

AML Policy of Prolific Trade N.V.

Private & Confidential

April 8th 2025

Information on the document

Prepared by: Miruna Mihailescu – Money Laundering Reporting Officer

Version History

Date	Version	Amended by	Brief description
07 Feb 2022	1.0	-	First issue
25 Nov 2022	1.1	Miruna Mihailescu	Revision
25 Nov 2023	1.2	-	Annual Review
23 Oct 2024	1.3	Miruna Mihailescu	Annual Review/ Updated regulatory framework to reflect recent changes in Curaçao's AML/CFT laws (NORUT and NOIS)/ Enhanced Risk-Based Approach (RBA) for high-risk customers and transactions/ Strengthened Know Your Customer (KYC) and Enhanced Due Diligence (EDD) procedures, including provisions for virtual assets and anonymous payment methods/ Incorporated the latest guidance from the Financial Action Task Force (FATF) and Caribbean Financial Action Task Force (CFATF)/ Revised ongoing monitoring and transaction reporting protocols. Added scope of application for employee roles. Updated Curaçao regulatory references. Included aptitude testing guidelines for new hires.
08 April 2025	1.4	Miruna Mihailescu	Comprehensive update to align with Curaçao's AML/CFT/CPF regulatory framework (January 2025). Changes include: – Replaced CDD threshold from €2,000 to XCG. 4,000 – Integrated Counter-Proliferation Financing (CPF) obligations throughout the policy – Added CPF definition to background and regulatory framework sections – Revised CRA, EWRA, and SOW/SOF sections to reflect CPF-specific risk factors and red flags – Added requirement to follow Curaçao's

			“Process for the Freezing of Resources” in CPF-related cases – Included CPF screening and triggers in KYC, CDD, ongoing monitoring, adverse media, and suspicious activity – Expanded high-risk indicators and denied onboarding criteria to include CPF exposure and WMD sanctions – Updated Section 2.2.1 with new GCB guidance on CPF, EWRA, sanctions, and compliance officer independence – Updated prohibited jurisdictions list in accordance with current Curaçao and international regulatory restrictions
--	--	--	---

Table of Contents

Abbreviations.....	5
1. Introduction	6
1.1 Background.....	6
1.2 The Policy	6
1.3 Licensing Objectives.....	7
2. Regulatory Framework.....	7
2.1 National Regulations.....	7
2.2 International Regulations.....	8
2.2.1 Curaçao Gaming Control Board (GCB) Guidelines	9
2.3 Definition of Money Laundering	10
2.4 Stages of Money Laundering	10
Placement.....	10
Layering	11
Integration	11
2.5 Funding of Terrorism.....	11
2.6 Counter-Proliferation Financing (CPF)	11
3.	11
2.7 The Financial Intelligence Unit.....	12
3. The Risk Based Approach	12
3.1 Overview	13
3.2 Risk Identification and Assessment	13
3.3 Risk Factors.....	13
3.3.1 Customer Risk	14
3.3.2 Geographic Risk.....	14
3.3.3 Product, Service and Transaction Risk	15
3. .3.5 Interface Risk	15
3.4 Mitigating Measures.....	15
3.5 Residual Risk.....	16
3.6 Review and Update of Risk Assessment	16
3.7 Scope of Application: Employees and Departments Subject to the Policy.....	17
4. The Customer Acceptance Policy	18
4.1 Denied on-boarding	18
4.2 Prohibited Jurisdictions.....	19
5. The Customer Risk Assessment (CRA).....	19
5.1 Medium-Risk customers	20
5.2 High-Risk customers:.....	20
5.3 Mandatory High-Risk customers	21

5.4	Not acceptable High-Risk customers	21
5.5	Periodical CRA review and ML/TF risk level reclassification	21
5.6	Recognizing Suspicious Activity	22
6.	KYC Procedure	22
6.1	Overview of KYC Measures	22
6.2	Standard Customer Due Diligence Measures (CDD).....	23
6.2.1	Identification and Verification of the Customer	23
6.2.2	Obtaining information on the Purpose and Intended Nature of the Business Relationship	24
6.2.3	On-Going Monitoring	24
6.2.4	Application, Extent and Timing of CDD Measures	25
6.3	Enhanced Due Diligence Measures (EDD).....	26
6.5	Politically Exposed Persons (PEP)	28
6.5.1	Member of the PEP family	29
6.5.2	Persons known as close associated of PEP	29
6.6	Adverse Media	30
6.7	Virtual Assets and Anonymous Payment Methods.....	32
6.7	Inability to complete CDD measures	32
7.	Reporting Procedure.....	33
7.2	Objective	33
7.3	Money Laundering Reporting Officer	33
7.4	Internal Reporting.....	34
7.5	Internal Control Processes	35
7.6	Internal Audit	36
8.	Employee Training	37
8.1	Initial Training.....	37
8.2	On-Going Training.....	37
9.	VETTING OF EMPLOYEES.....	38

Abbreviations

AML/CFT/CPF	Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing Policy
ML/FT	Money laundering and funding of terrorism
CPF	Counter-Proliferation Financing
EWRA	Enterprise-wide risk assessment
CRA	Customer Risk Assessment
CAP	Customer Acceptance Policy
RBA	Risk Based Approach
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
SDD	Simplified Due Diligence
EU	European Union
FATF	Financial Action Task Force
FIAU	Financial Intelligence Analysis Unit
CGCB	Curaçao Gaming Control Board
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
IAR	Internal Activity Report

1. Introduction

This Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing Policy (“AML/CFT/CPF Policy”) outlines the Company’s internal controls, procedures, and measures for detecting and deterring money laundering (ML), the financing of terrorism (FT), and the financing of the proliferation of weapons of mass destruction (CPF).

The Company is committed to identifying, mitigating, and reporting any activities that may contribute to ML, FT, or CPF, and to complying with the applicable national and international standards, including those issued by the Curaçao Gaming Control Board (GCB), the Financial Action Task Force (FATF), and the Caribbean Financial Action Task Force (CFATF). This Manual applies to all customers and operational 3rd party providers of the Company. All relevant officers and employees of the Company must be thoroughly familiar with it and strictly adhere to this Manual.

1.1 Background

Money laundering (ML), the financing of terrorism (FT), and the financing of the proliferation of weapons of mass destruction (CPF) are serious international threats to global security and financial integrity. These activities undermine the rule of law, enable organized crime, and pose systemic risks to the international financial system. It is essential that such threats are identified, mitigated, and reported using all available legal, technological, and operational means.

Prolific Trade N.V. fully recognizes its obligations under national and international law to implement robust Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing (CPF) measures. These obligations form a fundamental part of the Company’s licensing conditions and compliance commitments.

Accordingly, the Company maintains a zero-tolerance policy toward accepting any players whose funds are suspected to originate from unlawful activities or who may be involved in, or linked to, terrorist financing or proliferation-related networks. Prolific Trade N.V. is committed to implementing effective systems, controls, and governance frameworks to detect, prevent, and report any suspicious or unusual activity in accordance with Curaçao’s regulatory requirements, FATF Recommendations, and the guidance of the Curaçao Gaming Control Board (GCB).

1.2 The Policy

This Policy sets out the standards, controls and processes adhered to by Prolific Trade N.V., (hereinafter, “the “Company”), with its headquarters at Groot Kwartierweg 10, Curacao. Company Registration number 150731. This Policy is drafted in accordance with the legal, regulatory, and licensing obligations applicable to the Company.

1.3 Licensing Objectives

The Company will continually review and revise its policies and procedures considering relevant legislation, regulation, and industry guidance/learning, including guidance provided by the Curaçao Gaming Control Board (GCB) and any other applicable regulatory bodies to meet its licensing objectives.

The Company shall make sure to comply with all relevant AML and CTF obligations to which it is subject, in addition to any relevant industry codes of practice.

The Company is committed to keeping financial crime out of gambling, complying with all applicable laws, codes and guidance, identifying money laundering and terrorist risks to its business, designing and implementing policies and procedures to try and reduce those risks, monitoring and improving the effect and operation of these controls and keep records of all the policies and procedures and any amendments thereof.

2. Regulatory Framework

2.1 National Regulations

Pursuant to the National Ordinance 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:

- The National Ordinance on Money Laundering (P.B. 1993, no. 52).
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 2024, no.41(N.G.2017, no. 92) 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.
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 2024 no.41 (N.G. 2017, no. 99) 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
- The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70).
- 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); and
- 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.

Curaçao's regulatory framework for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) has undergone significant changes in recent years. The company remains committed to adhering to the most up-to-date regulations and guidance issued by Curaçao's regulatory authorities, including the Curaçao Gaming Control Board (GCB) and the Financial Intelligence Unit (FIU).

Curaçao's AML/CFT regulatory framework also includes obligations to counter the financing of the proliferation of weapons of mass destruction (CPF), in accordance with United Nations Security Council Resolutions and FATF Recommendation 7. Prolific Trade N.V. has integrated CPF into its internal risk assessments, customer due diligence procedures, and sanctions screening protocols.

Key applicable regulations include:

- **The National Ordinance on the Reporting of Unusual Transactions (NORUT):** This ordinance requires all reporting entities to notify the FIU of any suspicious transactions. The recent amendments (2023) strengthen the requirement for operators to enhance transaction monitoring and adopt more sophisticated suspicious activity detection mechanisms.
- **The National Ordinance on Identification of Clients when Rendering Services (NOIS):** Updated in 2023, this ordinance emphasizes stricter customer identification and verification processes, particularly for politically exposed persons (PEPs), high-risk jurisdictions, and customers involved in the use of anonymous financial instruments such as prepaid cards or cryptocurrencies.
- **The Sanctions National Decrees:** Amendments to sanctions decrees now include tighter restrictions on transactions involving individuals or entities linked to high-risk jurisdictions or those on updated sanctions lists as designated by the United Nations and the European Union.

In addition to these core regulations, Prolific Trade N.V. follows all relevant national decrees and laws addressing the identification, reporting, and prevention of money laundering and the financing of terrorism. The company also closely monitors ongoing regulatory changes in Curaçao to ensure compliance with evolving AML/CFT obligations.

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.

2.2 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 an 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.

Recent developments include:

- The FATF's updated guidance on **virtual assets and virtual asset service providers (VASPs)**, requiring enhanced due diligence measures and stricter transaction monitoring for customers involved in virtual currencies. Curaçao has transposed these requirements into national law, and Prolific Trade N.V. has adopted internal procedures to ensure compliance with these guidelines.
- Continuous updates from the **European Commission's list of high-risk third countries** with strategic deficiencies in their AML/CFT frameworks. Prolific Trade N.V. integrates this list into its **Customer Risk Assessment (CRA)** and enhanced due diligence (EDD) processes to mitigate risks from clients based in or connected to these jurisdictions.

2.2.1 Curaçao Gaming Control Board (GCB) Guidelines

In response to international regulatory developments and national initiatives, the GCB has issued new compliance guidelines for licensed entities.

These guidelines are designed to strengthen the overall effectiveness of Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing (CPF) frameworks across the gaming sector.

Key areas of emphasis include:

- Expanding the Enterprise-Wide Risk Assessment (EWRA):
Licensees must integrate risk indicators for virtual assets, digital payment methods, and CPF-related exposures (e.g., customers from jurisdictions or sectors known for proliferation-related risks).
- Customer Risk Assessments (CRA):
Operators are required to perform more frequent and risk-sensitive CRA updates, particularly for high-net-worth individuals, politically exposed persons (PEPs), and users of anonymous or cross-border payment mechanisms.
- Sanctions and CPF Monitoring:
Casinos must implement automated systems to screen and freeze accounts in line with UN, EU, and local sanctions frameworks and must adopt procedures aligned with Curaçao's "Process for the Freezing of Resources."

➤ Compliance Officer Requirements:

The Compliance Officer must operate independently from commercial functions, meet fit and proper criteria (including certification or experience thresholds), complete 10 hours of AML/CFT/CPF-specific training annually, and have unrestricted access to customer data and monitoring systems.

➤ Internal Reporting and Independent Audit Function:

The GCB requires licensees to maintain robust internal reporting mechanisms for suspicious activity and an independent audit function to periodically assess the effectiveness of the AML/CFT/CPF program, employee training, transaction monitoring, and recordkeeping practices.

These guidelines reflect the GCB's alignment with FATF Recommendations and are designed to ensure Curaçao-based operators remain compliant with international expectations and resilient to emerging threats.

2.3 Definition of Money Laundering

The below definition provides an exhaustive list of acts that constitute money laundering which are the following:

- (i) the conversion or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act or acts of participation in criminal activity, for the purpose of or purposes of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity;
- (ii) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;
- (iii) the acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;
- (iv) retention without reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

2.4 Stages of Money Laundering

Typically ML involves three stages:

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 banking system to start the process of ML. At this stage 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 any attention. Methods for a launderer to perform the placement stage include but are not limited to the following; cash deposit cheques, traveler's cheques, gambling, loan repayments, insurances on life policy's, deposits in amount of less than 10,000, mixing legitimate with illegitimate funds and asset purchasing.

Layering

At this stage the funds have managed to be deposited into the financial system; it is at this point layering is conducted with the aim to disguise ownership of the funds. This may happen by conducting transactions to different jurisdictions. This process is directed also to try to confuse any investigation and mislead the traceability of the funds. It is important to prevent layering by:

- Questioning suspicious transaction by asking the right questions to address the concern and avoid alerting the customer of any wrongdoing
- Monitoring of transaction and amounts

These are amongst a few methods combat layering

Integration

At this stage the money derived from criminal activity has been made to look legitimate and the funds are reintroduced into the financial system as legitimate funds. At this stage the launderer has been successful in laundering the funds. We are most likely to become involved in the integration stage but potentially could be involved in any stage.

2.5 Funding of Terrorism

The funding of terrorism is the process of making funds or other assets available to support, even indirectly the terrorist activities.

The funding of terrorist activity, terrorist organizations or individual terrorists may take place through funds derived from legitimate sources or from a combination of lawful and unlawful sources. Funding from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations. While the former may thrive on funds derived from legitimate sources, money laundering necessarily involves funds derived from illegal sources.

While the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds, and avails himself of the profits of crime, the terrorist's ultimate aim is not to generate profit from the fund-raising mechanisms but to obtain resources to support terrorist operations.

2.6 Counter-Proliferation Financing (CPF)

3.

The financing of the proliferation of weapons of mass destruction (WMDs) involves providing funds or financial services to support the development, production, stockpiling, acquisition, transportation, or use of nuclear, chemical, or biological weapons and related materials.

CPF poses a unique and serious threat to international peace and security. Proliferation of Weapons of Mass Destruction (PWMD) is

committed to identifying and mitigating risks related to the misuse of its platform for proliferation financing, and adheres to United Nations Security Council Resolutions (UNSCRs), FATF Recommendation 7, and Curaçao's "Process for the Freezing of Resources."

All customers are screened against applicable CPF-related sanctions lists, and any matches are escalated to the MLRO and reported to the FIU in line with applicable laws.

2.7 The Financial Intelligence Unit

The FIU is a mandatorily required national government agency, having a distinct legal personality, that handles financial intelligence.

FIU Curaçao became operational in 1997 as a part of the Ministry of Finance. FIU Curaçao acts as an independent buffer between the private sector and the criminal justice system, in the joint combat against money laundering and the financing of terrorism.

The FIU receives reports of suspicious transactions (STRs) from subject persons, supervisory and other competent authorities, as well as other persons or entities, analyzes them and disseminates the resulting intelligence to the relevant authorities, other competent authorities and foreign FIUs to combat ML/FT.

3. The Risk Based Approach

Current legislation in the EU where the Company conducts business, as well as Curaçao's AML/CFT/CPF regime, imposes compulsory operational compliance processes that must be satisfied in order to preserve the Company's licensing and regulatory standing.

The Company, its directors, and employees view the risks posed by non-compliance with Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing (CPF) obligations very seriously. Any suspected breach will be fully investigated and appropriate measures taken to mitigate risk and report suspicious activity in a timely manner.

Within the legal framework, there is flexibility to tailor internal controls, procedures, and tools that are proportionate to the risks associated with laundering criminal proceeds, financing terrorism, or facilitating the proliferation of weapons of mass destruction (WMDs). The risk-based approach begins with the understanding that most customers are not engaged in ML, FT, or CPF, but risk exposure must be evaluated systematically.

Accordingly, the Company identifies and assesses the ML/FT/CPF risks to which it is exposed and adopts appropriate policies, controls, and procedures to manage those risks effectively.

The risk prior to applying controls is defined as the inherent risk. The likelihood of a threat manifesting and its potential impact are assessed to determine the inherent risk level. The remaining risk following the application of mitigating controls is defined as the residual risk.

Therefore: Level of Inherent Risk – Mitigating Measures = Residual Risk

Risk is assessed through both:

1. an Enterprise-Wide Risk Assessment (EWRA), which incorporates specific risk factors related to AML, CFT, and CPF (e.g. exposure to high-risk jurisdictions, use of virtual assets, links to sanctioned entities); and

2. a Customer Risk Assessment (CRA) for each individual business relationship or occasional transaction.

CPF-specific risks, such as dealing with customers from jurisdictions under WMD-related sanctions or entities in sectors vulnerable to dual-use goods trafficking, are considered within both the EWRA and CRA frameworks.

The Company updates its EWRA whenever there is a significant change to its business structure, products, technology, customer profile, or the legal/regulatory environment. CRA updates are also triggered by changes in the customer's behavior or risk profile.

The EWRA is reviewed at least annually to ensure ongoing relevance and alignment with the latest guidance from the Curaçao Gaming Control Board (GCB), FATF, and national legislation.

3.1 Overview

Prolific Trade N.V. adopts a risk-based approach (RBA) to managing its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) obligations. This approach enables the company to identify, assess, and mitigate the risks of money laundering and terrorism financing in a manner that is proportionate to the risks posed by its business relationships and transactions, including those related to the financing of proliferation.

As required by both Curaçao's regulatory authorities and international standards (FATF and CFATF), the company tailors its policies and procedures to address these risks, focusing its resources where they are most needed. This ensures the effectiveness of our AML/CFT compliance program.

3.2 Risk Identification and Assessment

Prolific Trade N.V. identifies and assesses the money laundering (ML) and terrorist financing (TF) risks it is exposed to by conducting two primary forms of assessment:

1. **Enterprise-Wide Risk Assessment (EWRA):** This assessment evaluates the inherent and residual risks associated with the company's entire business operations. It considers factors such as customer base, products and services offered, transaction types, geographic exposure, and delivery channels. The EWRA is updated annually or when there are significant changes in the business environment or regulatory requirements.
2. **Customer Risk Assessment (CRA):** Every new and existing customer is subject to a risk assessment based on a variety of factors, including their identity, geographic location, source of funds, and transaction behaviors. The CRA is updated periodically and whenever there are changes in the customer's behavior or profile.

3.3 Risk Factors

The company considers several risk factors when assessing customers and transactions. These include as per the below.

3.3.1 Customer Risk

As part of our risk-based approach, the Company will carry out a risk assessment on our customers by considering the following issues:

- a. natural person customers that are PEP, member of PEP family or persons known to be close associates of PEP (mandatorily);
- b. players with a high level of expenses – the high level of expenses is established to include the customer in the VIP category;
- c. when the business relationship is conducted under uncommon circumstances;
- d. when players reside in geographical areas with a high-risk.
- e. the time that the business relationship with the customer has existed.
- f. mix of high volume, low volume, regular and occasional customers.
- g. the use of 3rd party payment methods.
- h. the unwillingness of the player to provide evidence of ID or any other requested information.

Additionally, the Company acknowledges the following:

- a. The majority of customers carry minimal risk of money laundering and will be employed with a regular source of income.
- b. There are a proportion of overseas clients where electronic CDD is difficult to achieve and our CDD will be commensurate with the State and where the customer resides.
- c. Formal risk assessments will be carried out when criteria changes or perceived risk is increased.

Factors such as the customer's status as a Politically Exposed Person (PEP), high-net-worth individual, or connection to high-risk jurisdictions may increase the risk.

Prolific Trade N.V. applies enhanced due diligence (EDD) to customers that present higher risks, such as PEPs, customers with complex ownership structures, and those using anonymous payment methods, including cryptocurrencies or prepaid cards.

3.3.2 Geographic Risk

The geographical risk is the risk posed to the Company by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of a customer have to be taken into account.

Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organizations operating within are to be considered as high risk. The opposite may also be taken into consideration and may therefore be considered as presenting a medium or low risk of ML/FT.

To assess the risk posed, the Company has to consider the following geographic risk:

- a. countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;

- b. countries identified by other credible sources as having serious deficiencies within their AML/CFT framework (example: FATF);
- c. countries subject to sanctions, embargoes or similar measures issued by international organizations, such as the United Nations Security Council or the European Union, including those related to the proliferation of weapons of mass destruction;
- d. countries identified by credible sources as providing funding or support for terrorist activities or that have terrorist organizations operating within them;
- e. countries identified as having significant levels of corruption or other criminal activity through credible sources, like the Corruption Perception Index compiled by Transparency International;
- f. countries that have shown a lack of willingness to comply with international tax transparency and information sharing standards (example: failure to adhere to or apply the Common Reporting Standard); and
- g. countries that fail to implement effective beneficial ownership transparency and availability measures and hence allow the legal entities or arrangements set up in that jurisdiction to be used as secretive vehicles and misused for ML/FT purposes.

3.3.3 Product, Service and Transaction Risk

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others.

The use of specific funding methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. This includes cash and other similar anonymous payment methods that do not always leave, or otherwise complicate, the funds' audit trail, and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual financial assets. The use by a customer of accounts held or cards issued in the name of third parties is also to be regarded as a high-risk factor. Conversely, where a customer transfers funds from a bank account or a card linked to a bank account held in his/her name with an institution established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions are themselves subject persons and one would expect that as part of their CDD obligations they would monitor on an on-going basis any account or card activity.

1.3.5 Interface Risk

The channels through which a business relationship is established and/ or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk. While situations where interaction with the customer takes place on a nonface to face basis no longer lead to the relationship automatically being considered as high- risk, interacting in this manner is still to be considered as a high-risk factor for risk assessment purposes unless technological measures and controls are adopted to address the heightened risk of identity fraud or impersonation.

3.4 Mitigating Measures

Prolific Trade N.V. mitigates these risks by applying a range of controls and procedures:

- **Customer Due Diligence (CDD):** Standard CDD is applied to all customers to verify their identity, determine the nature of their relationship with the company, and assess the risk they pose. Customers are required to provide valid identification documents and disclose their source of funds and wealth, where applicable.
- **Enhanced Due Diligence (EDD):** For customers or transactions deemed higher risk, additional due diligence measures are implemented, including verifying the customer's source of wealth, applying stricter ongoing monitoring, and gathering more in-depth documentation.
- **Ongoing Monitoring:** All customer transactions are continuously monitored to ensure that activity is consistent with the customer's profile. Any deviations or unusual patterns of behavior trigger a review, potentially leading to the implementation of further due diligence measures.
- **Automated Transaction Monitoring Systems:** The company's systems are configured to detect suspicious patterns in transaction volumes, frequency, and geographic connections. Alerts generated by these systems are investigated by the compliance team to ensure timely identification and reporting of suspicious activities.

Sanctions and Proliferation Screening: All customers and transactions are screened against relevant UN, EU, and local CPF-related sanctions lists. Any positive match triggers immediate escalation to the MLRO and implementation of the "Process for the Freezing of Resources" as required by Curaçao regulations.

3.5 Residual Risk

After applying mitigating measures, ensuring that significant ML/TF/CPF risks are thoroughly mitigated, any remaining risk is classified as residual risk. Prolific Trade N.V. maintains a policy of zero tolerance toward high residual risks, ensuring that significant ML/TF risks are thoroughly mitigated or that business relationships with such customers are terminated. The company documents all assessments and risk mitigation measures taken, ensuring that adequate records are kept in compliance with Curaçao's regulatory requirements.

3.6 Review and Update of Risk Assessment

The **Enterprise-Wide Risk Assessment (EWRA)** and **Customer Risk Assessment (CRA)** are reviewed:

- Annually, as part of the company's regular compliance review process.
- Whenever there are significant changes in the regulatory environment, such as new guidance from the Curaçao Gaming Control Board (GCB), the FIU, or international bodies like FATF — including updates on proliferation financing and targeted financial sanctions. When new products or services are introduced, or significant changes occur in the company's operational or geographic exposure.

This ensures that the risk management framework remains dynamic and responsive to new and evolving threats in the industry.

3.7 Scope of Application: Employees and Departments Subject to the Policy

This AML/CFT/CPF Policy applies to all departments, employees, and contractors involved in Prolific Trade N.V.'s operations, with specific responsibilities based on role and level of exposure to potential AML/CFT risks.

Key areas of responsibility include:

- **Compliance Department:** Responsible for the overall management, implementation, and monitoring of the AML/CFT Policy. Compliance Officers, the Money Laundering Reporting Officer (MLRO), and other compliance staff ensure the policy is followed across the organization.
- **Customer Support and Customer Service:** Engages directly with players and is responsible for adhering to customer due diligence procedures, identifying suspicious behaviors, and escalating potential AML/CFT issues.
- **Fraud and Payments Department:** Manages all customer transactions, monitors payment activities, and identifies transaction patterns to prevent financial crimes. The Finance team is integral to spotting irregularities and reporting them for further review.
- **VIP Management:** Manages high-value or VIP clients and requires strict adherence to enhanced due diligence measures, as VIP clients may pose higher risk levels. Account managers, VIP managers, and Marketing staff must follow the policy guidelines for monitoring high-risk clients.
- **IT and Security Department:** Provides technical support to AML/CFT monitoring systems, maintains the security and functionality of geo-blocking, transaction monitoring, and reporting systems, and ensures data integrity for compliance purposes.
- **Internal Audit:** Conducts periodic reviews to test the effectiveness of AML/CFT policies and procedures and ensures that all compliance measures are up-to-date and consistently implemented.
- **Senior Management and Executive Roles:** Ensures overall accountability for AML/CFT compliance, supports a culture of compliance within the organization, and allocates sufficient resources to maintain an effective AML/CFT program.

Each department and employee are required to understand their responsibilities under this policy and undergo relevant training to ensure consistent compliance with AML/CFT regulations. Any breaches or failures to adhere to this policy may result in disciplinary action in accordance with company protocols.

4. The Customer Acceptance Policy

relationship or an occasional transaction being considered as presenting a low, medium or high risk of ML/FT, the level of DD measures including ongoing monitoring to be applied in their relation and under what circumstances the Company will decline to service a customer.

It is pertinent that the Customer Acceptance Policy is followed at all times, due to the company being a subject person. The Customer Acceptance Policy provides a better understanding of those customers the company is engaging with and those customers who, due to prohibited actions, risk awareness, sanctions or who display characteristics described in the CRA the company will not engage in any activity with.

The information collected to draw up the CRA will formulate the customer's profile. Based on the CRA, the Company can then assess the proper level of DD to address the identified risks.

4.1 Denied on-boarding

The following categories of players will not be accepted at registration/post registration checks:

- Players residing in non-operating jurisdictions
- IP login registered in a non- operating jurisdiction
- International sanctioned individuals
- Players under the age of 18
- Players subject to targeted financial sanctions (e.g., UN/EU listings for terrorist financing or the proliferation of weapons of mass destruction).
- Players residing in jurisdictions known for proliferation financing risks, or identified in relation to WMD-related export controls or dual-use goods trafficking.

Where a CPF-related sanction match is identified, the Company follows Curaçao's "Process for the Freezing of Resources" and reports immediately to the FIU. In such cases, onboarding is denied, and any associated assets or accounts are frozen in accordance with applicable law.

As part of the due diligence process, adverse Media checks are conducted on the player database. There may be instances where a previous criminal record (conviction) reported in the media may create an unwarranted risk appetite for the company. (Example: convicted former credit card fraudster). These cases are escalated to the MLRO for assessment and a decision may be taken to terminate the relationship with the said client.

Adverse media sources include:

- Traditional news sources and Media.
- Databases of International Organizations.
- Blogs and web articles – including websites that publish issues involving corruption, rackets and financial fraud.
- Social media and internet forums – examples include Reddit forums of fraudulent organizations and news searches on Facebook and Twitter.

A business decision may be made to retain the player relationship. In such instances the rationale is to document the detailed reasons why the relationship should be retained.

The additional recommendations will be owned and actioned directly by the team and the MLRO will be conducting additional checks on the requested monitoring activity to ensure that the controls have been adequately implemented and retained.

4.2 Prohibited Jurisdictions

Prolific Trade N.V. is committed to complying with international and national regulations by ensuring that its services are not available in prohibited jurisdictions. As part of its commitment to regulatory compliance and risk management, Prolific Trade N.V. enforces geo-blocking measures to prevent access to its services from specific jurisdictions where online gambling activities are restricted or prohibited.

The following jurisdictions are currently restricted and prohibited from accessing Prolific Trade N.V.'s services:

- The Netherlands
- Aruba
- Bonaire
- Curaçao
- Saba
- St. Eustatius
- St. Maarten
- Australia
- Belgium
- France
- Singapore
- Spain
- United Kingdom
- United States

Geo-blocking technology is implemented to ensure that users from these jurisdictions cannot access Prolific Trade N.V.'s platforms. Additionally, the company conducts periodic reviews to update the list of prohibited jurisdictions in line with changing regulatory requirements and legal standards.

Prolific Trade N.V. reserves the right to restrict or terminate accounts found to be accessing the platform from any prohibited jurisdiction, in accordance with applicable laws and internal policies.

5. The Customer Risk Assessment (CRA)

Prolific Trade N.V. is required to adopt a risk-based approach by applying a customer risk assessment (CRA) in dealing with the Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (CPF) risks posed by its customers, including recognizing the existence of risks, undertaking a risk assessment, and implementing systems and strategies to manage and mitigate the identified risks.

The relation between Prolific Trade N.V. and its customer is considered to be a “business relationship” as Prolific Trade N.V. is opening an account for its customer when providing online services, asking the customer to accept the T&C and this relationship is expected to have an element of duration.

In the case of a business relationship, the CRA is carried out not later than thirty (30) days .from when the pre-established threshold of **XCG. 4,000** (or its foreign currency equivalent) has been met

Through the BRA, the company is aware of the risks in the product and service offered. Having an understanding of the risks that may arise from the above factors, the company has developed sound risk management practices to assist the officers involved in the process and tools to

manage the risk posed by the threats of ML, FT or other illicit activity. The level of due diligence required is dynamic and depends on the actions and behavioral patterns of the Client.

The company has a twofold approach to the CRA:

1. Risk assessment: The risk assessment is in place to indicate behavioral patterns and pertinent information emanating from the Client.

2. Transactional triggers: These triggers are serious instances which give rise to possible ML/FT therefore all transactional triggers require an internal analysis of the action.

The risk score of the Client shall reflect the Client's current position whether at onboarding or ongoing monitoring. The Client is assigned a score which determines if the Client is Low, Medium or High Risk. Risks may be cleared following a manual assessment and/or the Client providing sufficient information to clarify any alerts generated by the system, the risk assessment can only be re-evaluated by the MLRO, with a written rationale to be left on the Client's account. Any alerts cleared shall be recorded but shall not affect the risk score of the Client. The risk score can be overwritten if the AMLCO officer has reasonable doubts. For example if an officer would like to place a low risk customer as a high risk, if reasonable justification is provided, they can do so.

5.1 Medium-Risk customers

If none of the below risk indicators are met, the Customer is classified as Medium-Risk.

5.2 High-Risk customers:

Each of following risk indicators shall increase 1 point the BRA residual value of the CRA and whenever the value amounts 8 points or more, the Customer is classified as High-Risk, and EDD measures are applied:

- the player was subject of an STR;
- the player is suspected of using multiple identities or multiple Online accounts;
- the player is suspected of playing on behalf of a different person;
- the player was subject of a suspension of the account for fraud investigations;
- the player is associated with persons known for committing crimes;
- the player makes deposits that do not turnover at least once through gambling activity;
- When the player conducts payments with anonymous instruments (prepaid cards, vouchers etc.);
- When the player deposits more than EURO 5,000, by a single or linked transactions within 30 days
- When the player is carrying out large one-off transactions;
- Large transactions that have no apparent economic or visible lawful purpose;
- Transactions with no apparent logical, economic or legal purpose;
- Unusual patterns of the transactions;
- Complex or unusually large transactions;

- When the player transacts in patterns that are not in line with their profile;
- A transaction that is likely to be related to ML/FT;
- When there are doubts as to whether the payment method used to fund the gaming account in fact doesn't belong to the player
- SOW/SOF:
 - Situations where the source of funds cannot be easily verified or where the audit trail has been broken/layered;
 - Frequent and unexplained movement of accounts to different entities as established from the SOW/F;
 - Clients who appear not to have a regular job are receiving regular transfers and will not provide information on the source of funds.

5.3 Mandatory High-Risk customers

If any of the following risk indicators are met, the EDD measures applied are escalated to the MLRO that conducts extensive CRA and requests approval from the Senior Manager for establishing/continuing or rejecting/terminating the business relationship with the Customer:

- The Customer is PEP (including the family members and the persons known as PEP associates);
- The Customer is associated with non-reputable jurisdictions, identified by the European Commission (countries which grant financing or support for terrorist activities or on the territory of which there are present terrorist organizations; countries having a high level of corruption or of other criminal activities; countries which do not have actual systems to fight against money laundering/terrorist financing; countries subject to certain sanctions, embargoes, or similar measures);
- The Customer is associated with jurisdictions or entities involved in the proliferation of weapons of mass destruction or subject to UN/EU CPF-related sanctions (e.g., dual-use goods traders, entities flagged in FATF public statements).

5.4 Not acceptable High-Risk customers

If the Customer is subject to international sanctions, the CDD/EDD measures applied by ARPs are escalated to MLRO for validating it and, if true positive, for requesting ARP to enforce rejecting/terminating the business relationship with the Customer. In cases of CPF-related sanction matches, the MLRO shall ensure compliance with Curaçao's "Process for the Freezing of Resources," and all related assets are frozen and reported to the FIU immediately.

Subsequently, MLRO shall fill a report with the Sanctions Monitoring Board regarding the not-acceptable High-Risk customer.

5.5 Periodical CRA review and ML/TF risk level reclassification

The initial CRA will have to be revised at a later stage of the business relationship, on a risk- based approach, as follows:

- Annually, for High-Risk customers;
- Every 24 months, for Medium-Risk customers.

The customer risk is re-evaluated when reviewing the KYC information, which may lead to:

- a. Keeping the customer in the same risk category – decision taken by the AML department, which does not need a MLRO decision;

- b. Escalating the risk category – decision taken by the AML department, which does not need a MLRO decision;
- c. Lowering the risk category – decision taken by the MLRO.

5.6 Recognizing Suspicious Activity

The incidence of one of the following suspicious indicators will be notified by the AML Dept to MLRO for, when MLRO assess and if confirmed the ML/FT suspicious, issuing a STR and submitting to the FIU:

- The player does not cooperate in the carrying out of DD.
- The player attempts to register more than one account with the Company.
- The player deposits more than EURO 5,000 /24h by means of multiple prepaid cards.
- The player deposits funds well in excess of what is required to sustain usual betting patterns.
- The player makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- The player makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- The player enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- The player carries out transactions which seem to be disproportionate when seen in the context of what is known about the customer's wealth, income, or financial situation.
- The player seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- The player displays suspicious behavior in playing games that are considered as high- risk.
- The player is associated with an entity flagged in relation to weapons proliferation, WMD-related programs, or dual-use goods trading.
- The player attempts to transact with countries under targeted financial sanctions for proliferation-related activity (e.g., DPRK, Iran).
- The player is linked to export-controlled sectors (e.g., chemicals, aerospace) without a clear explanation.

The reporting to the FIU is carried out in accordance with the legal provisions, transposed internally through the Reporting Procedure.

6. KYC Procedure

6.1 Overview of KYC Measures

Prolific Trade N.V. applies a risk-based KYC framework to prevent misuse of its services for money laundering (ML), terrorist financing (TF), or the financing of the proliferation of weapons of mass destruction. The primary purpose of KYC is to identify customers, verify their identity, and assess the risks they pose based on the nature of their transactions and business relationships with the company. The extent of KYC measures depends on the level of risk identified during the customer risk assessment (CRA).

6.2 Standard Customer Due Diligence Measures (CDD)

6.2.1 Identification and Verification of the Customer

- a. In accordance with Curaçao's latest regulatory requirements, Prolific Trade N.V. collects and verifies the following information from each customer: name and surname
- b. permanent residential address
- c. date of birth
- d. place of birth
- e. nationality
- f. tax reference number

The company requires valid government-issued identification documents for verification. In cases where customers cannot provide standard identification, alternative verification measures, such as reliable electronic sources, are used, provided they meet the required regulatory standards.

Additional Requirement for High-Risk Customers: For high-risk customers, including Politically Exposed Persons (PEPs) or customers transacting from high-risk jurisdictions, Prolific Trade N.V. collects further documentation to verify their identity, source of funds, and source of wealth.

Prolific Trade N.V. has systems in place, (including systems implemented for on-going monitoring purposes), which enable it to corroborate the location or other personal details of the customer. When such systems detect inconsistencies in the personal information provided by the customer, the Company's identification and verification processes should consider whether additional identification and verification measures are required.

Verification of the Customer is carried out by Prolific Trade N.V. by using data, documents or information obtained from an independent and reliable source, as documentary electronic sources.

The verification of identity through Documentary Sources is carried out by referring to a valid government-issued document containing photographic evidence of the customer's identity (e.g., passport, identity card, residence permit, driving license etc.). When using documentary sources for verification purposes, the Company is to ensure as much as possible through specialized software that the documents obtained are authentic or reproduce authentic ones.

All customers are screened against sanctions lists published by the UN, EU, and local Curaçao authorities, including lists related to terrorist financing and the proliferation of weapons of mass destruction (WMDs).

Where a customer match is found in a CPF-related list, the Company follows Curaçao's "Process for the Freezing of Resources," immediately reports to the FIU, and blocks access to services and accounts.

Prolific Trade N.V. will make sure that customers are registering an account to play and transact on their behalf, by including specific wording in the T&C that a registering player must explicitly accept, together with a declaration in the form of a tick box that a player is registering to play on his/her own behalf.

Prolific Trade N.V. will not merely rely on the said declaration, but its ongoing procedures allow for the detection of possible instances where the player is in fact playing on behalf of third parties.

Also, Prolific Trade N.V. will decline to enter into business relations with one or more players funded by a syndicate.

6.2.2 Obtaining information on the Purpose and Intended Nature of the Business Relationship

For all customers, Prolific Trade N.V. seeks to understand the purpose and intended nature of the business relationship by gathering information on:

- The type of gaming or financial services they intend to use.
- The expected volume and frequency of transactions.
- The geographical regions involved in their transactions.

When dealing with higher-risk customers or transactions, the company requires more detailed information on the customer's source of wealth, especially for those involved in large or unusual transactions. For high-risk customers or transactions, particularly those involving cross-border payments or customers from proliferation-sensitive jurisdictions, additional verification steps may include industry-sector inquiries, adverse media screening for proliferation financing, and evidence of legitimate business activity.

As within the context of the remote gaming sector, the purpose behind the opening of a gaming account is quite self-evident and, limited to this aspect, Prolific Trade N.V. is not required by law and will not obtain any additional information from its customers.

However, where the risk is not high, Prolific Trade N.V. will collect a declaration from the customer with some details (e.g., nature of employment/business, usual annual salary etc.) to establish a customer's source of wealth as well as the expected level of activity.

In developing a customer business and risk profile, Prolific Trade N.V. may also consider using statistical data to gauge a customer's activity rather than collect source of wealth information, by using data collected from official economic indicators such as average national income, average disposable income etc. issued by national public bodies or reputable financial institutions.

6.2.3 On-Going Monitoring

On-going monitoring is a critical part of Prolific Trade N.V.'s CDD process. The company continuously monitors customer activity to ensure that it is consistent with the customer's profile and the expected behavior established during the initial risk assessment.

In carrying out an on-going monitoring of a business relationship, Prolific Trade N.V. is ensuring that the documents, data, or information held are kept up-to-date, and will apply the following measures:

- a. Request and obtain fresh identification documents when the expiry date of identification documents held on file is reached
- b. Question the data and information already in Prolific Trade N.V. possession whenever any inconsistencies arise
- c. Where documents are not expired and in the absence of any inconsistencies as referred to hereinabove, periodical review and where necessary update the said data and information from time to time on a risk-sensitive basis
- d. Regularly reviewing transaction patterns and comparing them to the customer's established profile.
- e. Updating customer information, such as identification documents or proof of address, when changes occur or as part of periodic reviews.
- f. Flagging any unusual or suspicious activities for further investigation by the compliance team.

Additional indicators triggering review may include:

- Transactions involving jurisdictions listed by FATF or the UN for proliferation-related concerns.
- Use of payment processors or intermediaries based in countries with weak export controls or known dual-use goods trafficking.
- Changes in customer behavior involving sectors vulnerable to proliferation (e.g., chemicals, aerospace, defense).
- Receipt of funds from or sending to entities flagged for WMD-related activities.
- Repeated use of third-party or anonymous payment methods from high-risk countries.

Transactions or behaviors that deviate from the customer's expected activity may trigger a review of the customer's risk profile and potentially escalate to Enhanced Due Diligence (EDD).

Prolific Trade N.V. shall determine on a risk sensitive basis whether any new information needs to be verified or whether changes are so substantial as to require the carrying out of its customer risk assessment and/or its CDD afresh.

6.2.4 Application, Extent and Timing of CDD Measures

Simultaneously with the opening of an online account and prior to the Customer's deposits reaching the threshold of **XCG 4,000 (or its foreign currency equivalent)**, Prolific Trade N.V. applies a minimum level of CDD measures that consists of identifying (but not verifying the identity of) the customer by collecting the personal data as referred to in Section 6.2.1.

Moreover, before reaching the threshold of **XCG. 4,000 (or its foreign currency equivalent)...**", Prolific N.V. has systems in place which allow the application of on-going monitoring, to:

- a) determine the moment in time when the XCG. 4,000 threshold is met;
- b) prevent the player to avoid the application of CDD measures when reaching the XCG 4,000 threshold by
 - linking all accounts held by a customer with Prolific Trade N.V., irrespective of the platform used (if it falls under Prolific N.V.) or the brand under which the customer makes use of the Prolific N.V.'s services;
 - detecting the opening of accounts by the same customer while using third party identities, be they real or fake
- c) deny the opening of an account by a person who has inputted manifestly false details
- d) detect instances which give rise to a suspicion of ML/FT as prescribed above in Section 5.6

Given the limited nature of on-going monitoring to be carried out at this stage, the Company is not conducting a CRA on the said Customer.

The CRA is carried out and the remaining CDD obligations (as referred to in Section 6.2.1) are applied when:

- a. the XCG. 4,000 threshold is reached by the funds deposited by the Customer onto an online account, whether in a single transaction or several related transactions, calculated on a daily basis taking into account all deposits performed by a customer since the establishment of the business relationship.
- b. inconsistencies are noticed between the information provided by the Customer and any other information that might be acquired through interaction with the Customer.
- c. there are suspicions of ML/FT, regardless of the incidence of provisions derogating from the obligation to apply the measures of CDD established by Law and the value of the operation.

In carrying out the CDD measures, customers may be allowed to continue using their gaming

account while Prolific N.V. obtains any necessary information from the customer concerned.

However, until Prolific Trade N.V. obtains the necessary information and documentation from the customer to meet its CDD obligations, the customer is not to be allowed to conduct any withdrawals from the account independently of the amount involved.

Moreover, if following the lapse of thirty (30) days from when the XCG 4,000 threshold is met, the customer has not made the requested information and documentation available, Prolific Trade N.V. shall terminate the relationship.

6.3 Enhanced Due Diligence Measures (EDD)

For high-risk customers or transactions, such as those involving politically exposed persons (PEPs), virtual assets, or customers from high-risk jurisdictions, Prolific Trade N.V. applies Enhanced Due Diligence (EDD) measures. These measures are more thorough than standard CDD and aim to mitigate the increased risks associated with these customers.

The EDD measures to be applied whenever Prolific Trade N.V. identifies any High-Risk acceptable players may include:

- a. collecting more detailed information on the source of wealth and source of funds to be used in relation with the Company
- b. any additional measures deemed necessary to mitigate the risks identified through the customer risk assessment, including additional measures to ascertain and verify the identity of the customer.
- c. requesting to be provided with a clear image of the card showing the name of the cardholder or in the case of an e-wallet account, a screenshot of the account showing the name and the email address of the account holder (for when multiple payment methods are being used by the same Customer or there are doubts as to whether the payment method used to fund the gaming account in fact belongs to the customer).
- d. Verifying the legitimacy of the customer's financial activities by reviewing financial statements, business records, or other supporting documents.
- e. Applying more frequent and in-depth monitoring of transactions, particularly those involving large sums or transfers across multiple jurisdictions.

For customers utilizing anonymous or high-risk payment methods, such as prepaid cards, vouchers, or cryptocurrencies, the company implements stricter monitoring measures to prevent money laundering and terrorist financing.

6.4 Source of Funds and Wealth

The Source of Funds (SOF) is how the funds used for a particular transaction (or future transactions) were generated, and the Source of Wealth (SOW) describes the activities that have generated the total net worth of a customer.

We are not obligated to interrogate all Customers about their financial history, but we are required to take reasonable steps to ensure that the transactions are consistent with our knowledge and profile of the Customer. This is part of the ongoing monitoring process.

SOF/SOW may be requested at any point in the business relationship depending on the CRA; for example Customers may be asked to provide SOF/SOW in the following circumstances:

- Due to ML/FT concerns on the account, the Customer is deemed to be Medium or High risk following a CRA;
- Adverse Media Hits, especially regarding Fraud or Financial Crime;
- If a Client generates income through trading of financial assets;
- Clients who are from or suspected of financing their activity via funds originating from high-risk jurisdictions, including those associated with terrorist activity or the proliferation of weapons of mass destruction (CPF). If following the request for documentation, it is found that the Client's source of wealth or funds is coming from a high-risk or non-reputable jurisdictions, such Clients are to be immediately brought to the attention of the MLRO;
- Suspicion or Confirmation of a Customer's bankruptcy or tax avoidance purposes;
- The level of the Customer's activity is inconsistent with their profile;
- Suspicion raised from KYC received eg fake documents or transactions from bank statement.
- A suspicion that a customer's activity is funded via a third party.
- The Customer deposits more than Euro 15,000 into their custodial wallet in a Calendar 365-day period.
- A manual review of the account is conducted if there is a mismatch on the SOW/F information provided by the Customer and background research. SOW/F verification is required to corroborate the information provided by the Customer. Manual review may also be triggered by CPF-related red flags such as links to companies in proliferation-sensitive industries, unexplained funding from export-controlled jurisdictions, or sanctions exposure.

Our three-step process for establishing source of wealth is as follows:

Step one: Obtain information on the customer's net worth

- Indication of a customer's net worth is established through relevant representations obtained from the customer.
- It is not necessary to obtain the exact amount and might be impractical to do so.

Step two: Obtain information on the sources of the customer's net worth

- With the customer's net worth established, the Company obtains the information on where it came from (inheritance, employment, business, investment or company's profits generated from legitimate business and commercial activities).
- Generally, no single source is likely to account for the total value of net worth; but categories are likely to be few and generally well understood. The level of detail is based on the customer's risk assessment (reasonable measure).

Step Three: Verify the information on a risk sensitive basis

Source of wealth documents need to be from a reliable, independent source that confirms how the wealth was generated. SOW can be established through a combination of sources, such as: publicly available property registers, past transactions, internet searches, evidence of title, copies of trust deeds, documents confirming salary, tax returns and bank statements.

Examples of sources of wealth and proof of wealth documents: Inheritance of a family fortune:

- Name of deceased

- Relationship to client
- Date of death
- Date it was received
- Entire amount
- Solicitor's details
- Tax clearance documents
- Employment:
- Nature of employer's business
- Name and address of the employer
- Annual salary and bonuses for the last couple of year
- Last month/recent pay slip
- Confirmation from the employer of annual salary
- Latest accounts or tax declaration if self employed

Business gain from a company sale:

- Copy of the contract of sale
- Internet research of Company Registry
- Name and Address of Company
- Total sales price
- Clients' share participation
- Nature of business
- Sale date and the receipt of funds
- Media coverage

For high-risk customers or those making large or complex transactions, Prolific Trade N.V. requires proof of the source of funds (SOF) and source of wealth (SOW) as part of its EDD measures. This may include:

- Proof of employment or business ownership.
- Financial statements or tax returns.
- Documents related to property ownership, investments, or inheritance.

Customers who fail to provide satisfactory SOF or SOW documentation will be subject to further scrutiny, and their accounts may be restricted or closed if the risks cannot be mitigated.

Where CPF-related risk factors are identified, the Company verifies the legitimacy of the source of funds and wealth with heightened scrutiny, ensuring screening against UN, EU, and national sanctions lists, and escalating any matches in line with Curaçao's "Process for the Freezing of Resources.

6.5 Politically Exposed Persons (PEP)

A Politically Exposed Person is someone who has been entrusted with a prominent public function, such as a senior political figure and indicated in the definitions above. Individuals closely related to this person, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a ML risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

If a PEP or close associate is found, the Client will be escalated to the MLRO, who will then notify the CEO of the same. The Company will conduct enhanced due diligence in relation to the PEP or close associate.

The following is an exhaustive list of public functions which are considered as prominent public functions and would therefore render the holder thereof a PEP. This comprises:

- i. Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- ii. Members of Parliament or similar legislative bodies.
- iii. Members of the governing bodies of political parties.
- iv. Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances.
- v. Members of courts of auditors, or of the boards of central banks.
- vi. Ambassadors, charge d'affaires and other high-ranking officers in the armed forces.
- vii. Members of the administrative, management or supervisory boards of state-owned enterprises.

The Company will consider to be a PEP any natural persons exercising or who used to exercise important public positions during the last 12 months. After the expiry of a period of one year from the date on which the PEP ceased to hold any important public position, the Company will no longer consider that person to be a PEP.

6.5.1 Member of the PEP family

The family members of a person exposed to the public are:

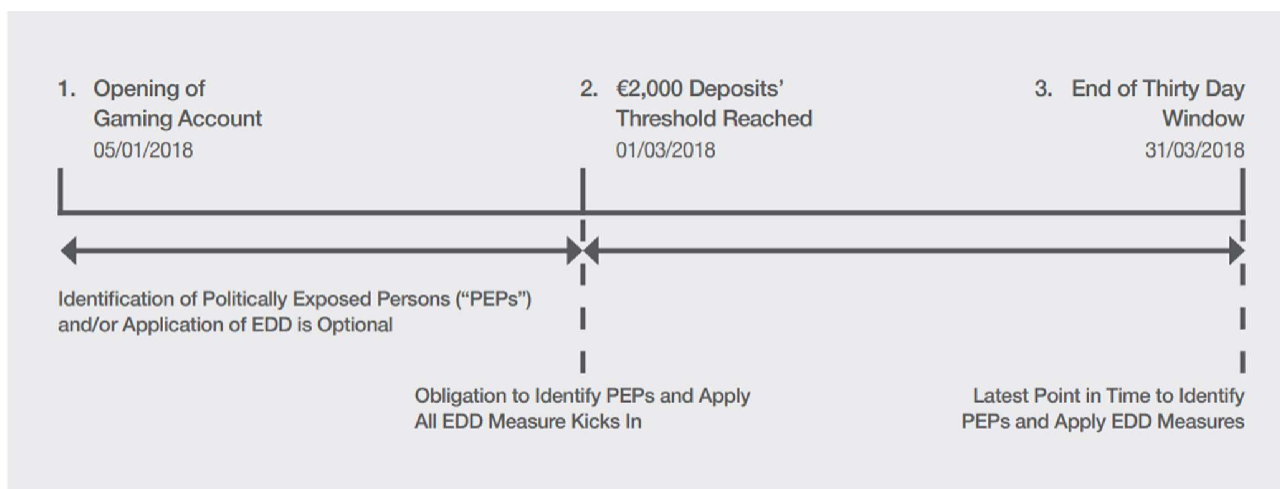
- a. the spouse of the PEP or their concubine / the person with whom they are in relations similar to those of the spouses
- b. children and their spouses or concubines, the persons with whom the children are in relations similar to those of the spouses
- c. Parents

6.5.2 Persons known as close associated of PEP

The persons known as close associates of PEP are:

- a. natural persons known as the beneficial owners of a legal person, of an entity without legal personality or a similar legal arrangement similar to them together with a PEP or as having any other close business relationship with a PEP.
- b. natural persons who are the single beneficial owners of a legal person, of an entity without legal personality or of a similar legal construction, known to be established for the de facto benefit of a PEP.

For PEPs, the following Timeline will be applied:



6.6 Adverse Media

Adverse Media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, Terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Adverse Media Screening is to be conducted when establishing a business relationship with a Customer. Instances where a Customer is connected to Adverse Media, will be evaluated prior to granting a business relationship.

When analyzing Adverse Media hits, we are looking at individuals that are both convicted and not fully convicted, meaning; allegations, cases under investigation pending the legal procedure, wanted individuals and any intelligence which gives rise to knowledge or suspicion that the Customer is involved with ML/TF.

Adverse Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offense raise concerns, they shall be raised with the MLRO.

Adverse Media is categorized 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 that may be covered in both traditional and emerging media.

ii) Violence

- Violence involving Customers directly, or carried out on their behalf, may generate significantly different types of adverse media, especially when 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 and includes fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offense and, while the majority of cases involve improper financial gain, it may also involve property or immigration.

v) Narcotics

- Narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offenses 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 offenses 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 offenses 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 offenses 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 offense, trafficking is often related to other offenses, 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 offenses, including ML and cybercrime.

xi) Proliferation Financing / WMD Risk

- Adverse media may include references to individuals or entities involved in the financing, manufacture, export, or trafficking of weapons of mass destruction (WMDs) or dual-use goods.
- This includes links to front companies, defense contractors in high-risk jurisdictions, violations of export controls, or involvement in networks named by the United Nations Security Council or FATF for proliferation-related risks.

Any of the offenses indicated above, whether convicted or alleged, shall be evaluated and terminated accordingly if the media is deemed to be a positive match. This includes offenses or media references related to CPF typologies or WMD-related proliferation risks.

6.7 Virtual Assets and Anonymous Payment Methods

Prolific Trade N.V. acknowledges the increased risks posed by virtual assets (e.g., cryptocurrencies) and anonymous payment methods. To address these risks, the company applies additional verification and monitoring procedures:

- **Virtual Asset Service Providers (VASPs):** For customers engaging in transactions involving virtual assets, Prolific Trade N.V. ensures compliance with FATF's updated guidelines on VASPs, which mandate stricter due diligence measures and closer monitoring of transactions.
- **Anonymous Payment Methods:** For customers using prepaid cards, vouchers, or other anonymous instruments, Prolific Trade N.V. requires additional verification steps, such as obtaining documentation to confirm the ownership of the payment method.

All transactions involving virtual assets or anonymous payment methods are flagged for enhanced monitoring, and any suspicious activity is immediately reported to the compliance team for further investigation.

6.7 Inability to complete CDD measures

When the Customer will not be willing to provide with the necessary information or documentation and thus the Company is not able to apply CDD, Prolific N.V. will terminate its business relationship with the Customer by not allowing any activity of any kind on the account held in the customer's name or provide any other service to the customer.

Prolific Trade N.V. may decide to either close the account or to keep it blocked and suspended in its entirety. In the latter case, Prolific Trade N.V. is to ensure that the account has a NIL balance at the time it is blocked and suspended, with any funds standing to the credit of any such account being disposed of as set out hereunder.

The reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT.

If there are grounds to suspect ML/FT, the MLRO will submit a Suspicious Transaction Report ("STR") to the FIU, at the earliest possible moment in time, even though the thirty days allowed for the collection of the necessary CDD information or documentation may not have lapsed or the customer may not have approached Prolific Trade N.V. to carry out any further transactions.

Where there are no grounds to suspect ML/FT or the transaction has not been suspended by the FIU or by operation of the law, nor is there an attachment or freezing order, Prolific Trade N.V. would have no reason rooted in the AML/CFT regime justifying the retention of any such funds.

Thus, where funds are to be remitted back, Prolific Trade N.V. shall:

- a. Consider whether there is any other legal impediment to the remittance of the funds
- b. Remit the funds to the same source through the same channels used to receive the funds

In the event Prolific Trade N.V. is unable to remit the funds to the same source through the same channels, it will inevitably have to request fresh instructions from the customer.

In the event that these instructions give rise to a suspicion on the part of the Prolific Trade N.V. the MLRO should submit a STR and suspend the remittance pending the FIU expressing its opposition or otherwise to the said transaction.

All the records of the verifications carried out must be documented in writing and will be made available upon request of the relevant authorities (the FIU, MGA etc.).

7. Reporting Procedure

7.1 Purpose

The main purpose of the Reporting Procedure is to report any knowledge, suspicion, or reasonable grounds to suspect ML/FT that funds or property used in relation to our Company are the proceeds of criminal activity. References to knowledge or suspicion of ML/FT are to be deemed as also including reasonable grounds for suspicion or to an attempt to carry out a transaction or activity related to proceeds of criminal activity or funding of terrorism.

7.2 Objective

This Reporting Procedure regulates the measures applied by the Prolific N.V.'s Money Laundering Reporting Officer hereinafter referred to as „MLRO”).

The Company's MLRO is Miruna Mihailescu, miruna.mihailescu@blaze.com, mobile +35699636396.

7.3 Money Laundering Reporting Officer

The MLRO's main responsibility is to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up the same by filing a STR/SAR with the FIU. The MLRO is also the main contact point with the FIU, and the MLRO is to act as the main channel through which any communications with the FIU are to be conducted.

MLRO Responsibilities include as follows:

- a. To prepare and file reports with the FIU based on the information obtained from Prolific Trade N.V. employees who have AML/CFT responsibilities on the transactions on which they have knowledge or suspicions on the money laundering or terrorist financing activities;
- b. To provide Prolific Trade N.V.'s management with AML advice and expert knowledge in handling the betting activity to minimize Prolific Trade N.V.s exposure to money laundering and terrorist financing risks;
- c. To prepare the AML Policy and subsequent procedures on accepting customers and send it to Prolific Trade N.V.'s management for review and approval purposes;
- d. To support Prolific Trade N.V.'s internal departments in terms of transposing the AML policy and procedures in their own instructions and implement AML controls;
- e. To monitor and assess the correct and efficient implementation of policies, practices, measures, procedures, and controls. Should he/she identify deficiencies and/or vulnerabilities in the implementation of the practices, measures, procedures, and necessary controls, to offer proper guidance for corrective actions and inform Prolific Trade N.V. management;

- f. To procedurally prepare and maintain the lists classified by customers in accordance with a risk-based approach (low, medium, high-risk);
- g. To detect, register and assess, at least yearly, all risks posed by existing and new customers, new instruments and services and update and change the systems and procedures implemented by the Company with a view to efficiently managing the risks mentioned above;
- h. To assess and approve cooperation with the systems and procedures of third parties relied upon by Prolific Trade N.V. to identify and know its customers.
- i. To offer guidance/opinions to Prolific Trade N.V. employees on ML/FT issues;
- j. To identify Prolific Trade N.V.'s departments and employees that require additional training and education for ML/FT purposes and organize training sessions/workshops. To this effect, they shall prepare and implement an annual staff training program. They shall assess whether the education and training offered are appropriate;
- k. To prepare MLRO's annual report, as well as MLRO's monthly reports;
- l. To secure connection and be a contact point for AML/CFT issues with regulatory authorities, law enforcement authorities or other national authorities;
- m. To keep a record including at least the following:
 - i. Internal Reports on Suspicious Transactions;
 - ii. Reports providing reasons for not filing SARs/STRs with the FIU;
 - iii. Internal Assessment Reports
 - iv. MLRO reports to the Office;
 - v. All requests for information from the Regulatory entities;
 - vi. All documents registering the fulfillment of his/her tasks;

Compliance Officer Fit & Proper Criteria

As of January 2025, in accordance with the GCB Guidelines, the appointed Compliance Officer must meet specific competence and integrity standards. This includes either:

- Holding a recognized AML certification (e.g., CAMS, AMLFC) and having at least two years of experience in AML/CFT reporting roles, or
- Having four years of experience in AML/CFT reporting roles without certification.
- Alternatively, the individual may qualify if they have served for at least two years as an MLRO in another jurisdiction.
- The Compliance Officer must complete at least 10 hours of AML-specific training annually and must not hold positions that could result in a conflict of interest (e.g., UBO, CEO, CFO, Casino Manager, or internal auditor roles).
- Prolific Trade N.V. confirms that the Compliance Officer has unrestricted access to all KYC, CDD, transaction monitoring, and audit information and acts independently from operational management.

7.4 Internal Reporting

When an employee becomes aware of any information or matter that in his/her opinion gives rise to knowledge or suspicion that a person or a transaction is connected in any way to ML/FT practices, the Company's internal reporting procedure needs to be followed.

When an employee becomes aware of any such information or matter, he/she shall treat the case with the utmost urgency and shall report the matter to the MLRO without delay.

The report is to be made by not later than the next working day. At the initial employment stage, all employees are informed of the identity of the appointed MLRO to whom the report must be made and the information that has to be made available within the report. In the event the MLRO is unavailable for a period of time, the relevant team is informed via email so that the designated employee is contacted in the MLRO's absence.

The report shall include details on the customer and/or the transactions/activity that is the subject of concern and as full a statement as possible presenting the information or matter that gives rise to the employee's concern. The report must be submitted in writing, whether on paper or electronically.

surrounding a particular customer or transaction with his/her immediate superior or the MLRO prior to determining whether to submit an internal report. In any eventuality, the internal report should be raised with the MLRO within the next working day from when the employee becomes aware of the information or matter that gave rise to his/her suspicion.

It is possible that additional internal reports may have to be made following the submission of an initial report since the employee may notice further related transactions or activities that give rise to knowledge or suspicion of ML/FT. These too need to be reported to the MLRO.

The MLRO must consider, with the utmost urgency and without unreasonable delay, every internal report he/she receives to decide whether:

- a. the information contained in the report does give rise to a knowledge or suspicion of ML/FT in which case the MLRO should proceed to submit a STR/SAR to the FIU in a prompt manner as explained hereunder; or
- b. additional information is necessary to reach this determination.

In view of this requirement, the MLRO should be granted unrestricted access to all relevant documentation and information.

Where additional information is deemed necessary, the MLRO must collect and consider any additional information and/or documentation he/she deems relevant to make this determination, which may include:

- a. previous transactions, transaction patterns and volumes, previous patterns of instructions, the duration of the business relationship and CDD information;
- b. where applicable, other connected accounts and the existence of other relationships, including those where other persons were suspected of ML/FT practices;

Other information or documents that are reasonably accessible through public sources, or that may be obtained from the customer subject of that internal report.

Where the MLRO identifies the need to obtain information from the customer or any person or other external sources, the request should be made immediately and followed up regularly.

If the MLRO, after having obtained and considered the additional information necessary to reach his/her determination, concludes, for justifiable reasons, that an internal report does not give rise to knowledge or suspicion of ML/FT, the MLRO need not file a report with or otherwise inform the FIU. In this case, the MLRO must keep a written record (electronic format) of the internal report received, the assessment carried out, the outcome and the reasons why the report was not submitted to the FIU.

7.5 Internal Control Processes

The internal control activity shall fall under the responsibility of MLRO. During the internal control,

MLRO shall verify, on a sample basis, compliance with the AML Policy requirements in the following fields:

MLRO shall verify the implementation of CDD measures by:

- Checking the categories of personal data on customers collected by operators;
- Checking the customers' records on PEP, high-risk countries, and international sanctions status;
- Checking collected identity documents;
- Checking results on customers, by using public information sources;
- Checking how customers are included in risk classes;
- Checking the implementation of document keeping policy.

MLRO shall verify whether EDD measures were implemented accordingly by:

- Checking the risk factors leading to the implementation of additional measures;
- Checking how additional checks were made via public sources;
- Checking the circuit of approvals from the higher management of Prolific N.V. (if applicable);
- Checking how the source of income was established (if applicable);
- Checking the implementation of the document keeping policy.

MLRO shall check the monitoring of the suspicion indicators from the AML Policy and the steps followed if the transaction is reported as suspicious.

Verifications shall be conducted during the internal control conducted by MLRO to identify possible transactions which were not reported, despite the fact of showing suspicion indicators, by:

- Verifying information on customer;
- Verifying records;
- Conducting interviews with APR staff;
- Any other means of evaluating the efficacy of the Manual's provisions and its implementation are also acceptable.

7.6 Internal Audit

The Internal audit function plays a critical, yet independent role in assessing the Company's compliance with regulatory requirements and documented policies and procedures, as well as regulatory expectations including ML/FT. The Internal Audit function ensures that through its impartiality and objectivity it can provide recommendations to the Board to ensure proper governance and oversight, including gaps in policies and procedures.

The Internal Audit reports directly to the Company's Board of Directors. The Internal audit function forms part of the third line of defence. This will give the Internal Audit a proper channel to forward any matters identified during audit. In relation to ML/FT the Internal Audit assesses the compliance culture of the Company, can assess the different lines of defence and the manner this is working in practice, provide regular updates to the Company's Board of Directors and provide recommendations on policies, procedures and operational issues together with its recommendations.

Internal Audit conduct periodic reviews of the Company's policies and procedures, not only on AML but on every aspect of the Company. Reviews are conducted periodically with reports being provided to the Board, the former being the body which oversees the implementation.

8. Employee Training

8.1 Initial Training

The program of initial training in the AML/CFT sector shall be conducted at the beginning of the employment and shall include information on the legislative requirements in this sector, as well as distinct practices, intended to permit employees to implement the regulations in this field accordingly.

Consequently, by the AML/CFT module, employees acquire knowledge on the AML Manual, and shall be required to meet their duties in terms of:

- a. The obligation to know their customer
- b. Risk-based approach and customer risk classes
- c. MLRO duties
- d. Standard and improved due diligence measures
- e. PEP identification and implementation of procedures for accepting PEP customers
- f. Identifying suspicious transactions based on established indicators
- g. Identifying and reporting to MLRO suspicious transactions
- h. Documents required to collect and send for submission purposes by MLRO of a report on the suspicious transactions to FIU
- i. Methodology for document keeping within the AML/CFT area
- j. Internal communication procedures with line managers and MLRO, and the use of internal communication channels for the purpose of implementing the AML/CFT Policy
- k. The obligation to keep the confidentiality of the information collected for the purpose of implementing the AML/CFT policy, and prohibition of disclosure
- l. Punishments set forth for breaching the obligations set forth under the AML/CFT laws and regulations

At the same time, employees shall have to be informed that they are granted protection in the exercise of their duties, according to law.

8.2 On-Going Training

The Company provides continuous training of the staff, so that all employees with duties in the AML/CFT field enjoy a training that is proper, updated and adjusted to the Company's actual needs.

The continuous training of the staff whose duties include the AML/CFT activity shall be conducted based on the training plan and topics prepared by the MLRO.

Also, if further to internal controls or in the case of legislative amendments a need occurs to organize new training sessions with the employees, the MLRO shall organize training sessions in addition to those established in the training plan.

The training plan shall include general information on the relevant laws, practical training of the staff for recognizing suspicious transactions, measures which must be taken in such cases and debates on actual situations dealt with by employees during the fulfillment of their duties.

9. VETTING OF EMPLOYEES

Staff members are recruited following either a public call or through recruitment agencies. Depending on the role the new employee will hold, a list of requirements for the relative role will be drawn up. Prior to sitting for an interview, the prospective employee will provide a copy of the Curriculum Vitae which is vetted by senior members of the Company. Employment history and qualifications are also requested. Following an interview, prospective employees would need to complete a psychometric test which will give more insight into integrity and the abilities of the employee, and the way they would handle certain situations.

The Company conducts screening against sanction lists and adverse media prior to engagement, every three years and whenever an employee assumes a senior role, in accordance with the HR Procedure. A Police Conduct Certificate is obtained once the employee is chosen but before the employment contract is signed since apart from knowledge and experience in the industry, Prolific Trade N.V thrives to engage employees with integrity and who are honest and exemplary.

In certain circumstances, prospective employees may be required to complete aptitude tests to assess their job-related skills, integrity, and their approach to handling various situations.