Anti-Money Laundering and Countering the Financing of Terrorism
Business Risk Assessment

Version Control:

Version	Date	Changes Made	Approved By
1.0	December 2022	Initial BRA prepared in line with LID, LMOT, and FATF standards	MLRO
1.1	November 2023	Enhanced customer risk typologies, updated delivery channel assessment	MLRO
1.2	November 2024	Added product-specific risk breakdown, refined residual risk methodology	MLRO/Board
1.3	April 2025	Added executive summary, qualitative placeholders for quantitative data, risk register table, governance and control testing framework	

eMoore N.V., Managing Director
Repr. by: C. van der Leeuw, Proxy holder
Signed December 1, 2025

eMoore N.V.
P.O. Box 422
Curaçao
Tel.: +59997471401

Contents

Executive Summary – Business Risk Assessment (BRA) 2025

Entity: Prolific Trade N.V.

Sector: Remote Gambling (Online Casino, Sports Betting)

Prepared by: MLRO – Miruna Georgiana Mihailescu

Last Review: April 2025

Next Scheduled Review: Within 12 months or upon material trigger

This BRA has been prepared in alignment with the National Ordinance on Identification (LID), the National Ordinance on Reporting Unusual Transactions (LMOT), and the supervisory expectations of the Curaçao Gaming Control Board (GCB), as well as FATF Recommendation 1.

Introduction

A Business Risk Assessment ('BRA') is a process whereby Prolific Trade N.V. identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT risks. Based on this assessment, it will be able to determine which areas to prioritize in terms of AML/CFT and ensure that its AML/CFT measures, policies, controls, and procedures are commensurate with the ML/FT risks it faces to mitigate the same. The BRA is, therefore, the foundation of the risk-based approach and the National Ordinance on identification when rendering services (LID) and the National Ordinance on the reporting of unusual transactions (LMOT) impose an obligation on Prolific Trade N.V. to "take appropriate steps, proportionate to the nature and size of its business, to identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business".

This Anti-Money Laundering and Countering the Financing of Terrorism Risk Assessment is documented in accordance with FATF Recommendations and the National Ordinance Reporting Unusual Transactions (NORUT) and the National Ordinance Identification when Rendering Services or NOIS, and has been drafted in order to ensure Prolific Trade N.V. designs, implements and maintains a risk-based Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") program with all relevant supporting controls and procedures aimed at mitigation of identified risks. It may serve as evidence upon request from any relevant authority or regulatory body to support the design of the AML/CFT Programme but is otherwise for internal use and reference only.

The Risk Assessment is documented and maintained by the MLRO who is currently Ms. Miruna Georgiana Drljic Mihailescu, holding Romanian nationality and bearing Passport 060943515, in collaboration with relevant control and process owners, is reviewed by the Compliance Officer, presented to the Board Limited annually for adoption. This Risk Assessment will be reviewed annually or based on relevant trigger events.

The FATF Recommendations and Article 8 EU Directive 2015/849 declares that obliged entities shall take appropriate steps to identify and assess the risk of money laundering and terrorist financing, considering risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels.

The risk assessment shall be documented, kept up-to-date, and made available to the relevant competent authorities.

Scope of the assessment

The scope of the business risk assessment is to ensure that the business is aware of the risks likely to face from the current risks within the institution and serve as a prevention against new and perceived threats. The risk assessment shall as at a minimum be reviewed annually and any changes are to be displayed in the list of changes and implement the new and updated scoring accordingly.

Governance and Oversight
This Business Risk Assessment is reviewed and approved by the Board of Directors of Prolific Trade N.V. on an annual basis or upon the occurrence of trigger events, such as significant changes in the business model, product offerings, risk exposure, or relevant regulatory requirements.
The latest review and approval were completed on [Insert Date] as per Board Meeting [Insert Meeting Ref or Minute No.].

The MLRO is responsible for ensuring the document reflects the company's risk appetite and remains aligned with evolving threats. Evidence of review and approval is retained and made available to the GCB or other competent authorities upon request.

1.0 Company Risk Appetite - Prolific Trade N.V. adopts a conservative risk appetite for all ML/TF threats, particularly when engaging with high-risk jurisdictions, anonymous payment methods, or complex customer structures. The company does not accept:

- Unverified customers;
- Anonymous funding sources;
- Clients from restricted or sanctioned jurisdictions;
- Clients with non-transparent corporate ownership or crypto-only activities.

Where residual risk exceeds defined thresholds, enhanced controls or outright rejection of the relationship or activity is applied.

1.1 The Risk Assessment is of utmost importance in identifying the risks the business is likely to face, including risks for that the company has to prevent before any materialization.

1.2 The following Business Risk Assessment document covers only the risks connected to Money Laundering and Terrorism Financing and not the other business risks the Company is exposed to.

1.3 The Business Risk Assessment Document reflects a Risk-Based Approach which provides a level of importance to some factors over others.

1.4 The Business Risk Assessment must be reviewed and updated on a regular basis at least once a year by the MLRO. In case of any changes within the business structure or business environment, the Business Risk Assessment document must be updated accordingly.

1.5 The Risk Assessment is a cyclical process, which means that the company is required to perform the whole cycle of identification, analysis, and testing of the effectiveness of controls at regular intervals.

Business overview

The company has a diverse line of business, which is that of an operator engaged in the digital gambling industry, offering a wide range of casino games and betting opportunities to customers over the Internet. This industry encompasses various games of chance, including slot machines, table games, card games, live dealer games, and sports betting. The primary goal of the Company, as an online casino operator, is to provide an entertaining and secure platform for players to wager on casino games and sports events remotely, using computers, smartphones, or other digital devices.

The company's main business activities are listed below, as well as the risks emanating from these business activities:

1) Online Casino Games: The operator offers a wide range of virtual casino games, including slots, table games (such as blackjack, roulette, and poker), live dealer games, and specialty games. Players can access these games through the casino's website or mobile app.
2) Sports Betting: Many online casinos also include sports betting platforms where players can wager on sporting events, including football, basketball, tennis, and more. Sportsbook services allow users to place bets on various sports outcomes.
3) Promotional Offers: Online casinos frequently provide promotional offers, bonuses, and loyalty programs to attract and retain customers. These can include welcome bonuses, free spins, and cashback rewards.
4) Payment Processing: The operator facilitates secure payment processing, enabling players to deposit funds into their casino accounts and withdraw winnings. Various payment methods, including credit cards, e-wallets, and cryptocurrencies, are typically supported.
5) Customer Support: Providing customer support is crucial to address player inquiries, resolve issues, and offer assistance with responsible gaming. This includes live chat, email support, and telephone assistance.
6) Responsible Gaming: Online casinos are responsible for promoting responsible gambling practices. They implement self-exclusion options, deposit limits, and other responsible gaming features to protect players from excessive gambling.

Risks Emanating from Business Activities:

Regulatory Compliance Risk: Operating in the highly regulated gambling industry, online casinos face substantial regulatory compliance risks. Non-compliance with licensing requirements and responsible gaming regulations can result in fines and license revocation.

Financial Risk: Online casinos are exposed to financial risks, such as fluctuations in revenue due to player wins or losses. Economic downturns and payment processing issues can also impact the financial stability of the operator.

Cybersecurity and Data Breach Risk: Online casinos store sensitive customer information and financial data. They are susceptible to cybersecurity threats, including hacking attempts, data breaches, and ransomware attacks, which can compromise player data and lead to legal consequences.

Reputation Risk: Any negative publicity related to unfair gaming practices, delayed payments, or security breaches can harm the operator's reputation, resulting in a loss of player trust and decreased market share.

Operational Risk: Operational risks encompass technical glitches, server outages, and software malfunctions that can disrupt gameplay and affect customer satisfaction.

Market Competition: The online gambling industry is highly competitive. The operator faces the risk of losing customers to rival casinos offering better promotions, games, or user experiences.

Addiction and Responsible Gaming Risk: Encouraging responsible gaming is essential to prevent player addiction and mitigate potential harm. Failure to do so can lead to negative publicity and legal consequences.

Fraud and Cheating Risk: Online casinos must watch for fraudulent activities, such as bonus abuse, collusion, and cheating in games. These activities can lead to financial losses and damage the integrity of the platform.

Payment Processing Risk: Ensuring smooth payment processing is crucial. Delays or issues with deposits and withdrawals can lead to player dissatisfaction and complaints.

Legal and Compliance Risks in Different Jurisdictions: Operating in multiple jurisdictions may expose the operator to varying legal and compliance requirements. Understanding and adhering to these regulations is essential to avoid legal issues.

Having assessed the risk environment, manifestations of risks have been identified and listed within the business risk assessment, for which measures are in place to further mitigate any associated risks. Upon assessment the MLRO shall engage in scenario's and further describe any means required to prevent such risk from manifesting itself. If a risk or weakness have been identified and give cause to further business concern such will be raised to the board of directors accompanied by any findings and further recommendations.

The Risk Environment

Vulnerabilities to Money Laundering (ML)

Money laundering and funding of terrorism is a threat that may be perceived as:

- Domestic Money laundering and funding of terrorism threats – are mainly related to drug supply and drugs offenses, fraud and tax evasion, cybercrime, acquisitive crime, organized immigration crime, prostitution, and modern slavery.
- International Money Laundering and funding of terrorism threats – are mainly related to organized crime and overseas corruption, remittances as well as other financial flows and international financial centres where criminals may launder the proceeds of their crimes.

The inherent threats have been devised based on the risk the company is likely to face:

-Transfer of funds from legitimate and illegitimate customers. Rogue agents usually perform transactions using fake IDs and fake invoices.

- Proceeds of crime are placed in the financial system through a regulated company offering payment accounts or similar products. Perpetrators may also use such regulated company providers to channel their funds.

- Funds are placed and/or transferred through money remittance services. Risks of money laundering / terrorist financing activity may be particularly high when funds to be transferred are received in cash or in anonymous e-money.

Organized crime groups have increasingly found ways to exploit the gambling industry and online remote casino operators for various illicit activities. These criminal organizations use the gambling sector as a means to legitimize and launder their ill-gotten gains, as well as to generate substantial revenues. Below we have described how organized crime groups are using the gambling industry and online casinos:

Money Laundering:

One of the primary ways organized crime groups infiltrate the gambling industry is through money laundering. They often introduce "dirty money" into the system by placing large sums of illicitly acquired funds as bets or deposits. These funds are then circulated within the casino environment through gambling transactions. Criminals intentionally lose some of the wagers to "clean" the money, as winnings can be withdrawn as "clean" funds. This process obscures the origins of the illicit proceeds.

Loan Sharking:

Organized crime groups may offer loans to desperate gamblers within or around casinos. These loans often come with exorbitant interest rates and stringent repayment terms. Borrowers who can't repay their debts may be subjected to threats, violence, or extortion. Loan sharking within the gambling environment is a common tactic employed by criminal organizations to generate profits.

Match-Fixing and Sports Betting Fraud:

Organized crime groups can manipulate sporting events to secure guaranteed outcomes, a practice commonly known as match-fixing. By controlling players, referees, or other stakeholders, criminals ensure that bets placed on predetermined results will yield significant profits. This fraudulent activity undermines the integrity of sports and the fairness of sports betting markets.

Illegal Online Gambling Sites:

Some criminal organizations operate their own illicit online gambling platforms or collaborate with existing operators to run illegal websites. These sites often lack proper licensing and regulatory oversight, making them attractive to individuals seeking to engage in illegal gambling activities.

Extortion and Threats:

Organized crime groups may attempt to exert control over casino operators or employees through intimidation, threats, or extortion. These tactics can be used to gain influence within the industry or manipulate outcomes in their favour.

Money Transfers through Cryptocurrencies:

With the rise of cryptocurrencies, organized crime groups have found a new way to move funds across borders and obfuscate their financial trails. They may use cryptocurrencies for both money laundering and transferring illicit proceeds related to gambling.

Online Fraud and Identity Theft:

Criminals sometimes engage in online fraud and identity theft within the context of online gambling. They may create fake accounts, use stolen identities, or engage in fraudulent payment transactions to manipulate online casinos and exploit promotional offers.

Illegal Gambling Dens:

In some cases, organized crime groups establish or oversee illegal gambling dens that operate outside the boundaries of regulatory oversight. These establishments can engage in various forms of illegal gambling, including unregulated betting, slot machines, and card games.

Regulatory Evasion:

To continue their operations undetected, criminal organizations may attempt to evade regulatory authorities. This can involve disguising their ownership of gambling businesses, engaging in unlicensed activities, or operating in jurisdictions with lax regulatory enforcement.

It is essential for law enforcement agencies, regulatory bodies, and the gambling industry to remain vigilant and cooperative in detecting and combating these activities. A robust regulatory framework, effective enforcement measures, and strong compliance practices within the gambling sector are critical in preventing organized crime's infiltration and manipulation of the industry.

Vulnerabilities to Terrorist Financing (TF)

The main terrorist financing threats emanate internationally 'the company' considers threats not only from non-reputable or high-risk jurisdictions but also terrorism. Terrorism will always be assessed as severe due to the likelihood of loss of life. The main threats are from Terrorist organisations within areas of conflict which are mainly in Syria and Iraq. Although terrorism has no boundaries, individuals to have domiciled in such jurisdictions may still be subject to extremist beliefs and may also engage in the funding thereof.

Islamist extremists from regions in the Middle East, North and West Africa, and South and Southeast Asia, however, there is also a significant threat posed from individuals with extreme views and one hence cannot measure the extremity of such involvement. One must be aware of any direct or indirect involvement especially since the trail of terrorist financing is different from the perceived money laundering methods. Emphasis should be made on the withdrawal and any links to non-reputable or high-risk jurisdictions or individuals who may be directly or indirectly associated with such beliefs.

Risk Assessment Methodology

The Company conducts its ML/TF risk assessment in accordance with the following process, following exhaustive research and understanding of the product, potential threats, potential breaches or circumvention of controls currently in place:

Step 1 - Risk Identification

The main risks to the business are identified under the following risk headers.

1. Client risk
2. Payment/Transaction risk /Product
3. Geographical risk
4. Delivery channel
5. Internal controls risks
6. Employees
7. MLRO duties
8. Internal security

Inherent risk: Likelihood vs Impact

The inherent risk is the risk that is evaluated if no controls had to be in place hence what threat is likely to emanate without control. The impact is the relevant effect of such events unfolding. The likelihood and impact were plotted on a graph to clearly indicate the total score of such risk. It is important to note that the company did not assess only those threats that exist but has taken active measures to include threats that the company is likely to face prior to the inception of a business relationship or an occasional transaction and at the stage of attempting to commit offense through the company.

The data to further provide a clear assessment of the current business profile is based on the information held internally which provides an overview of the current clients, also including an analysis of threats and evaluation on reported cases, also those cases which were deemed not to hold sufficient evidence to report. Since the company has taken a stance to also address external threats, that will automatically be a breach of the customer acceptance policy or the company has taken a stance to immediately decline such business, such are reflected as a preventative measure and to ensure that such external risk remains at bay and to maintain the ability to deter any business that may be deemed to be damaging.

Step 2 - Risk Mitigation – Evaluation of risk control progra

The internal policies and procedures are addressed and updated accordingly depending on any new or emerging threats or vulnerabilities are identified. The business risk assessment shall serve as the foundation of developing such policies and procedures and further strengthen any changes within the policy to mitigate risk. Due to the change within the 'modus operandi' of financial crime, and as stated the dynamic approach adopted by the company, the companies' policies, procedures, customer acceptance policy and the day – to -day execution of business may be updated and amended depending on new and evolving threats.

In those instances where it has been identified that the company is not sufficiently equipped to mitigate any identifiable risk, such will require changes within the policy and procedures, updating of employee's and delay any launch or execution of any product or service until such risk is controlled and adequately managed.

Step 3 – Assessing Residual Risk

Assess the level of exposure to each risk considering all the mitigating measures (controls) in place set against the risk profile of the company specifically. The residual risk shall have to fall within the parameters of the risk appetite being the controls that are sufficiently in place to prevent any money laundering and funding of terrorism. Hence, the scores shall always have to be a low, meaning that there are sufficient controls in place to mitigate such risk.

If a product ranks at high risk, it means that action needs to be taken to mitigate the risk emanating from such a product, and such will have to be embedded within the risk framework to mitigate accordingly due to the high-risk appetite held by the company.

Step 4 – Risk Monitoring and Review

Once the appropriate risk mitigation measures are in place and the Company is operating at the residual risk level, there are measures in place to monitor the identified risks to ensure that the mitigation measures remain proportionate to the risk.

The Company is aware that the risk assessment process cannot remain static and dynamic approach, as such, in relation to changes to customer base, products and services, business practices or regulations will result in a review of the risk assessment and appropriate updates will be made on an ongoing basis, either annually or on a specific trigger basis.

Risk categorization used is High, Medium, Low. Inherent risk is assessed cognisant of the national, regulatory, and Company operations, with residual risk rating assigned based on the extent and effectiveness of the internal control environment.

Risk Matrix

The following risk matrices of likelihood vs Impact, and total residual risk which calculates the strength of the controls currently in place against the inherent risk, such has been used as part of the risk matrix to further calculate the residual risk and whether the company is willing to accept such risk or whether more stringent controls are to be in place.

Initial workings

The identification of the threats and vulnerabilities one is exposed to requires a consideration of the risk areas and risk factors both from a qualitative and a quantitative point of view.

As of the date of this assessment, Prolific Trade N.V. is in the process of implementing data capture tools to support quantitative risk assessment. While comprehensive customer and transactional metrics are not yet systematically aggregated, the following qualitative observations are available:

- The customer base remains limited in scale and restricted to jurisdictions with low to moderate risk profiles.
- The business model does not currently target high-risk customer types (e.g., PEPs, complex corporate structures).
- All customers undergo full KYC prior to onboarding, and any red flags during the lifecycle are escalated.
- No transactions from sanctioned or FATF high-risk jurisdictions have been identified during onboarding or ongoing monitoring.

A full quantitative summary of customer segmentation, transaction volumes, and jurisdictional exposure will be introduced in the next annual BRA review cycle, once the reporting functionality within the compliance monitoring tools is fully operational.

Thus, for the purposes of the BRA, it is not sufficient for Prolific Trade N.V. to merely draw up an inventory of the threats or vulnerabilities; the Company also recognises the importance of assessing the scale and frequency of these risks. While comprehensive quantitative data is not yet available, Prolific Trade N.V. considers a number of qualitative indicators and commits to enhancing its data collection capabilities to support future risk assessments with more granular, measurable insights.

a) Customer Risk

Customer risk is the potential AML/CTF risk posed by the customer which commences at account opening and continues throughout the customer journey and through the business relationship and includes the ongoing monitoring and screening of customer account activity and transactions.

Customer Risk is assessed within the general environment of a Low-risk appetite to player type; hence, the company has adopted a strict approach in providing its products and services through restricted markets, and also to those individuals who are eligible to hold a Photo I.D. as one of the risk mitigating factors. Further manifestations of risk are identified, and the mitigating controls have been deemed sufficient for which the residual element is within the company's risk appetite. As stated, the business risk is a dynamic approach and review of which being both manifestations of risk and internal controls are assessed accordingly.

Within this section the company has taken an understanding of the existing client base, and any external threats the company is likely to face. External threats, unless robust measures are in place to mitigate the risk, are deemed to be pertinent in the continuous development and mitigation of the company's risk appetite.

Risk is a dynamic approach in understanding not only the customer but the behavioural aspects of the customer. Further, where players are subject to an internal disclosure in most instances the player relationship has been closed / terminated within site conditions at the point it is escalated as a disclosure.

Where an unusual/suspicious behaviour is identified by a member of staff, it is subject to the internal escalation process. This will lead to the submission and logging of an internal disclosure, an investigation of the player account and activity, and an external suspicious activity report where the FIU is raised and the reporting standards are met.

The Customer Risk is assessed by considering the following:

- the number of customers within each customer risk type;
- the maturity of the client base, i.e., the duration of existing business relationships; and
- the volume of business.
- the complexity of structure.

The following is a non-exhaustive list of the customer risk types identified by Prolific Trade N.V.:

- Unregulated virtual currency exchanges
- Corporate Structures using bearer shares
- Non-Profit Organizations
- Correspondent Banks
- Fiduciary Arrangements
- Politically Exposed Persons (PEPs)
- Individuals who acquired citizenship by investment (IIPs)
- High Profile Figures/ International sportsman
- Highly Paid Employees
- General Public
- Directors/CEOs/CFOs of Banks/Multinational companies
- Other individuals (e.g. pensioners, average-salaries employees, students)
- Money Service Business/Casino/Dealers in Precious Metals
- Credit/Financial Institution
- Listed Entity

Prolific Trade N.V. also looks at the following non-exhaustive risks posed by the reputation and behavior of the customer:

- Adverse Media Reports
- Allegations of criminal activity
- whether any of the customers had their assets frozen

- whether any of the customers or beneficial owners have been subject to an STR
- Customer not forthcoming with information
- Complex Structures
- Whether any of the customers changed radically the business operations
- Structure and Purpose are not legally valid.
- Source of Wealth not duly substantiated
- Complex Transactions
- Customer requests unnecessary levels of secrecy
- Money Laundering Risks
- Fraud Risks
- Cheating and Collusion
- Chargebacks and Disputes
- Problem Gambling and Responsible Gaming
- Reputation Damage
- Regulatory Compliance Risks
- Bonus Abuse
- Insider information and Match-Fixing
- High-Value customers
- Reputation Risk for High-Value Customers
- Self-Exclusion and Responsible Gaming Violations
- Identity Theft and Fraudulent Accounts
- Non-Payment and Default Risk
- Cybersecurity and Hacking

As per the applicable regulations, the adverse media information has been enhanced with further practical guidance, reiterating the fact that the absence of an arraignment or a conviction should not be automatically taken to mean that any adverse reports can be ignored. The regulations emphasize that acquittals should also not be taken at face value but should, instead, be factored in when assessing the reputation of the person being scrutinized. When reviewing the adverse media information, Prolific Trade N.V. must consider the reasons that led to the acquittal and whether such reasons serve to dispel any concerns about the individual/entity involved. Furthermore, the FIU also clarifies that the nature of the adverse news will also have an impact on its actual relevance for risk assessment purposes. Additionally, Prolific Trade N.V. officers and employees should be able to discern what is considered reliable media reports and what impact these can have on one's risk understanding. Additional emphasis is brought on the importance of the passage of time with respect to adverse media, remarking that the impact of adverse media can depend on how remote in time it is. Thus, the longer the passage of time from the date of the media item (or the date of the adverse activity reported on in the media item), the less likely it is that the facts reported on will have an ML/FT impact.

The context of the adverse media also needs to be assessed so that adverse media is not viewed in isolation – for instance, the question of whether, following any adverse media reports, there were subsequent reports that either showed that the earlier information was groundless or else which otherwise downplayed the gravity and severity of any such prior information should also be taken into consideration. Where the adverse media gives rise to suspicion of ML/FT, the obligation to report to the FIU remains in place.

In those situations where the customer of the Company is a listed entity or a person carrying on a relevant financial business, and where the customer has been the subject of supervisory or regulatory action, the following considerations will be considered when performing the risk assessment:

- when the regulatory action was taken;
- whether the breach is impacted by supervening legislative or regulatory changes (for instance, something which may have been considered a breach originally may later no longer be considered to be a breach);
- the nature of the breach itself where the FIU distinguishes the one-off failure by the customer to file a regulatory return from a more serious failure to properly monitor the customer's clients on an ongoing basis or some other more serious AML-CFT breach;
- the nature of the regulatory action taken, where the FIU distinguishes between mere remedial action and the imposition of a hefty administrative penalty or even the pressing of criminal charges against the customer for the breach committed;
- whether the regulatory issues have been resolved.

Overall Residual Geographical Risk – Medium

b) Geographical Risk

There is a risk that players have links to high-risk jurisdictions, which may have poor governance structures, political instability, and/or threats of criminal/terrorist activity. Linkages through the province of the funds and any country that has indicated instability or sanctions issued against.

The company has mitigated such risk by only accepting customers whose nationality and residence have been verified. Where customers are linked to high-risk jurisdictions, the company will enforce Enhanced Due Diligence.

The Geographical Risk is calculated by considering the following factors:

- the number of subsidiaries or branches within a given jurisdiction;
- the number of customers and/or beneficial owners from a given jurisdiction;
- the number of transactions to/from a given jurisdiction; and the number of any other links that expose it to a given jurisdiction.

When formulating the BRA, Prolific Trade N.V. looks at the number of customers, jurisdictional links, and transactions emanating from the following jurisdictional categories:

- Brazil;
- EU/EEA;
- Non-EU/EEA;
- High Risk Jurisdictions;
- Restricted Jurisdictions;
- Countries Listed on the FATF List/EU List listing AML/CFT High Risk Deficiencies;
- Sanctioned Countries

Overall Residual Geographical Risk – Low

c) Products, Services, and Transaction Risk

There is a low risk that our products may be used to facilitate activity involving low-risk wagering or minimal activity followed by a withdrawal of the account balance through the same payment method and only one payment mechanism is in place for such players, which is through the bank account which holds bank I.D. Such places a low risk on the company, as the funds are remitted directly through a banking institution linked to the individual. The products have all been assessed for their attractiveness in being used for illicit purposes.

The product, service and transaction risk is calculated by considering the following:

- the number of products, services (including correspondent and trade finance relationships) and transactions;
- the number of customers per product and service;
- the volume per product and service.

Prolific Trade N.V. looks at the risks emanating from the following types of services:

- Certainly, here is a list of the types of services offered by a remote gambling operator, along with a description of the risk level associated with each service:
- Sports Betting:
  - Risk Level: Moderate
  - Description: Sports betting involves wagering on the outcome of sporting events. While it has a moderate risk level due to the unpredictability of sports outcomes, operators must monitor for potential match-fixing and the use of insider information for betting.
- Casino Games:
  - Risk Level: Moderate to High
  - Description: Online casinos offer various games such as slots, roulette, blackjack, and poker. The risk level can vary depending on the type of game, with games like poker having a higher risk of collusion and cheating.
- Online Poker:
  - Risk Level: High
  - Description: Online poker carries a high risk of collusion among players and the use of bots. Operators must implement robust anti-collusion measures and fraud detection systems.
- Live Dealer Games:
  - Risk Level: Moderate to High
  - Description: Live dealer games, such as live roulette and blackjack, involve real-time interaction with dealers. The risk level can be high due to potential collusion between players and dealers.
- In-Play Betting:
  - Risk Level: High
  - Description: In-play or live betting allows players to wager on events as they unfold. It carries a high risk of manipulation and requires real-time monitoring to detect suspicious activity.
- Peer-to-Peer Betting:
  - Risk Level: High
  - Description: Peer-to-peer betting platforms allow users to bet against each other. The risk is high due to the potential for collusion, match-fixing, and disputes between users.

  Prolific Trade N.V. also looks at the following industry types:

Industry Type	**Risk Level**

Accountancy, Audit & Provision of Tax Advisory Services	High
Administrative and Support Services (Accounts clerks, secretaries, etc)	Low
Affiliate Marketing	High
Agriculture & Fisheries (farming)	Low
Architect/Draftsmen	Low
Auctioneer, Antique & Finer Art Dealers	High
Aviation	High
Gaming	High
Transportation	High
Charity/Associations/Non-Profit Organisations	High
Civil Service	High
Construction & Property Development	High
Consultancy Services Provider	Medium
Consumer Goods Retailer	High
Crypto Related	High
Educational Services	Medium

Electronic Money Services/Money Remittance	High
Entertainment & Recreational Services	Medium
Financial and Insurance Services	Medium
Foreign Exchange Services	High
Consumables (eg. Fuel/gas/petroleum)	High
Health Professionals	Low
Hospitality Industry	Medium
Information Technology & Scientific Services	Low
Trading in Precious Metals	High
Legal & Judicial Services	Low
Unskilled Labourers	Low
Manufacturing industry – metals (Iron, steel, coper)	High
Marine Services (Yacht Leasing/Yacht chartering)	High
Marketing	Medium
Pharmaceuticals	High
Professional Services	Medium

Real Estate	High
International Sportsman	High
Trustee/Fiduciary Services	High
Bearer Shares	High
Rental & Leasing	High
Manufacturing of Machinery	High
Services intended to render the customer anonymous	High
Internet Based Products	High
Credit Intermediaries	Medium
Securities	Medium
Portfolio Investments	Medium
Listed Financial Derivatives	Medium
Holding of shares, stocks & debentures	Medium
Manufacturing of wood, papers, leather, chemicals	Medium
Wholesale electronics	Medium
Agents/Brokers	Medium

Media	Medium
Administration of Human Resources Programs	Low
Regulated Employment Sector	Low
Environmental Quality Programs	Low
Renewable energy projects/services	Medium
Space Research Technologies	Low
Owner of Pleasure Yacht	Low

Overall Residual Product Risk – Medium

d) Delivery Channel

Delivery channels are very limited, as the player may only log in using the specific credentials created and there is no use of a master account setup. All registrations are done directly with the company and the further assessment of risk is carried out by the company.

All business relationships are carried out on a non-face-to-face method, but such risk is mitigated through the use of Photo I.D. and where suspicion is raised, the player shall be requested to provide further documentation.

The delivery channel is being calculated by considering the following:

- the number of relationships started on a non-face-to-face basis;
- the number of distributors and agents; and
- the number of customers introduced through introducers and intermediaries.

The combination and assessment of these risk factors will allow Prolific Trade N.V. to identify the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes. Having done so, it must determine the likelihood of any one scenario materializing, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk.

Overall Delivery Channel Risk – Low

Internal controls risk

Internal controls in relation to AML/CFT that are currently in place are set to ensure that regulatory requirements are met and duties in relation to reporting of suspicious activity. Emphasis is made on holding up-to-date policies and procedures, in order to continue to ensure proper adherence to

AML/CFT procedures. A four-eye approach is in place and quarterly reporting is raised with the board of directors.

The effectiveness of these controls is evaluated through internal monitoring, quarterly reporting to the Board, and periodic audits. Where necessary, control testing is performed to assess the adequacy of staff training, policy adherence, and alert response times within the AML program.

An internal calendar is in place to periodically prompt any review or changes, unless a situation or trigger even arises which may require all documentation to be reviewed prior to the set dates. A list of risks has been listed and the internal controls held to mitigate such risk have been deemed to be sufficient and the overall result of the Internal controls risk has been deemed to be low.

Control effectiveness is assessed via quarterly transaction reviews, sample-based testing of KYC/EDD files, and an annual internal audit review. Material deficiencies are escalated to the MLRO and Board for remediation.

Overall internal controls risk – Low

Staff Risk/Employee

The Company is vulnerable to Staff risk where Staff collude with external parties with the intent to launder criminal funds. Staff may use their position, access, security approvals, and knowledge of the company systems to collude with external third parties/players to facilitate the movement of criminal funds through the business.

Overall residual Staff Risk – Low

MLRO risk

The duties of the MLRO (money laundering reporting officer) are pertinent to ensure proper compliance and ensure that all suspicion is being reported accordingly. The MLRO duties have been specifically devised to ensure that all aspects required to adhere with proper compliance are in place.

Overall residual MLRO risk – Low

A Likelihood Scale refers to the potential of an ML/FT risk occurring in the business for the particular risk being assessed. Four levels of risk are shown in Table 1:

Likelihood scale Likelihood Scale Frequency	Likelihood of ML/FT Risk
4 – Extreme	Can occur several times a year — very high chance
3 – High	Can occur a few times a year – reasonable chance
2 – Medium	Can occur once a year – small chance
1 – Low	Can occur less than once a year – very unlikely

Table 2 – Impact scale

Consequence	Impact of ML/FT Risk
4 – Extreme	Severe loss or damage, heavy supervisory action – long term effect
3 – High	Large loss or damage, supervisory action – medium- term effect
2 – Medium	Limited loss or damage, minor supervisory action – short-term effect
1 – Low	Negligible loss or damage, no supervisory action – no effect

Table 3 – Inherent Risk

Impact / **Likelihood**	**1**	**2**	**3**	**4**
1	Low Risk	Low Risk	Moderate Risk	High Risk
2	Low Risk	Low Risk	Moderate Risk	Extreme Risk
3	Moderate Risk	Moderate Risk	High Risk	Extreme Risk
4	High Risk	High Risk	Extreme Risk	Extreme Risk

Table 4 – Effectiveness

4 – Strong	There are measures in place to control risk that are fully operational and fully effective
3 – Effective	Risk is managed adequately but could be improved in certain parts – mitigating measures work adequately and are effective

2 – Ineffective	Risk is not managed adequately, substantial improvement necessary but has some effect
1 – Non-existent	No controls or controls are ineffective

Considering the inherent risk level in light of the effectiveness score will enable Prolific Trade N.V. to determine the residual risk.

Example: *Low inherent risk and ineffective level of mitigation = low or medium residual risk High inherent risk and ineffective level of mitigation = high residual risk.*

It is important to note that the effectiveness of the measures adopted will leave the inherent risk unchanged, independently of how effective a mitigating measure may be, a high-risk situation will remain high risk.

The residual risk will allow Prolific Trade N.V. to determine whether it is able to tolerate that risk as it falls within its risk appetite, or whether it needs to take further remedial action; that is, either taking additional measures to further mitigate the risk and bring it within acceptable levels, or to decline to pursue that particular business in its entirety.

Risk Category	Inherent Risk Score	Mitigating Controls	Effectiveness Score	Residual Risk	Owner / Reviewer
Customer Risk	Medium to High	KYC checks, EDD, restricted markets, ID verification	Effective (3)	Low to Medium	MLRO
Geographical Risk	High	Nationality/residency verification, FATF list screening	Effective (3)	Low	MLRO
Product/Service Risk	Moderate to High	Monitoring of game types, payout behavior, limited payment channels	Effective (3)	Medium	MLRO
Delivery Channel Risk	Moderate	Non-face-to-face ID checks, document collection, direct registration	Strong (4)	Low	MLRO
Internal Controls Risk	Moderate	Up-to-date policies, four-eyes principle, compliance calendar	Strong (4)	Low	MLRO / Board
Staff/Employee Risk	Moderate	Access control, monitoring, segregation of duties	Strong (4)	Low	HR / MLRO
MLRO Risk	Moderate	Clear duties, reporting lines, competence checks	Strong (4)	Low	Board of Directors

Carrying out the Business Risk Assessment

The BRA, changes thereto, and any connected decision have to be duly documented to retain evidence that an appropriate review has taken place, and are to be made available to the FIAU and relevant supervisory authorities on demand. Prolific Trade N.V. must balance its risk assessment sophistication depending on its business model.

Prolific Trade N.V. considers all aspects of the BRA including the following:

a) the methodology adopted by Prolific Trade N.V.;
b) the reasons for considering a risk factor as presenting a low, medium, or high risk;
c) the outcome of the BRA; as well as
d) any information sources used.

The BRA, revisions thereof, as well as any decision taken in relation thereto, have to be approved by the Prolific Trade's Board of Directors and also updated it as may be necessary from time to time.

Revising the Business Risk Assessment

FATF Recommendation 1 lays down that a BRA is regularly reviewed and kept up to date. This requirement stems from the very nature of risk, which is not static but evolves continuously in view of external changes as well as changes in the activities or services of Prolific Trade N.V. The Company is therefore required to revise and update its BRA:

- **whenever new threats and vulnerabilities are identified.** It is possible that in carrying out its activities, Prolific Trade N.V. will become aware of risks that it did not factor in during its original BRA. Information may also become available so that new threats have arisen that are exploiting certain vulnerabilities;
- **whenever there are changes to its business model/structures/activities**. There are many changes that may require a revision of the BRA. The mere increase in the number of clients serviced may be sufficient to expose Prolific Trade N.V to a higher risk of ML/FT than originally considered. The same applies if new markets are ventured into, be it through an increase in the portfolio of services, products or transactions offered or the targeting of new customer segments and/or jurisdictions.

The use of new technologies in delivering services, and products or affecting transactions may also increase the possibility of ML/FT. Moreover, the adoption of new technologies may also impact the ability to fulfill the AML/CFT obligations, increasing the operational and legal risks to which Prolific Trade N.V. is usually exposed.

When a revision of the BRA is occasioned through planned changes to be implemented, the revision should take place prior to any such change being implemented. This will enable Prolific Trade N.V. to understand whether this change will heighten the ML/FT risk it is exposed to and ensure that any necessary action is taken to adequately address the change in risk; and

- **whenever there are changes to the external environment within which Prolific Trade N.V. is operating.** These may be brought about by, for instance, regulatory changes and developments in technologies creating new threats.

The absence of any event provided for above does not mean that the BRA does not require periodical review. Prolific Trade N.V. should consider whether there have been any other changes that may affect the reliability and relevance of its BRA on an annual basis. If it is found that there is no need to change or alter the BRA, a note should be kept stating that, following a review of the BRA, it was determined that it was still current and valid, without requiring any updates.

Consideration of Emerging Risks
The Company also monitors and includes emerging risk factors relevant to the digital gambling sector. These may include:

- Use of AI-driven automation and gameplay manipulation;
- Stablecoin or crypto wallet misuse in payment flows;
- Sanctions evasion via affiliate channels or digital assets;
- Misuse of responsible gaming features to disguise layering behaviour;
- Cross-border transaction abuse involving high-volume/low-value movements.

These risks are periodically assessed and may trigger an ad-hoc review of internal controls or client segmentation practices.