

Trivico B.V.

Curacao – AML Policy

Document Control

Criteria	Information
Licence	Curacao
Document Title	Anti-Money Laundering Policy

Version	1.0
Effective Date	31/05/2025
Approved By	MLRO
Approval Date	28/05/2025
Department	Legal & Compliance Department
Document Owner	MLRO
Document to be updated on	28/05/2026

Document history

Date	Updated information	Version
28/05/2025	Creation of Policy	1.0

Preface

TRIVICO B.V. (the Company) is firmly committed to conducting its business in full compliance with both the letter and spirit of all applicable anti-money laundering (AML) and counter-terrorist financing (CFT) laws and regulations in every country and territory in which it operates.

This policy encompasses all relevant AML/CFT procedures and escalation protocols applicable to the jurisdictions covered under TRIVICO B.V.'s Curaçao gambling licence, as issued by the Curaçao Gaming Authority (hereinafter referred to as the "Curaçao market").

The Compliance Officer (CO), Senior Management, and the Board of Directors are actively involved in identifying, assessing, and managing money laundering and terrorist financing risks. They play an integral role in the decision-making process to ensure that all policies and procedures align with applicable legal and regulatory requirements.

Table of Contents

1. Introduction	3
2. The Risk-based approach.....	5
2.1. The Business Risk Assessment (BRA).....	5

2.2. The Customer Risk Assessment (CRA)	5
3. Customer Due Diligence (CDD).....	7
3.1. When is CDD applied?	7
3.2. Identification	8
3.3. Verification	9
3.4. Purpose and Nature of the Business Relationship.....	11
3.5. What Documents?	12
3.6. How is CDD Conducted?	14
3.7. Ongoing Monitoring.....	15
3.8. Enhanced Due Diligence (EDD)	16
3.9. Simplified Due Diligence (SDD)	17
4. Reporting	17
4.1. Reporting of unusual transactions	18
4.2. Record Keeping	18
5. Anti-Money Laundering Compliance Program	19
5.1. Employee Screening Program	19
5.2. Employee Training Program	20
5.3. Compliance Officer (CO):.....	20

1. Introduction

- i. **Money laundering** (ML) refers to the process of disguising the proceeds of crime and corruption as legitimate assets. It typically involves three key stages: first, the illicit funds are introduced into the financial system ("placement"); second, a series of complex financial transactions are carried out to obscure the origin of the funds ("layering"); and third, the laundered money is re-integrated into the economy as seemingly lawful assets ("integration"). Depending on the specific circumstances, some of these stages may be bypassed.

- ii. **Terrorist financing (FT)** - The process by which terrorists fund their operations to perform terrorist acts. The main difference between money laundering and terrorist financing is that terrorist financing can be derived from legitimate funds, whereas money laundering is always derived from illicit activity.
- iii. **Proceeds of Crime** - Proceeds of crime refer to funds obtained through unlawful means, which may provide financial benefit or personal gain. Even if the intent is not to launder the money or finance terrorism, the activity remains illegal. Therefore, subject persons are required to treat such instances with the same level of scrutiny as money laundering or terrorist financing and must report them accordingly.
- iv. **Predicate offence** - A predicate offence is a criminal act that generates illicit funds, which then become the basis for money laundering activities. Money laundering cannot occur without the existence of such unlawfully obtained proceeds. The European Union's 6th Anti-Money Laundering Directive (6AMLD) outlines 22 predicate offences, including but not limited to drug trafficking, fraud, cybercrime, bribery, kidnapping, and arms trafficking. These crimes produce illegal financial gains that are often subject to laundering in an attempt to conceal their criminal origin.
- v. **Sanctions** - Sanctions are international measures targeting specific countries, entities, or individuals. TRIVICO B.V. complies with all applicable anti-money laundering (AML) and counter-terrorist financing (CFT) laws, including those under the 4th EU Anti-Money Laundering Directive and national regulations linked to its Curaçao gambling license.

The company also adheres to relevant legal obligations in jurisdictions where it serves customers. Sanctions lists (SLs) must be observed in line with Curaçao's international commitments and those of the EU and other licensing countries.

Compliance with the Sanctions National Ordinance (N.G. 2014, no. 55) and the Kingdom Sanctions Act (N.G. 2016, no. 54) is a key component of TRIVICO B.V.'s efforts to prevent money laundering, terrorist financing, and the financing of weapons proliferation.

The scope of this Policy is to establish policies from which procedures on internal control, risk assessment, risk management and compliance in relation to AML/CFT will be drawn up.

As a gambling operator licensed in Curaçao, TRIVICO B.V. understands that it must comply with the following legislations:

- **The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);**
- **The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);**
- **Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);**
- **Sanctions National Ordinance (N.G. 2014, no. 55);**
- **Kingdom Sanction Act (N.G. 2016, no. 54);**
- **National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);**
- **National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);**

- **National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);**
- **National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);** • **National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);**
- **The Code of Criminal Law (Penal Code) (N.G. 2011, no.48).**

This Policy is grounded in the applicable laws and regulations governing the Curaçao Gaming Sector, which form the primary legal basis for combating money laundering, terrorist financing, and the proliferation of weapons.

Unless otherwise stated, terms used herein shall carry the same meaning as defined under the relevant legal and regulatory provisions.

This AML Policy sets out the Company's internal standards for AML/CFT compliance, which are to be followed by all management and employees.

2. The Risk-based approach

The Company assess its exposure to money laundering and terrorist financing risks by identifying the most likely ways it could be exploited. Based on this assessment, a risk-based approach to Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and transaction monitoring is developed and documented herein. Approval of this policy by the Board of Directors constitutes formal approval of both the underlying risk assessment and the risk-based approach.

2.1. The Business Risk Assessment (BRA)

The Company performs an annual (minimum) Business Risk Assessment in order to:

- Identify ML/FT Vulnerabilities.
- Identify ML/FT Threats; and
- For each issue identified, assess the level of risk based on frequency, likelihood, and impact.

Based on findings from the BRA, measures, policies, controls and training are reviewed in order to minimise new/existing risks. Substantial changes to the Company's system, process and operation or changes to the licencing conditions can also trigger a BRA review. Such assessment and any outcomes are to be kept on file and made readily available for review upon request.

The MLRO incorporates relevant supranational, national, and sector-specific risk assessments into the company's overall risk evaluation. The resulting BRA is formally documented and approved by the Board of Directors. This assessment is reviewed annually, or earlier if there are significant changes in the regulatory landscape, the company's operational environment, business structure, activities, or prior to the launch of new gambling products.

2.2. The Customer Risk Assessment (CRA)

A key element of the risk-based approach is the assessment of customer relationships through the Customer Risk Assessment (CRA). This process enables the Company to identify, understand, and appropriately manage risks associated with individual customers by applying tailored control measures.

TRIVICO B.V. utilizes a third-party AML/CFT platform to perform CRAs across its entire registered customer base. This advanced solution provides real-time transaction monitoring, customer due diligence (CDD), source of wealth/funds (SOW/SOF) verification, document management, and immediate customer risk profiling. It supports the company in establishing a customer's business and risk profile at the outset of the relationship.

The monitoring system is configurable to detect specific risk indicators, including but not limited to:

- Transactions exceeding predefined thresholds
- High frequency of transactions within a given period
- Unusual or anomalous account activity (e.g., gameplay spikes, non-wagering behavior, or non-closed loop transactions)
- Involvement of individuals listed on international sanctions lists
- Transactions involving politically exposed persons (PEPs)
- Activity linked to high-risk jurisdictions
- Transactions inconsistent with the customer's known risk profile
- Adverse media that may affect a customer's risk status
- Accounts under enhanced ongoing monitoring
- Accounts requiring review due to expired documents or outstanding due diligence requests

This risk-based monitoring framework ensures that TRIVICO B.V. can proactively detect and respond to potential money laundering and terrorist financing threats.

As part of its ongoing Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) obligations, TRIVICO B.V. conducts a comprehensive Customer Risk Assessment (CRA) based on four primary risk pillars:

- **Customer Risk** - Customer risk refers to the exposure to ML/FT risk arising from the nature and profile of the customer. Contributing factors include the customer's business or professional activity, public reputation, known involvement in high-risk sectors, political exposure (e.g., status as a Politically Exposed Person), and other characteristics inherent to the customer.
- **Geographic Risk** - Geographic risk is associated with the jurisdictions connected to the customer. Risk levels vary based on the strength and effectiveness of AML/CFT frameworks in those jurisdictions. Relevant geographies may include:
 - i. The country in which the customer is established or primarily operates;
 - ii. Jurisdictions where the customer derives wealth or conducts significant business; and/or
 - iii. Countries linked to the customer or its beneficial owner through residency, citizenship, or close personal ties
- **Product and Service Risk** – This refers to the inherent risk involved in the products or services offered. Key factors influencing this risk include:

i. The degree of transparency or anonymity the product provides; ii. The complexity of the product or service structure; iii. The value or volume of transactions typically associated with the product.

- **Channel and Interface Risk** - This risk arises from the channels used to establish and maintain the customer relationship. It includes the method of delivery and interaction, such as face-to-face or non-face-to-face engagements. While non-face-to-face interactions are not automatically highrisk, they are assessed in the context of the product, customer type, and overall risk profile.

Each of the four risk pillars is further broken down into sub-parameters. These are applied on a caseby-case basis, taking into account:

- The type of subject person using the system;
- The nature of the customer's activities and their role in such activities;
- The customer classification (e.g., individual, legal entity, high-net-worth, PEP).

The company has also developed a Customer Acceptance Policy which (i) describes the category of players that are likely to pose a higher risk of ML/FT than others (ii) showcases the level of CDD measures and ongoing monitoring to be applied (iii) explains the risk indicators presenting low, medium and high risk and (iv) circumstances under which a player is declined an account.

All customers ("Players") are subject to a risk assessment at the time of onboarding. This risk rating is dynamic and will be automatically updated based on the customer's ongoing activity, including product usage, transaction behaviour, and payment methods.

Where there is a change in customer activity that may affect the assessed risk level, TRIVICO B.V. will initiate a risk review. Priority is given to customers classified as Critical or High Risk. These reviews are conducted on an ongoing basis after the establishment of the business relationship and may result in one or more of the following actions:

- Implementation of additional Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) measures;
- Termination of the business relationship;
- Submission of a Suspicious Transaction Report (STR) to the relevant Financial Intelligence Unit (FIU);
- Requests for supporting documentation, including Source of Funds (SoF) and Source of Wealth (SoW).

3. Customer Due Diligence (CDD)

3.1. When is CDD applied?

Section III.1 of the Regulation for combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass destruction (Curacao AML/CFT Regulation) stipulates that the Company is required to perform CDD when any of the below thresholds are reached:

- Players engage in financial transactions equal to or above Naf. 4,000;
- Carrying out occasional transactions above the monetary equivalent of Naf. 4,000;
- There is a suspicion of money laundering or terrorist financing; or
- They have doubts about the veracity or adequacy of previously obtained customer identification data.

Since the company operates as a “card not present merchant” and non-customer facing, in addition to the above, CDD may also be applies in the following situations:

- Doubts about the authenticity, accuracy, or adequacy of previously obtained customer identification or verification information.
- Suspicion or knowledge of criminal proceeds, money laundering, or terrorist financing, regardless of thresholds or exemptions.
- Multiple account registrations from the same IP, device, or identity, or any attempt to circumvent system controls.
- Reaching the EUR 4,000 transaction threshold, in line with AML regulatory requirements.
- Use of third-party funding.
- Changes in signatories, beneficial owners, or controlling persons.
- Suspicion that the customer or their account is involved in ML/TF activity.
- Identification or reclassification of the customer as a Politically Exposed Person (PEP).
- Expired or invalid identification documents, or changes in customer information (e.g., name, address, gender).
- Any material change to the customer's identity or documentation.

3.2. Identification

Customer identification involves the collection of specific personal information to establish and verify the identity of the individual entering into a business relationship with the company.

All registering players are required to provide complete and accurate information during the account registration process. The following personal details must be submitted as part of regulatory requirements under remote gaming and AML obligations:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Official identity number (e.g., national ID or passport number)

Account activation must be completed through a verification process using either the registered email address or phone number. A confirmation link or code is sent to the player as evidence of validity.

The company strictly prohibits the registration of any individual below the legal age of majority—18 years, or higher if stipulated by the jurisdiction of residence. Date of birth is a required field and is validated to ensure age compliance.

In the event a minor is found to have registered:

- The business relationship shall be immediately terminated due to a breach of the platform's Terms and Conditions.
- All bets, winnings, and bonuses shall be forfeited. • Any remaining deposit balance shall be refunded.
- The account will be permanently blocked.

All newly created accounts are subject to a review for data integrity. Any irregularities or suspicious indicators will result in account suspension and may trigger a simplified or standard due diligence process, based on the risk level and nature of the concern.

3.3. Verification

Verification involves confirming the personal information collected during the identification process by using data, documentation, or information obtained from independent and reliable sources. The specific personal details to be verified, as well as the extent of verification required, are determined in accordance with the customer's overall risk rating.

The applicable level of due diligence is outlined in the Risk Matrix provided below.

System Risk Rating	Action	Level of Due Diligence
Low	• Verification of Identity Information (including full name, residential address, date of birth, nationality) • Apply ongoing monitoring.	Simplified Due Diligence (SDD)
Low - Medium	• Verification of Identity Information (including full name, residential address, date of birth, nationality) • Analyse player logins and links • Apply Ongoing Monitoring	Basic Customer Due Diligence (SDD/CDD)

Medium	• Verification of personal details through photographic documents (such as government-issued ID or passport, utility bills for residential address) and/or Bank ID. • Apply enhanced ongoing monitoring. Obtain • SOW info (e.g. Occupation, Industry, expected level of spend, annual gross income, additional nationalities) • Background Check (OSINT)	Customer Due Diligence (CDD)
Medium - High	• Verification of personal details through photographic documents (such as government-issued ID or passport, utility bills for residential address). • Obtain SOW info (e.g Occupation, Industry, expected level of spend, annual gross income, additional nationalities) • Customer to provide selfie while upholding identification document. • Provide copies of registered payment methods used on the casino account. • Background Check (OSINT) • Apply enhanced ongoing monitoring. •	Additional Customer Due Diligence (CDD)
	• Verification of personal details through photographic documents (such as government-issued ID or passport, utility bills for residential address).	

High	• Provide copies of registered payment methods used on the casino account. • Obtain copies of SOW/ SOF such as Payslips and Bank statements confirming Occupation and income. • Apply enhanced ongoing monitoring/terminate the business relationship. • Raise an internal STR	Enhanced Due Diligence (EDD)
Critical	The business relationship is permanently terminated on the basis that; • The customer risk falls outside the business's risk appetite and risk tolerance. • There is enough ground to suspect or confirm proceeds of crime. • The customer has breached the terms and conditions (forged documents, identity fraud, chargebacks) • There has been contact from the local authorities requesting information on a particular subject based on fraud or Money laundering charges. • The customer is sanctioned. • An STR/SAR has been raised externally to the FIU	No other Due Diligence is needed.

3.4. Purpose and Nature of the Business Relationship

Part III.2.3 of the Curacao AML/CFT Regulation states that the purpose of opening a gaming account is generally clear, and therefore casinos are not required to obtain additional information from customers solely for this reason. Nonetheless, it remains essential to collect adequate information and, when necessary, supporting documentation to verify the customer's source of wealth and anticipated level of activity.

3.5. What Documents?

Verification is typically conducted using documents obtained from sources that are both reliable and independent. An “independent” source is one that is separate from the customer, while a “reliable” source is reputable and trusted to provide accurate information. Therefore, customer declarations alone do not meet verification requirements, as they lack independence; however, such statements may still be useful for other aspects of Customer Due Diligence (CDD). Similarly, statements from individuals who are merely acquaintances of the customer do not meet the reliability standard.

Examples of independent and reliable sources include, but are not limited to:

- a government authority, department or agency;
- a regulated utility company; or
- a subject person carrying out relevant financial business in Malta or equivalent activities in a Member State of the EU or in a reputable jurisdiction (such as a bank, financial institution or investment services firm)

TRIVICO B.V **accepts** the following types of Identification documents:

- Driver’s License (Provisional Also Accepted)
- Residence Permit Card (front and back)
- National ID card (Front and Back)
- Temporary ID card (Front and Back)
- Passport (Showing MRZ and passport number)
- Bank cards with Photo ID and DOB on the backside. (Norway Only)

TRIVICO B.V **does not** accept the following as proof of Identity:

- Proof of Age verification (18+ cards)
- Library Card
- Expired Identity Card
- Donor ID Card
- Tax ID card
- Voter ID

TRIVICO B.V **accepts** the following proof of address:

- Copy of bank statement in a PDF-format.
- Copy of a Utility bill • Online bill in PDF-format.
- Property Tax Receipt
- Local tax bill
- Any form of ID or Driving License which holds an address (ex; Malta, Poland, Germany ID cards)
- Certified Tenancy Letter of agreement

TRIVICO B.V **does not** accept the following as proof of address:

- Pay slips (the reason is that employees can state an address to their employer and receive the pay slip without it being sent to the address)
- Screenshots of invoices or customer details deriving from eBay, PayPal or similar (accounts without 2FA such as eBay or PayPal are not accepted to verify one's address. Furthermore, such information can easily be changed or updated without further DD checks from the provider's side.)
- Any hand-written document used as Proof of address
- Screenshot or photo of address in closed mail
- Mobile bills

Documents used for verification must be no older than six (6) months at the time they are submitted to the Firm. An exception applies to lease contracts or agreements, where the six-month rule does not apply; however, it must be confirmed that the lease remains valid and current.

An additional reliable and independent method of verification is through Bank e-ID, a secure electronic identification system widely adopted in several European countries, including Norway, Finland, and Sweden. Bank e-ID offers a personal and secure means of verifying identity and electronically signing documents. Its uniqueness significantly reduces the risk of identity fraud or impersonation.

This method is implemented via the Zimpler's Pay N Play mechanism and is mandatory for all new and existing Finnish customers.

The Company integrates with Zimpler through an API interface, allowing Zimpler to automatically transmit the customer's personal information, such as full name, date of birth, and address, to the Company's back-end systems. Additional contact details are then collected directly from the customer during onboarding through the Company's registration portal.

The identification information received from Zimpler is provided to TRIVICO B.V in the form of a bank ID certificate, which Analysts can download at any given time. Information contained in this certificate includes;

- End User ID
- Full Name,
- Personal ID
- Date of Birth,
- Gender
- Address,
- Postal Code
- City
- Method of Verification
- Time of Verification
- Verification ID
- Bank Account Number

As the information is received directly from Zimpler, a regulated entity, the identification and verification data provided is deemed authentic and reliable.

Should any customer identification details change (e.g., use of a new bank account for deposits or transactions), Zimpler detects and updates this information automatically, allowing the Firm to access the most current data at any time.

A Bank ID verification is performed upon the customer's first deposit and is repeated with each subsequent deposit.

When a customer reaches the 4,000 NAF threshold, in line with CGA requirements, Bank ID verification is considered sufficient for Customer Due Diligence (CDD), provided no additional risk factors arise. Unless an increase in the customer's risk profile is identified (as outlined in the Risk Matrix), the customer will not be required to submit physical copies of identification documents, as Zimpler's Pay N Play process already fulfills the verification requirement.

3.6. How is CDD Conducted?

A. Bank ID Verification

When a customer makes their first deposit using Zimpler, the system simultaneously creates the account by retrieving personal details directly from the customer's bank or financial institution. To verify the data, the agent must search for the customer in the Zimpler's Back Office (BO) using the External ID under the correct brand. Upon loading, verify that the name, address, and date of birth match the registered customer details. If evidence needs to be retained, the relevant documents can be downloaded from the Back Office itself.

For Zimpler, log into the Zimpler Back Office and navigate to Orders, select a relevant deposit, and click KYC Document. Only successful deposits will have an associated identification number. To verify, select the appropriate date and country code, and ensure the "Deposits" option is checked. Do not select a brand, as this may prevent transactions from displaying due to a known system issue. Clicking the identification number will redirect to a page showing the customer's details, which can then be exported and uploaded to the Firm's Back Office under Address and Age, ID for record-keeping.

Since Pay N Play users are verified through Zimpler's KYC tools, agents are not required to manually verify these customers. The KYC section in the summary page of the customer's profile will already display as verified (green status).

The agent's responsibility is to ensure that the customer's details in Zimpler match the information in the company's Back Office. After confirmation, update the account's notes/comments and status accordingly. The relevant system tag will be applied automatically. Finally, update the customer category to "Real User Verified (C1)."

B. Termination of Business Relationship

If a customer fails to provide the required identification details and/or supporting documentation within 30 days of reaching the €4,000 threshold, their account will be closed under the status '**CLOSED_FOR_KYC_FAIL**' with the note: '**RFP – Account Closed. KYC Failure**'.

Verification Tags and Notes - When a document fails verification, the appropriate reason must be selected from the KYC Status Fail Reason drop-down menu. If the specific reason is not listed, select 'Other' and choose from the extended list of available options. Common KYC Failure Reasons include:

- Incorrect or invalid document
- Unofficial document
- Incorrect file format
- Expired document
- Missing front and/or back of the document
- Information does not match customer records
- Poor image quality
- Document is older than six (6) months

3.7. Ongoing Monitoring

A critical component of an effective due diligence program and risk-based approach is the implementation of ongoing monitoring and periodic screening, particularly where customer risk has materialized or follow-up is warranted after a review.

Following the establishment of a business relationship, the Company is required to carry out ongoing monitoring, which consists of two primary measures:

- **Transaction Monitoring:** Reviewing transactions throughout the relationship to ensure they align with the Company's understanding of the customer's profile, expected activity, and overall risk level.
- **Information Maintenance:** Ensuring that all relevant documentation, data, and customer information is accurate and up to date. Customer risk assessments may be updated as part of this process to reflect any new or revised information.

In line with these obligations, Companyup will re-assess a customer's risk profile each time they reach a new deposit threshold. This approach helps maintain an accurate and current understanding of the customer and ensures that risk levels are properly evaluated over time.

To support this, the Company has developed a standardized Customer Risk Assessment (CRA) template for use at the following deposit thresholds:

- €2,000
- €10,000 • €25,000
- €50,000
- €100,000

As a customer's lifetime deposits grow, additional information is required once higher thresholds are met. The AML Analyst completes the relevant template, which is then uploaded to the customer's profile on KYC Matic. These templates are available in the AML section of the company's JIRA. The firm must maintain processes to monitor and update CDD documentation according to each customer's risk profile, including:

- Collecting updated identification documents upon expiry, either based on risk or specific triggers.
- Investigating any inconsistencies found in existing data, regardless of how they are discovered.

- Periodically reviewing and updating data on a risk-sensitive basis when documents are valid and no inconsistencies exist.

The AML transaction monitoring tool automatically flags expired or outdated documents. The frequency of these monitoring activities is detailed in the following Matrix (if no additional triggers are present).

Critical Risk Players	Business Relationship is Terminated
High Risk Players	Every 12 months
Medium - High Risk Players	Every 15 months
Medium Risk Players	Every 18 months
Low - Medium Risk Players	Every 21 months
Low Risk Players	Every 24 months

Once an account is triggered for a follow up this will be listed in the 'Tasks' as an action item to do. The AML Analysts will then follow up and review the account accordingly.

3.8. Enhanced Due Diligence (EDD)

EDD is required when the customer and the associated product or service present a higher risk level. This elevated due diligence is necessary to effectively mitigate the increased risk. High-risk scenarios typically arise when there is a greater potential for money laundering or terrorist financing through the business relationship.

The scope and nature of EDD measures depend on the specific risk identified. Additional due diligence may include, but is not limited to, obtaining further information to verify the customer's identity or source of funds, or conducting adverse media checks. These measures are applied on a case-by-case basis and are proportionate to the level of risk, ensuring confidence that the risk is managed and unlikely to materialize.

Examples of high-risk situations include, but are not limited to, non-face-to-face customer interactions or dealings with politically exposed persons (PEPs). It is important to note that identifying a customer as high risk does not imply involvement in criminal activity, but rather indicates an increased potential exposure to such risks.

A. When does the Company apply EDD measures?

Listed below is a non-exhaustive list of scenarios where EDD would be applied. However, this would depend upon different factors and is subject to the risk transpiring or whether the source of the information is reliable.

- The subject is linked to or resides in countries listed as High-Risk Third Countries or where AML controls are known to be deficient.
- Politically Exposed Persons (PEPs), Heads of International Organizations (HIOs), or their immediate family members and close associates.
- Use of higher-risk payment methods, such as prepaid options like Paysafe or prepaid bank cards.

- Large or frequent deposits, particularly when the customer is evasive or provides unconvincing explanations about the source of funds.
- Doubts regarding the authenticity or accuracy of customer documents, including suspected forgeries or counterfeits.
- Customers with high-risk occupations or whose declared spending is inconsistent with their occupation or known profile.
- Transaction activity that is unexplained or inconsistent with the customer's known profile.
- When the customer risk assessment classifies the account as High Risk (refer to the Risk Matrix).

EDD will consist of the following:

- Collecting additional customer information and updating the customer profile more frequently, including identification details (see the Due Diligence Matrix).
- Investigating the background and purpose of the transaction to the extent reasonably possible.
- Enhancing the monitoring of the business relationship and related transactions to identify any suspicious activity.
- Obtaining approval from the CO or Senior Management before continuing the business relationship.
- Requesting Photo Holding ID
- Investigation with third party payment providers.
- SOW/ SOF (e.g. Bank Statements to verify occupation and source of income).
- Requiring Certified Copies of Documents (notarised and stamped).
- Adverse Media Check (If for a legal entity, this could involve Insolvency and Bankruptcy checks).

If we are unable to complete proper due diligence on a correspondent account, the group CO will decide whether to refuse account opening, suspend transactions, file a suspicious transaction report (STR), close the account, or take other necessary actions.

3.9. Simplified Due Diligence (SDD)

This is the lowest level of due diligence, applied only when a risk assessment confirms that the customer poses a low risk of money laundering or terrorist financing. SDD does not eliminate the requirement to perform Customer Due Diligence (CDD), but allows for a reduced scope or delayed timing based on the lower risk.

When SDD is applied, the justification must be clearly documented in line with the group's risk assessment. Ongoing monitoring must continue to ensure that the low-risk conditions remain valid. Importantly, applying SDD does not exempt TRIVICO B.V. from monitoring for suspicious activity or filing a Suspicious Transaction Report (STR) when necessary.

4. Reporting

All employees, contractors, and consultants engaged by The Company shall, at the commencement of their engagement, be informed of the identity, location, and contact details of the Compliance Officer (CO). Any individual who becomes aware of potentially suspicious activity is required to report such concerns directly to the CO without delay. Reports must be treated with the strictest confidentiality and handled in accordance with internal procedures and legal obligations.

No prior authorisation is required to submit a suspicious activity report. The CO is obligated to record and assess all reports received and to take appropriate action in accordance with applicable laws and regulatory guidance.

4.1. Reporting of unusual transactions

Where the Money Laundering Reporting Officer (CO), whether through internal reporting or other means, knows, suspects, or has reasonable grounds to suspect that:

- funds may be the proceeds of criminal activity;
- a transaction may be linked to money laundering or terrorist financing;
- a person may be involved in, or connected to, money laundering or terrorist financing; • or money laundering or terrorist financing has been, is being, or may be attempted,

The CO shall, as soon as reasonably practicable upon the formation of such knowledge or suspicion, submit a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to the relevant competent authority. This disclosure must be supported by the appropriate identification and related documentation.

Where a report is filed, the CO may suspend the transaction or terminate the business relationship unless doing so poses a material risk of “tipping off” the subject. In such cases, the CO may seek guidance or authorisation from the competent authority before taking further action.

As a general principle, suspicious transactions should not be executed and related business relationships should be terminated. However, if this would result in tipping off the subject, the transaction must proceed, and the business relationship must continue. Where doubt exists, staff must escalate the matter to the CO for a final decision. The CO will maintain a secure and comprehensive register of all SARs/STRs submitted.

The CO will serve as the primary liaison with law enforcement, the Financial Intelligence Unit (FIU), and other relevant authorities, and is responsible for coordinating responses to requests for information and supporting any related investigations.

4.2. Record Keeping

The Company shall maintain comprehensive records of all business relationships and transactions conducted. This record-keeping obligation is essential for ensuring compliance with applicable AML/CFT legislation and for supporting the detection, analysis, and investigation of money laundering and terrorist financing activities.

The following categories of records shall be maintained:

1. **Customer Personal Registration Details**

2. **Customer Due Diligence (CDD) Documentation**, including all information and documents collected for identification and identity verification purposes
3. **Transaction Records**, covering all transactions conducted within the context of a business relationship or as part of an occasional transaction
4. **Additional Relevant Records**, as may be reasonably required to demonstrate compliance with AML/CFT obligations or for statistical and regulatory reporting purposes

All records shall be retained for a minimum period of five (5) years from the date of the transaction or the end of the business relationship, whichever is later. Where necessary, and in accordance with requests from relevant authorities, records may be retained for a longer period. However, the total retention period shall not exceed ten (10) years.

5. Anti-Money Laundering Compliance Program

5.1. Employee Screening Program

The Company is committed to maintaining the highest standards of integrity among its employees. To support this objective, the company implements robust pre-employment screening procedures, which require all prospective employees to provide:

- A valid Police Conduct Certificate
- An up-to-date Curriculum Vitae (CV)

The Human Resources (HR) department is responsible for verifying the integrity and background of all new hires. This process is a critical control to mitigate the risk of the company being exploited for money laundering or terrorist financing purposes.

Despite the use of automated systems in certain compliance processes, human judgement and oversight remain essential. Accordingly, all relevant new hires undergo comprehensive background checks and a structured interview process to confirm the absence of criminal history and to assess their qualifications and suitability for the role.

Should concerns arise regarding the integrity of an existing employee, the company will take appropriate investigative and corrective actions to mitigate potential risks to its regulatory and licensing obligations. In cases where criminal conduct is suspected:

- The employee's access to systems and facilities will be revoked;
- Their employment status will be reviewed;
- Relevant authorities will be notified;
- An internal Suspicious Transaction Report (STR) will be considered or filed where applicable.

TRIVICO B.V. upholds a zero-tolerance policy toward misconduct and prioritizes proactive risk management to ensure the integrity and security of its operations.

5.2. Employee Training Program

The Company is committed to ensuring that all employees—particularly those in customer-facing roles or functions with the ability to detect, prevent, or mitigate money laundering and terrorist financing (e.g., RFP, CS, AML, RG, VIP teams)—are fully aware of their legal obligations and receive regular training in accordance with applicable regulatory requirements.

All relevant staff are trained to understand the nature and methods of money laundering and terrorist financing, and are equipped to identify and respond to suspicious activity. Employees are required to remain vigilant and must not:

- Knowingly or negligently assist in the concealment, transfer, acquisition, use, or possession of criminal property;
- Fail to report knowledge or suspicion, or reasonable grounds to suspect, that another person is engaged in money laundering, terrorist financing, or handling the proceeds of crime;
- Engage in “tipping off” or otherwise prejudice any investigation.

To support this, the company may implement a formal Compliance Training Policy and Procedure. All training will be conducted in line with this framework, ensuring consistency and effectiveness.

Training Requirements:

- **Onboarding:** All new employees must complete AML/CFT training within the first 30 days of employment.
- **Ongoing Training:** Refresher training is provided at least annually, or as soon as practicable in response to:
 - Significant changes to laws, internal policies, procedures, systems, or payment methods;
 - The acquisition of new licenses in additional jurisdictions; ○
The implementation of new tools or technologies.

Training is delivered through a combination of internal and external trainers to balance regulatory expertise with company-specific practices. Both online and in-person formats may be used.

All training sessions are followed by an assessment to evaluate employee understanding of AML/CFT obligations, company procedures, and overall competence. This also serves to measure the effectiveness of the training program.

5.3. Compliance Officer (CO):

A Compliance Officer (CO) is considered as a senior-management level who is independent from day-to-day gaming operations. This individual shall be responsible for overseeing the company’s Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) framework, including the detection, prevention, and deterrence of money laundering and terrorist financing activities.

The CO’s responsibilities shall include but are not limited to:

- **Design and Implementation of the AML/CFT Program** - Develop, implement, and maintain an effective AML/CFT compliance program that aligns with both local and international regulatory standards.
- **Regulatory Compliance Monitoring** - Ensure ongoing compliance with all applicable laws, regulations, and guidance related to the detection and prevention of money laundering and terrorist financing.
- **Internal Policy Adherence Review** - Regularly assess the casino's AML/CFT policies and procedures to confirm adherence and effectiveness, recommending updates where necessary.
- **Staff Training and Awareness** - Organize and deliver regular training sessions for staff on AML/CFT obligations, risk indicators, and compliance protocols to ensure awareness and competence across the organization.
- **Transaction Monitoring and Reporting Analysis** - Monitor transactions and assess whether they meet the criteria for reporting as set forth in the Ministerial Decree on Indicators for Unusual Transactions.
- **Review of Internally Reported Transactions** - Review all unusual transaction reports submitted internally to ensure completeness, accuracy, and consistency with external data or sources.
- **Record Maintenance** - Maintain comprehensive records of all internally and externally reported unusual transactions, ensuring these are available for audit and regulatory review.
- **Reporting and Account Management Procedures** - Establish internal procedures to determine when reporting of unusual transactions should result in the freezing or blocking of customer accounts, while carefully managing the risk of tipping off the individual involved.
- **In-Depth Transaction Investigation** - Conduct enhanced investigation of unusual or suspicious transactions when warranted, ensuring appropriate documentation and escalation.
- **External Reporting** - Prepare and submit Suspicious Transaction Reports (STRs) or Unusual Transaction Reports (UTRs) to the appropriate authorities in a timely and compliant manner.
- **Program Review and Enhancement** - Recommend and implement necessary updates or changes to the AML/CFT program to address emerging risks or regulatory developments.
- **Regulatory and Industry Awareness** - Stay informed of developments in AML/CFT regulations, typologies, and best practices both locally and internationally, and advise management on necessary adaptations.

- **Management Reporting** - Prepare and submit regular reports to senior management outlining the company's efforts, performance, and compliance status related to AML/CFT and counter-proliferation financing obligations.
-