

Risk assessment

Twino Trading N.V.

Version:	1
Date of version:	20.05.2025
Approved by:	Internal Compliance Committee
Confidentiality level	Internal

Change history

Version	Date	Author	Comment

I. INTRODUCTION

All gambling operators, whether remote or non-remote, have the responsibility to work towards keeping financial crime out of gambling. Legislation, regulation and guidance in each applicable jurisdiction place an obligation on operators to be alerted of customers' attempts to gamble with the proceeds of crime. This includes both the act of using criminal proceeds to fund gambling, or by extension, attempting to obtain legitimate or 'clean' money in return. A risk-based approach is required, with risk-based rules and criteria to proportionately manage Money Laundering ("ML") and Terrorist Financing ("TF") risk.

Twino Trading N.V. (the "**Company**" or "**Twino** ") aims to ensure that gambling activity is conducted in a fair and open way while making the utmost effort to prevent any use of the platform for fraudulent activities and money laundering. Using funds in casinos, regardless of the amount, that are the proceeds of any crime can amount to money laundering if the person using or taking the money knows or suspects that it is the proceeds of crime. Money laundering offenses can be committed by both the customer and casino employees, depending on their respective levels of knowledge or suspicion. The Company recognizes the need to have in place systems and procedures to combat money laundering, terrorist financing and other criminal activity, to identify criminals and to protect the company, those employed by it and its business reputation.

II. SCOPE, METHODOLOGY AND PURPOSE OF THE RISK ASSESSMENT

1. Scope

Our money laundering and terrorist financing risk assessment is a function of three key factors as defined by FIU.

Threats – which are persons, or groups of people, objects or activities with the potential to cause harm, including criminals, terrorist groups and their facilitators, their funds, as well as past, present and future money laundering or terrorist financing activities.

Vulnerabilities – which are those things that can be exploited by the threat or that may support or facilitate its activities and means focusing on the factors that represent weaknesses in AML/CTF systems, controls or certain features of a country, particular sector, financial product or type of service that make them attractive for money laundering and terrorist financing

Consequences – which refers to the impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally

2. Methodology

The Company takes into consideration the core risk factors, such as the categories of customers onboard (particularly high-risk customers), the products and services offered, transactions, the jurisdictions (geographical risk), payment methods used and the interface and delivery channels. Our approach includes the following stages as described:

Identifying

The identification process begins by developing an initial list of potential risks or risk factors when combating money laundering and terrorist financing. Risk factors are the specific threats or vulnerabilities that are the causes, sources or drivers of money laundering and terrorist financing risks. This list will be drawn from known or suspected threats or vulnerabilities. The identification process should be as comprehensive as possible, although newly identified or previously unidentified risks may also be considered at any stage in the process.

Analyzing

Analysis involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors.

Evaluating

The evaluation stage involves assessing the risks analyzed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process.

Others

Money laundering and terrorist financing risks may be measured using several factors. The standard risk categories used by FATF for casinos are as follows: (i) Country or geographic risk; (ii) Customer risk; (iii) Transactional risk, and (iv) Product risk.

The inherent risk probability is the chance of an identified ML/TF risk materializing as part of everyday operations and can also be interpreted as the vulnerability of each area identified as well as how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others. Consideration is given to factors such as the below when determining the probability of an identified risk: (i) Company exposure to a particular risk through business intelligence reports (data of a company); (ii) If the market is more prone to a particular risk over others, considering ML/TF tendencies in that jurisdiction; (iii) Reports issued by relevant authorities on severity and frequency of risks materializing.

The inherent risk impact describes the expected impact to the Company, should the identified ML/TF risk materialize without any specific control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others. Consideration should be given to factors, such as the below, when determining the impact of an identified risk: (i) Risk ratings provided by the relevant authorities in national risk assessments and sector specific guidance; (ii) Facilitation of criminal conduct; (iii) Risk of regulatory fines and legal prosecution; (iv) Reputational damage to the Company.

3. Purpose

All of the Company's activities must be managed in accordance with the risk assessment, including but not limited to (i) Ensure that the company does not assist in laundering the

proceeds of crime; (ii) Report any knowledge or suspicion or any reasonable grounds for knowing or suspecting that the company is being used for money laundering or terrorist financing purposes to the MLRO (or Compliance/AML Officer); and (iii) Conduct ongoing monitoring of the relationship with existing clients and of transactions.

Where we engage the services of third parties to assist in our compliance with AML and CTF laws, the responsibility for compliance remains with us, unless expressly agreed otherwise. This Risk Assessment is conducted in relation to the Company' activities in Curacao as a whole and does not replace the individual customer risk assessments that are constantly being carried out.

III. RISK BASED APPROACH

1. Identifying particular risks

Our Anti-Money Laundering and Counter Terrorist Financing ("**AML/CTF**") policy underlines senior management commitment in this area, and the standards expected by employees. This approach involves a number of steps to assess the most proportionate way to manage and mitigate the ML and TF risks faced by the Company:

- Prevention (CDD measures);
- Internal control systems (employee training and screening)
- Identifying the ML and TF risks relevant to our operations (monitoring of suspicious activity);
- Designing and implementing policies, procedures, and processes to manage and mitigate the risks;
- Monitoring and improving the effective operation of these controls;
- Reporting (Suspicious transaction reports)

- Recording what has been done, and why.

In identifying potential risks and threats, the following categories have been considered:

- **Customer risk** – specific categories of customers and the resulting business relationships;
- **Payment risk** – payment methods offered by Twino and the degree to which their specific characteristics are vulnerable to ML/TF threats;
- **Geographical risk** – the risks posed by geographical factors (remote only).
- **Product risk** – products offered and the degree to which their specific characteristics may be attractive for the purpose of money laundering or financing terrorism.
- **Employee risk** – the risks posed by the employees of the Company.

2. Analyzing

Risk probability is the chance of an identified ML/TF risk materializing as part of everyday operations. This can also be interpreted as the vulnerability of each area identified and how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others.

Risk impact describes the expected damage to the Company and industry, should the identified ML/TF materialise without any specific control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others.

3. Evaluating

Control measures are applied to each identified risk, to bring the risk within an acceptable level. A residual risk assessment of high/medium/low is calculated by combining the probability of the risk materializing and the resulting impact or damage after control measures have been applied.

What remains, the residual risk, is the accepted level of risk after application of AML/CTF controls. The residual risk categories are monitored and reassessed, where there is a change in the original risk evaluation and due to the respective measures adopted by the Company.

The risk level assigned to each identified risk has been compiled according to the Guidelines provided by the Financial Intelligence Analysis Unit (FIU's industry annual report). The following normative basis was also taken into consideration and analysed prior to our assessment:

- *he 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.2024,no.41(N.G.2017,no.92)(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. 2024 no.41 (N.G. 2017, no. 99)) (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);*
- *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;*

- *National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);*
- *Kingdom Sanction Act (N.G. 2016, no. 54).*
- *The FATF Recommendations;*

The control measures' effectiveness within the Company is dependent on our rigorous and diligent application of them. Effective governance arrangements and oversight is essential in this process, and the Company must ensure that senior management is fully engaged in the process. Additionally, the evaluation of Twino 's individual risk assessment will be dependent upon our particular business specifics and the mitigation measures applied. Whilst the inherent risk scores are likely to be similar across the industry, residual risk score is unique, taking into consideration our particular mitigation measures and risk appetite.

Risk assessments will be reviewed and refreshed on an annual basis and in the event of material changes to the risk environment. This ensures that new risks are effectively assessed, and the appropriate control measures are put in place for emergent technologies, such as virtual currencies (which are not currently prevalent in the industry). The Risk Assessment and Residual Risk Assessment after Controls columns are simplified to show the original level of risk and the residual risk when the controls are applied by us as an operator.

IV. ASSESSMENT

1. Overall

AREA	No	RISK	DEFINITION	INDUST RY RISK LEVEL	RESIDUAL RISK (Anakatech)
CUSTOMER RISKS	1.	Unverified or front accounts	There is a risk that an account may be opened using false information or by someone other than the registered individual for the purpose of carrying out ML/TF activity. An unverified or front account poses a risk as the Company does not know with whom it is transacting.	High	Medium
	2.	High-value depositing customers	Where a high value deposit is made in a single transaction or cumulative deposits of significant value are made over a short time frame, an increased risk of ML/TF activity is posed – the deposit or deposits may represent the proceeds of crime which the customer intends to launder through, or spend with, Anakatech.	Medium	Low

	3.	Politically Exposed Persons (PEPs)	There is a higher risk associated with individuals who have a high political profile or have held public office (past or present), as their positions may make them vulnerable to corruption and bribery therefore increasing the risk of accounts being funded by the proceeds of crime by such individuals.	High	Low
	4.	Prohibited relationships and transactions (sanctions)	There is a risk that an individual subject to sanctions may attempt to open an account and transact with the Company. It is a criminal offence to transact with individuals who are subject to certain types of sanctions such as asset freezes.	High	Low
	5.	Dormant accounts	There is a risk that a customer may deposit funds and then not use his account for a significant period of time before looking to withdraw the funds at a later stage, following very little or no activity, in the hope to distance himself from his crimes by the passing of time.	Low	Low
	6.	Source of funds/wealth is unknown for higher-spending customers	If higher-spending customers are allowed to play without source of funds/wealth being established on a risk-sensitive basis, an increased risk of ML/TF activity is posed.	Medium	Low
	7.	Change to registered	A customer who changes his personal details such as residential address, email address or	Low	Low

		personal details for account holders	telephone number poses an increased ML/TF risk as he may not provide his up-to-date information to us. This poses a particular risk where the outdated information is used as part of ongoing monitoring (for example compromising sanctions screening processes) or enhanced due diligence checks and investigations.		
	8.	Drastic changes in betting behavior	A drastic change in betting behavior (i.e. unusually high activity when comparing to what may reasonably be deemed normal expected activity from the customer in question) may indicate that the account is now being used, by the customer or by someone on whose behalf the customer is acting, for money laundering purposes.	Medium	Medium
	9.	Multiple payment methods	Individuals using multiple payment methods to fund their accounts without obvious rationale behind such behaviour (e.g. registration of a new credit/debit card to replace an expired one) may be attempting to structure deposits representing the proceeds of crime in order to avoid detection. The use of multiple methods enables an individual to easily move funds to other betting sites or bank accounts. This may include both refundable and non-refundable payment methods.	Medium	Low

	10.	Payment card ownership	Where funds are deposited from a card which does not belong to the customer or is a corporate card, there is an increased risk that the customer may be using the card to either deposit unauthorised funds or criminally obtained funds. With corporate cards, there is a risk that a business is being used as a front for criminal activity, therefore corporate cards could be issued to disguise or transfer the proceeds of crime.	Low	Low
	11.	Multiple accounts	There is a risk that a customer may open multiple accounts using different names and identities, making it difficult to verify the real account holder (beneficial owner) and/or the source of the funds.	Medium	Low
	12.	Multiple accounts - different operator	Customers are free to spread their activities across a variety of operators, and each operator may therefore have little in terms of transaction history from which to identify unusual behaviour. This may also result in customer activity levels with single operators falling below internal reporting thresholds in accordance with the risk-based approach, where the customer would therefore not be highlighted for further investigation despite significant levels of deposit or drop activity with all operators.	High	High

	13.	VIP enhancements	There is a risk that VIPs are upgraded onto loyalty/reward schemes without having undergone proper due diligence, therefore potentially rewarding customers who have deposited the proceeds of crime with the operator. Additionally, considering the higher monetary values involved in such relationships, should any operator AML/CTF failings be published, they are likely to attract significant national press interest, negatively impacting on public perception of the integrity of the gambling sector.	Medium	N/A
	14.	Customer-to customer fund transfers	There is a risk that customers could pass the proceeds of crime from one account to another account held with us (belonging to a different individual) in order to create distance and confuse the money trail or transfer funds as a way of paying for goods or services related to criminal activity. For example: live games	High	Medium
PAYMENT RISK	1.	Cash-based payment methods	Customers using cash-based payment methods pose a higher ML/ TF risk as the source of funds is in the main unknown and difficult to trace. This type of payment method is often also non-refundable, meaning that withdrawals must be processed via an alternative source. The main risk is that customers may abuse these	Medium	Low

			characteristics in order to carry out ML/TF activity through their betting accounts.		
	2.	eWallet payment methods	eWallets payment methods are potentially higher-risk payment methods as potential means to mask the true origins of the deposited funds. The use of eWallet payment methods enables an individual to move funds easily to other betting sites, bank accounts or spend via associated debit cards. A customer depositing via an eWallet may pose an increased ML/TF risk to Twino as the source of funds is difficult to be traced and this payment method type offers a relative level of anonymity to the customer.	Medium	Low
PRODUCT RISK	1.	Withdrawing without play/ low-risk wagering/ covering all outcomes/ cash out	There is a risk that a customer may deposit criminal funds into his account and then withdraw them without wagering in any product, following minimal play, low-risk wagering activity, by covering all outcomes or by using the cash out facility	Medium	Low
	2.	Peer-to-peer gambling	Poker is classed as a higher-risk product for ML/TF purposes due to the potential for collusion and soft play as there is a risk for money to be deliberately passed between players on the same network which could be the proceeds of crime or funds could be passed to pay for goods or services related to criminal	Medium	Low

			activity. The Company doesn't offer this product to its customers.		
EMPLOYEE RISK	1.	Employee	Employees potentially pose a significant ML/TF threat by means of collusion through play, product or record manipulation. Without appropriate identification processes in place, operators may become vulnerable.	Low	Low
	2.	Staff knowledge	Employees may pose a significant risk where they have either not received adequate training to enable them to identify potential ML/ TF issues, or where they are unable to highlight such issues through the established channels. Without sufficient training and standards in place, there is a risk that staff may become involved in assisting in the commission of a ML offence.	High	Low
GEOGRAPHIC AL RISK	1.	Activity from outside a customer's registered country	A customer logging into his account from outside of his registered country poses a potential risk to Twino as the customer may not be who he claims to be and the information used to verify the account as well as the source of funds may be incorrect. This can pose an increased level of risk when logins are made from high-risk countries.	Low	Low
	2.	Mismatch in country of	There is a risk that a customer may be attempting to send funds to a source outside of	Low	Low

		residence/card country/bank country	his residential country in order to disguise the origin and/or the destination of the funds. This can pose an increased level of risk where payments come from high-risk countries.		
	3.	Accepting business from high-risk jurisdictions	There is a risk that customers from countries which have been highlighted by sources such as FATF as having strategic AML/CTF deficiencies look to abuse the sector for ML/TF activity. There is also a risk when accepting customer from countries that have high levels of corruption as this increases the risk of ML taking place.	Medium	Low
UNUSUAL ACTIVITY	1.	Unusual activity	There is a risk that instances of unusual activity are not escalated by employees where there is an indication that a customer and/or employee may be involved in potential ML/TF activity. This is applicable to the Customer, Payment, Product, Employee and Geographical risk areas.	Low	Low

2. Additional risk to be considered

New methods of payment by customers: In 2024 Twino has added additional deposit options to the already available methods as Skrill, Neteller and Paysafecard.

Skrill – Skrill is an e-wallet, part of the FCA-licensed Paysafe Group. As such, the company adheres to strict AML rules and has a robust KYC process to allow their customers to operate the e-wallet, minimizing and mitigating the risks that arise from the service they offer

Neteller – Neteller is a part of the same group of companies as Skrill and as such has adopted similar measures to prevent the use of the platform form

PaySafeCard – PaySafeCard is a prepaid online payment method based on vouchers with a 16-digit PIN code, independent of bank account, credit card, or other personal information. Customers can purchase vouchers at local sales outlets and pay online by entering the code at the checkout of the respective website

Pre-paid card (vouchers) for depositing on the player account are considered as more vulnerable to criminal exploitation because they provide customers with the possibility to mask their identity and their source of funding. These pose a high ML/TF risk as the purchaser of the vouchers might not be legitimate and it is difficult to carry out the same level of checks as may be performed on accounts held with financial institutions. Upon acceptance of prepaid cards, the same risk as for cash acceptance is present as the gambling operator is not able to make the same checks when prepaid cards are used, as they have in cases of regular bank accounts. If prepaid cards are accepted, it must therefore be included in the risk assessment. Customers who often use prepaid cards should therefore be categorized as high-risk customers and enhanced due diligence to be performed. Also, particular attention needs to be paid to customers who might be funding their play through money derived from crypto assets, since these are usually subject to specific requirements due to their high-risk nature.

Geographic Risk/Country Risk- Some countries pose an inherently higher money laundering or fraud risk than others. Customers will be checked for both their current IP and their issuer bank country (when available) in order to mitigate such risks.

If the issuer country of a credit card is different from the player's country the player will be subjected to enhanced due diligence. The country/geographic risk can also be considered in conjunction with the customer risk. The geographical risk arises from the geographical jurisdiction associated (by either nationality, residence, place of birth or source of funds) with the customers and third-party partners of Twino . We suggest including the following factors (accompanied each by a recommended source for establishing the actual "high risks" jurisdictions in these areas):

- AML/CTF - jurisdictions that do not have a satisfactory AML regime: The FATF [list](#);
- Corruption – jurisdictions known for high-corruption levels, funds originating from these jurisdictions may be "tainted": [Transparency International's global corruption index](#) (CPI)
- Terrorism – jurisdictions subject to international sanctions in connection with terrorism and/or jurisdictions which are known to have terrorist organizations operating within are to be considered as high risk: the "Terrorist Safe Havens" in the [US Department of State annual Country Report on Terrorism](#)
- Drugs – jurisdictions that are known as significant illicit drug manufacturers may pose a higher AML risk: the [US International Narcotics Strategy Control Report \(INSCR\)\]](#)

No	Area	Risks	Impact if Exploited	Overall Risk Level
1.	Money Laundering activity due to playing from a country that does not possess a satisfactory AML/CTF regime.	Money Laundering Activity from high-risk jurisdictions.	Moderate	Low
2.	Corruption by playing from a jurisdiction with high-corruption levels.	Illegal movement of funds Money Laundering	Moderate	Low
3.	Terrorist financing from from a jurisdiction subject to international sanctions.	Terrorist Financing	Moderate	Low

4.	Drugs financing	Illegal movement of funds Money Laundering	Moderate	Low
5.	Politically exposed persons (family members)	Illegal movement of funds Money Laundering	Moderate	Low

Third party reliance and outsourcing: Outsourcing performance of the money laundering obligations to a third party can be a risk factor in itself, thus control and accountability needs to be ensured. Outsourcing is defined as the use of a third party to perform a process, service, or activity on behalf of the operator, which would otherwise be undertaken by the operator itself. In a 'third-party reliance' scenario, the third party, which must be an entity in an EU Member State or a reputable jurisdiction, which is subject to AML/CFT requirements and supervision equivalent to those required in terms of applicable EU legislation, will usually have an existing business relationship with the customer, which is independent from the relationship of the customer with the relying operator, and would apply its own procedures to perform the CDD measures. However, even when relying to third party for certain aspects of the CDD, we as an operator remain ultimately responsible for compliance with our CDD obligations.

V. PREVENTION

Our approach to ML and TF is outlined as part of a four-stage approach for our Curacao operations and includes:

- AML/CTF Policy which outlines at a high level internally our commitment to put in place robust measures to ensure that efforts to launder the proceeds of crime are prevented or, where efforts cannot be prevented, to report incidents in accordance with our legal obligations.
- The current Risk Assessment, which is an ongoing process with regard to how the company could be used for ML/TF. Our AML risk assessments provide the basis for designing and upholding processes and procedures to highlight potential risks for attention. The risk assessment takes account of the respective risk assessments made available by MGA and/or FIU.
- AML Operations Guidance for internal stakeholders, highlighting our AML organisation, legal obligations, suspicious activity reporting protocols, and a summary of the procedures put in place to detect and mitigate ML & TF risks.
- AML Processes which describe the practical processes and systems specific to each jurisdiction and division to monitor customer activity for the purpose of identifying concerning or suspicious activity and conducting further investigations.

1. Customer Due Diligence & Ongoing Monitoring (KYC)

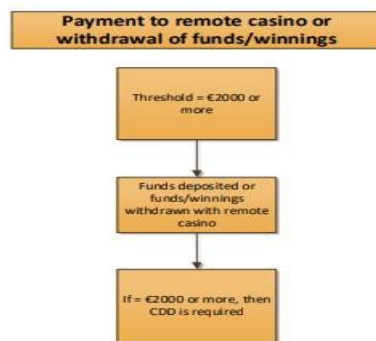
The best protection against abuse by money launderers is to know your customer – this is done through Customer Due Diligence (CDD). CDD refers to all processes and controls applied to ensure that at all stages of the business relationship we have a clear understanding of who the customer is and his behavioural pattern.

The main aim of CDD is to make sure that we have effective mechanisms in place in order to: (i) Identify a customer; (ii) Verify customer's identity; (iii) Establish the purpose and intended nature of the business relationship along with the customer's business and risk profile, and; (iv) Monitor customer's activity on an on-going basis to reduce fraudulent and ML/TF activity during the life cycle of a customer - based on internally developed triggers and constant monitoring by the appointed AML office. In our capacity of online casino operator, CDD has to be carried out at the

EUR 2000 threshold being reached (if not requested earlier).

We have systems in place to meet requirements to verify the identity, address, and date of birth of customers in our regulated online gambling business prior to any gambling activity. Customer's identity is verified further where required by Money Laundering Regulations at certain thresholds to satisfactorily reduce the potential specific risk posed by non-face-to-face business. Verification of customer identity involves verifying the customer information against documents or information (i.e. from 3rd party verification services) obtained from a reliable and independent source. Our Know Your Customer teams are responsible for this process. Our business seeks to establish customer identity on a risk-based approach in line with monitoring processes and regulatory guidance.

Figure 7: Determining when the threshold is reached (remote casinos)



Note:
Risk-based approach – operator analysis of spending behaviours and an objective assessment made of the likelihood of customers reaching the threshold. Measures then put in place need to capture all customers likely to hit the threshold.

Ongoing monitoring involves our AML teams reviewing customer's activity against prevailing procedures. This includes, for example, proactive risk-based customer's spent threshold reviews, reviews following internal suspicious activity reports, and reactively investigating adverse media or law enforcement alerts. Further enhanced due diligence, including source of funds and wealth are considered as appropriate in this framework, including ones in respect of PEPs. The frequency of ongoing customer review is determined by the framework and risk-based approach and managed through relevant case management systems.

Our Risk Operations function maintain rule sets to prevent and/or flag potential account risks in respect of geolocation, payment methods, and multiple accounts.

2. Enhanced customer due diligence measures

Where the risk associated with a business relationship is increased, we must apply enhanced customer due diligence measures (EDD) to manage and mitigate those high risks appropriately (e.g., where transactions are complex, unusually large or conducted in an unusual pattern). We apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks, especially in the following cases:

- in any case identified by the operator or in information provided by the Commission to the operator where there is a high risk of money laundering or terrorist financing;
- in any business relationship with a customer situated in a high-risk country identified by the European Commission or in relation to any transaction for which the operator is required to apply CDD measures, where either of the parties to the transaction is resident in a high-risk country;
- if the operator has determined that a customer or potential customer is a PEP, a family member or a known close associate of a PEP;
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the customer;

- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose;
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In the case of business relationships with customers situated in high-risk countries or transactions where either of the parties to the transaction are resident in a high-risk country, the enhanced measures undertaken includes:

- obtaining additional information on the customer and on the customer's beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
- obtaining information on the reasons for the transactions;
- obtaining approval of senior management for establishing or continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

VI. RECAPITULATION

During the annual preparation of the risk assessment report the Compliance officer considers if there are any additional risk factor or group of risk factors that must be added to the risk assessment. The monitoring of risks is carried out continuously on a daily basis with internal policies and procedures updated immediately when necessary.

With the addition of two e-wallet and three cash voucher options to the existing deposit options, the transaction risk has increased. For this reason Twino puts special effort in the monitoring

of transaction and wagering activity of players who use the high-risk methods and ensuring the proper levels of due diligence.

Regarding the product risk factors, it has to be considered that the main two products – scratch cards and slot machines in comparison to the roulette, blackjack, and other casino games, do not offer many opportunities to customers with suspicious behaviour. With the Blackjack and Roulette games, the same measures and the overall interest were closely monitored in order to exclude any potential risky behaviour in 2024 and will continue to be monitored in 2025.

The EDD check also includes affordability assessment, PEP and additional financial sanctions checks, where the customers who passed the last two checks are additionally checked using the services of the Ongoing monitoring system in order to remove the false positive results. 0 customers were identified as being part of the financial sanctions list. 0.7 % of the registered customers on in 2024 were identified as PEPs, where the false positive results because of a name match are also included. There have been zero positive matches.