLRO shall submit necessary reports to Curaçao Gaming Control Board (GCB) according to with the publication of the National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282) and the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283) and to the board of management of the Company as per Manual for AML Reporting (Appendix 3) and forms attached thereto – Suspicious Activity Report form, Politically Exposed Person Report form; Significant Transaction Report form; Terrorist property report form.

IX Risk Management

Risk Classification

The Company maintains a risk-based approach in relation Players in order to effectively detect and deter any risks it may be exposed to such as money laundering, the financing of terrorism or any prohibited transaction such as fraud.

The Company maintains the following risk classification:

- Low risk
- High risk

Low risk

All Players are classified as Low risk and are subjected to due diligence procedures related to the request for KYC documentation as per the process described above in Art.3 of Section VI and constant monitoring of activities on the account.

High Risk

The Player activity is the determining factor for the classification of a Player as High Risk. Any Player of which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High Risk, for which an due diligence procedure as described in Art.4 and/or Art.5 of Section VI is applied. The instances in which a High Risk classification is assigned includes but are not limited to those instances as mentioned in the section XI below.

X Internal Controls

1 Internal control procedures have been designed to comply with the regulations. Internal controls take the form of manual controls implemented on a daily basis by the Company's Operations Team (and/or Payments Team) and computer/automated controls inherent within the gaming system software.

2 Before signature of any Software license agreement the Company shall check conformity of every potential Customer to the following requirements:

1 on any website owned or controlled by Customer:

1.a Since July 30, 2012, the GCB and FMA have joined forces through a Cooperation Protocol, in the implementation of the Self-Exclusion Program, the combating and prevention of gambling addiction. Thus website contains terms and conditions on use of the website, including terms of responsible game. Terms and conditions contain a list of restricted territories conforming to the list of the Company in force at the time of the check; procedure of KYC providing sufficient anti-money laundering measures, that are in conformity with European Union law in force at the time of the check.

1.b website contains true information of the potential customer.

1.c website contains contact information (email, phone number), where to apply in case of player complaints.

1.d website contains reference to the valid gaming license (in case of existence of a validation link - validity of the gaming license has been checked via validation link) and the reference conforms with the information provided by the customer to the Company.

1.e website contains reference and links only to regulated payment mechanisms (make a list of all payment mechanisms contained on the website at the time of the check);

1.f website does not accept payments from land-based wagering agents and/or cash-based wager aggregators, website does not contain any reference to such options (in case of a negative answer – make a list of references not conforming to this requirement).

2 check via accessible means on reputation of the potential customer – review of references, player and/or business - partner opinions, feedback on potential customers available in internet sources most trusted and mostly used in industry at the time of the check (provide citations and source) – gives positive results.

3 check via accessible and most recognized sources in industry (e.g. search engines, websites, etc.) on existence of any kind of promotion material (advertisement, banner, etc.) of the potential customer and/or it's website(s) and conformity of detected promotion materials to the following criteria - promotion material in question prima facie seems legal (e.g. at first sight does not contain reference or item of any obviously unlicensed intellectual property, illegal promise and/or

statement).

3. Before signature of any White Label Agreement the Company shall perform Customer Due Diligence procedure as per Section VII.

XI Suspicious Transactions and Reporting

1 The MLRO will report any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a Player account involving EUR 1,000 or more of funds (either individually or in the aggregate) where the MLRO knows, suspects or has reason to suspect:

a The Player is included on any list of individuals assumed associated with terrorism or on a sanctions list;

b The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;

c The transaction has no ordinary lawful purpose or is not the sort in which the Player would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

d The transaction involves the use of the Company to facilitate criminal activity.

2 MLRO files a Suspicious Transaction Report (STR) with the Curaçao FIU if he suspects or has reasonable grounds to suspect that:

a a transaction may be related to Money Laundering (ML) or Funding Terrorism (FT), or

b a person may have been, is, or, may be connected with ML/FT; or

c ML/FT has been, is being, or may be committed or attempted.

3 The STR is drawn up by the MLRO as soon as reasonably practicable, but not later than 5 working days from when the suspicion first arose.

4 Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or filing of the suspicious activity report with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

XII Additional Measures

1 In addition, an AI which is overseen by the MRLO will look for any unusual behavior and report it right away to an employee of the Company.

2 According to a risk based approach and general experience the human employees will recheck all checks which are done before by the AI or other employees and may redo or do additional checks according to the situation. In addition, a data Scientist supported by modern, electronic, analytic systems will look for unusual behavior like:

1 Depositing and withdrawing without longer Betting sessions.

2 Attempts to use a different Bank account for Deposit and Withdraw, nationality changes, currency changes, behavior and activity changes as well as checks, if an account is used by it's original owner.

Also a Player has to use the same method for Withdrawal as he used for Deposit, for the amount of the initial Deposit to prevent any Money Laundering.

XIII Record Keeping

- 1 It is Company policy to maintain the following records;
 - 1 a copy of, or the references to, the evidence of the Customer's UBO or director's identity obtained; and
 - 2 the supporting evidence and records in respect of the Business Relationships and Occasional Transactions which are the subject of customer due diligence;
 - 3 all Player transaction, data, identification documents and/or any due diligence documentation;
 - 4 internal reports of MLRO and external reports made to the FIU;
 - 5 records of AML training provided to employees.
- 2 Records are maintained for a period of 5 years, beginning on the date on which the business relationship ends.

XIV Enterprise-wide risk assessment

- 1 As part of its risk-based approach, The Company has conducted an AML "Enterprise- wide risk assessment" (EWRA) to identify and understand risks specific to the Company and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the Website offers, the Players to whom services are offered, transactions performed by these Players, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.
- 2 The identification of AML risk categories is based on Company's understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.
- 3 The EWRA is yearly reassessed.

XV Auditing

Internal audit regularly (once a year or as necessary) establishes missions and reports about AML activities.

XVI Training Programs

- 1 The Company will develop ongoing employee training under the leadership of the MLRO and senior management. The training will occur on at least an annual basis. It will be based on the Company's size, its Player base, and its resources and be updated as necessary to reflect any new developments in the law.
- 2 The training will include, at a minimum:
 - 1 how to identify red flags and signs of money laundering that arise during the course of the employees' duties;
 - 2 what to do once the risk is identified (including how, when and to whom to escalate unusual Player activity or other red flags for analysis;
 - 3 what employees' roles are in the Company's compliance efforts and how to perform them;
 - 4 the Company's record retention policy;
 - 5 the disciplinary consequences for non-compliance with legislation.

XVII Data Security

All data given by any Player/Customer will be kept secure, will not be sold or given to anyone else. Only if forced by law, or to prevent money laundering data may be shared with the AML-authority of the affected state. You can read more about data security in Company's privacy policy.

XVIII MLRO Contact Details

Contact details of the MLRO of The Company:

Email: law@13aff.com

Appendices:

Appendix 1: Customer form

Appendix 2: Internal Suspicious Money Laundering Transaction Report

Appendix 3: Manual for AML Reporting,

Authorised signatory signature:

Vladyslav Kuzmenko

Date: 06.01.2025

Signature:



Kyryl Shvets

Date: 06.01.2025

Signature:



Customer form

In order to ensure our ongoing compliance with all Legal and Regulatory Requirements in relation to the prevention of Money Laundering and Terrorist Financing, we require you to provide the following information prior to the launch of Software.

Include additional sheets as necessary

Name of company, business address incl.country, phone number, e-mail address:	Boom LineB.V., Dr. M.J. Hugenholtzweg 25, Unit 11, Curacao,
Company MLRO-name, phone number, e-mail address:	
Company number and registered office:	159576, Dr. M.J. Hugenholtzweg 25, Unit 11, Curacao
List of URLs or proposed URLs:	13Spins.com Gangsta.casino Onlystake.com
License number and licensing authority	https://cert.gcb.cw/certificate?id=ZXIKcGRpSTZJbGh3T1ZFd2MzaFZPVWhSVIZCeFZsUlhwakJvVFdjOVBTSXNJblpoYkhWbElqb2IPVFP2UTBaaWRWcGhibkZLTTJGaIVXWTFPVTIzZHowOUIpd2liV0ZqSWpvaU5UTXhPVGswWkRGak1ESXpaakpqTIRsak1UWmxNbVF6TIRNd01HSTNZVFk1TUROallqY3INMkl3TIRZMllqZzNPR0ZqTUdFMVpqTmlaR05tTmPCak5DSXNJblJoWnlJNklpSjk= https://cert.gcb.cw/certificate?id=ZXIKcGRpSTZJbHBIYUZaWIRISTRTbmRYVfZSV1VYSnJTVmhMWW5jOVBTSXNJblpoYkhWbElqb2IURXA2UzNNMmNra3ZSV05uYzJkUE1VTklNVzILUVQwOUIpd2liV0ZqSWpvaVpUVmtNelkwWmpGak9EQmINVEUzWkRjMFpERXpaall4Tm1ZMU5EUTFaRGd6TORRME9HUTBZMkZoWIRoak5qSTVaVEUzWmpZd1pEQTF0ek0zWWpCbE9TSXNJblJoWnlJNklpSjk= https://cert.gcb.cw/certificate?id=ZXIKcGRpSTZJa3hhTmtadmVUVXZTaIF3Vnpnd1V6Uk1ZeTkWU0ZFOVBTSXNJblpoYkhWbElqb2IOalowY2pGd1kzbFNna3RwYzBONUswdzVhR3MxUVQwOUIpd2liV0ZqSWpvaU5qUXdaV15TKdKa01USTJNamhoTVdRMU9UQXpZVFF5WVRsa1kyRTVOMk14WIRGbvPpEWXINelEyWW1Zd05qa3hZamN3WkdFMU5UTTNNREprT
List of Directors (name and country of residence)	Odin Trust B.V.
List of Ultimate Beneficial Owners who control 25 % or more of the business or businesses in the group	Vladyslav Kuzmenko – 100%

(name and country of residence):	
----------------------------------	--

Please check this box to confirm that you will obtain and provide Company necessary AML documentation as required by Company.

Please check this box to warrant that all information provided is complete and accurate.

Authorised signatory signature:

Vladyslav Kuzmenko
Date: 06/01/2024



Kyryl Shvets
Date: 06/01/2024



Internal Suspicious Money Laundering Transaction Report

Specific to Employees to be submitted to the MLRO for completion of the form:

It is your legal duty and a requirement of your employment with this practice that you report any knowledge or suspicion concerning money laundering to the firm's MLRO.

In accordance with our internal procedures, you need to complete the report form as quickly as is practical. Should any delay be likely you need to contact the MLRO immediately.

The form should be completed in manuscript and delivered to the MLRO in a sealed envelope marked 'Addressee only'. Please do not take any copies.

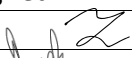
Tipping off is a criminal offence. You should therefore avoid discussing your suspicions or concerns with anyone other than the MLRO in all but the most unusual circumstances.

Failure to comply with these requirements may result in action being taken against you in line with the Company's usual disciplinary procedures.

To: The Money Laundering Reporting Officer
Date of the report: 06/01/2025
Prepared by: Kyril Shvets
Name of individual(s) suspected: Kyril Shvets
Name of Customer (if different): [Insert Customer name or confirm that no difference from the list above]
Reason for suspicion: [Give a detailed description of the reasons for your knowledge or suspicions]
Date suspicion first aroused: [insert date]
Names of all other colleagues who have been involved with this Customer's affairs: [Insert name of all individuals informed – each of whom should sign the declaration below]

Declaration

I am aware of the risks and penalties regarding "tipping off", or investigation of the above or related matters by the authorities.

Name:	Signed:	Dated:
Vladyslav Kuzmenko		06/01/2025
Kyryl Shvets		06/01/2025

Appendix 3:

Form to be completed by the Money Laundering Reporting Officer upon receiving the above report from an Employee

Date received Consideration of Disclosure:

Action Plan:

--

Outcome of Consideration of Disclosure:

Are there reasonable Grounds for suspicion?

--

Is consent required from the Financial Intelligence Analysis Unit (FIAU) to any ongoing or imminent transactions which would otherwise be prohibited acts?

YES

NO

If YES, please record authorisation and “way forward” details received from the Financial Intelligence Analysis Unit