

AML & CFT & KYC POLICY

Version: 1.0

Author: Daniel Tatar

Approver: MAURO ORRU`

Previous Version	Current Version	Review Date	Changes	Editor
---	1.0	MAR-2025	First Cut	N/A

CONFIDENTIALITY DISCLAIMER:

THIS DOCUMENT AND THE INFORMATION IN IT ARE PROVIDED IN CONFIDENCE, FOR THE SOLE PURPOSE DISCUSSED BETWEEN **DYNAMIK MARKETING B.V.** AND THE INTENDED AUDIENCE, AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY OR USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF A DIRECTOR OF **DYNAMIK MARKETING B.V.**

Definitions & Abbreviations

- 1. AML - Anti-Money Laundering*
- 2. BRA - Business Risk Assessment*
- 3. CDD - Customer due diligence*
- 4. CFT - Combatting the financing of terrorism*
- 5. EU - European Union and EGBA – European Gaming and Betting Association*
- 7. FATF - Financial Action Task Force*
- 8. FIs - Financial Institutions*
- 9. FIUs - Financial Intelligence Units*
- 10. KYC - Know-your-customer*
- 11. ML - Money Laundering*
- 12. SG- safer gambling*
- 13. STRs - Suspicious Transaction Reports*
- 14. TF - Terrorist Financing*
- 15. Player and customer are used interchangeably.*

1. GENERAL PROVISIONS

- 1.1. At Dynamik Marketing, we are recognizing the importance of Anti-Money Laundering (AML) laws and therefore we are dedicated to fighting money laundering and respecting our obligations as described in this Policy.
- 1.2. At Dynamik Marketing we are fully aware that online gambling is subject to AML regulations due to the opportunity to launder money by funneling criminal proceeds through a gambling platform, thereby obscuring their illicit origin.
- 1.3. At Dynamik Marketing we believe that the application of a risk-based approach to combating ML/TF is an essential element of an effective AML/CTF compliance structure. In conclusion, the controls to manage and mitigate ML/TF risks should be aimed at the:
 - Prevention (e.g., CDD measures).
 - Internal control systems (e.g., employee training and screening).
 - Detection (e.g., monitoring of suspicious activity).
 - Reporting.
 - Record-keeping to facilitate investigations

2. THE RISK-BASED APPROACH

- 2.1. As stated above, the application of a risk-based approach to combating ML/TF is an essential element of an effective AML/CTF compliance structure. Dynamik Marketing assessed the core risk factors at minimum, such as the categories of customers onboarded (particularly high-risk customers), the products and services offered, transactions, the jurisdictions Dynamik Marketing operate in, the interface and delivery channels used.
- 2.2. Dynamik Marketing assessed the risk on inherent and residual level, analyzing threats and vulnerabilities for each risk and considering the probability and impact of each risk materializing, consider the probability for the risk to materialize, as well as its impact, if the risk does materialize.
- 2.3. Dynamik Marketing understands that **probability of inherent risk** 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, and how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others. Consideration should be

given to factors such as the below when determining the probability of an identified risk:

- Dynamik Marketings' exposure to a particular risk through business intelligence reports (data of a company).
- If the market is more prone to a particular risk over others, considering ML/TF tendencies in that jurisdiction.
- Reports issued by relevant authorities on severity and frequency of risks materializing.

2.4. **The inherent risk impact** describes the expected impact on 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:

- Risk ratings provided by the relevant authorities in national risk assessments, the Supranational Risk Assessment and sector specific guidance.
- Facilitation of criminal conduct.
- Risk of regulatory fines and legal prosecution.
- Reputational damage to the Company.

2.5. After defining the inherent risk level and analyzing threats and vulnerabilities, Dynamik Marketing defined adequate control measures to be applied to each identified risk to bring the risk to an acceptable level. That acceptable risk level is the "residual risk" i.e., risk level after the application of the controls. A residual risk level should also be 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. Residual risk scores should be monitored and reassessed where there is a change in the original risk scoring.

3. BUSINESS RISK ASSESSMENT

3.1. Dynamik Marketing developed a Business Risk Assessment ('BRA'). The BRA is an essential document for building AML/CTF controls, since contains a list of the most important risks to which an organization is exposed, mitigating measures – controls, and a risk assessment.

3.2. Dynamik Marketing understand that BRA is not intended to be a static assessment but will be re-assessed on, at least, an annual basis, or

earlier, depending on how the circumstances develop (e.g., how the business changes for example through new products or markets offered, new technology, changes in relevant regulations, etc.), and how the threats evolve.

4. CUSTOMER RISK ASSESSMENT

- 4.1. Dynamik Marketing assessed, via the Customer Risk Assessment (CRA), the risks coming from a customer relationship, and therefore allows us to adequately address such risks via the application of different measures. The level of risk can most commonly be deemed to be low, medium, or high.
- 4.2. The key risk factors, which Dynamik Marketing addressed on the CRA can be grouped into:
 - a) **Customer risk:** determining the potential ML/TF risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. This depends on the type of customer. Categories of customers whose activities may indicate a higher risk include PEPs, high risk occupations, high spenders, disproportionate spenders, etc.
 - b) **Interface and delivery channels:** this risk relates to the different channels through which Dynamik Marketing establishes a business relationship with a customer. Considering Dynamik Marketing conducts only online business that does not take place face to face, such as online gaming, poses a higher ML/TF risk (e.g., risks of identity theft and other fraudulent acts relating to impersonation). However, Dynamik Marketing, due to the technological mitigating measures and controls put in place, can mitigate the risk to an acceptable level. Dynamik Marketing ensures that the internal procedures and processed documents are properly designed for that.
 - c) **Product risk:** Dynamik Marketing acknowledges that certain gaming products may be deemed more attractive for criminals to launder funds due to their specific nature. This may be due to the actual or perceived ease to disguise illicit funds. Games with hedging can be used to secure a return on wagers placed, whilst disguising the activity as normal gameplay for entertainment purposes. Where the outcome can be influenced by the customer, Dynamik Marketing will monitor for signs of individual misuse or collusion. Also, transfer of funds between the

accounts of different players within Dynamik Marketing (being considered the same *operator*) presents a risk factor, which must be considered due to its peer-to-peer nature. Dynamik Marketing categorized the products offered in accordance with the 'gaming type' (e.g., fixed odds games with or without hedging, sports betting, and peer-to-peer games) and assessed the vulnerabilities associated with the product.

- d) **Dynamik Marketing assessed the payment method/transaction risk:** this relates to the degree of anonymity and traceability that different payment methods offer. Some payment methods are more vulnerable to criminal exploitation because they provide customers with the possibility to mask their identity and their source of funding, such as pre-paid vouchers for depositing on the player account. 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. On the other hand, where a customer transfers funds from a bank account or a card linked to a bank account held in their name with an institution established in a reputable jurisdiction, the ML/TF risk is low. This is the case since credit, or financial institutions are themselves subject persons and as part of their CDD obligations they monitor customer accounts and card activity on an ongoing basis. Dynamik Marketing will not accept any payments that are not in the name player/client name.
- e) **Geographical risk:** Some countries pose an inherently higher ML/TF risk than others, as should be established via the jurisdictional risk assessment. Dynamik Marketing risk-rated all relevant countries against reliable and internationally credible sources (e.g., the Basel Index, Transparency International Index, FATF monitored jurisdictions and Global Sanctions listings). Countries with a high-level of corruption, lax or inexistant AML/CFT frameworks, low level of transparency/accountability or which are subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction, are risk rated as high, whilst countries with better risk metrics are rated as medium or low. Dynamik Marketing assesses any connections which customers might have with higher risk countries (for example, linked to their citizenship, country of business, country of residence, etc.).

Once the level of risk is determined, risk- specific process documents are in force for staff when dealing with the customer and adequate CDD measures are in place. **Policies, controls, and process documents are put in place accordingly and must have in-built flexibility to address the specific risk posed by the customer.**

- 4.3. Dynamik Marketing reviews the CRA from time to time depending on the risk level and where there are circumstances, which materially affect the initial assessment, and which may, therefore, warrant changes in the customer risk rating.

5.CUSTOMER DUE DILLIGENCE PROCESS (CDD)

5.1. Dynamik Marketing understands that 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 Dynamik Marketing has a clear understanding of who the customer is and their behavioral pattern.

5.2. DYNAMIK MARKETING APPLY CDD:

AT REGISTRATION

Verifying identity (also paragraph 6 applies)

- Customers are required to enter their date of birth, full address and nationality at Registration an acceptable proof of address (no older than 3 months) and a proof of identity (valid) and CREDITSAFE search solution will screen automatically against *Sanctions, Politically Exposed Persons (PEPs), and Adverse Media*. *If CREDITSAFE system works automatically (as it does for example for customers from Germany, Austria, Switzerland) no interaction with Compliance Team will be required.*
- ***If, CREDITSAFE system does not work automatically*** Customers are required to upload at Registration an acceptable proof of address¹ (no older than 3 months) and a proof of identity (valid) *and a member of the Compliance Team* will review the proof of identity of the customer and check if their full name, date of birth and

¹ Non-exhaustive examples of acceptable proof of identity:
National ID, passport, driving license etc.

address match the personal details that the customer provided at registration. Also, manually a member of the Compliance team will perform manually Creditsafe screening against Sanctions, Politically Exposed Persons (PEPs), and Adverse Media. If, Proof of address and Proof of ID are valid and compliant and Creditsafe results are <75 or >75 but false positives after checks, a member of the Compliance team will active the client manually and email the Customer. Internal Processes regarding Compliance Quality check/double check applies.

- *Dynamik Marketing will not start business relationships with any Sanctioned and PEP Customers.*
- **The COMPLIANCE TEAM will check if the customer is over 18 years old, since onboarding underaged is illegal.**
- The expiration date of the document will also be checked. If the document doesn't mention the expiration date, the compliance officer will use open sources to verify the document.

Verifying address

- The Compliance Team will check if the registered address matches the address stated on the document.
- The proof of address must not be older than three months prior to the date of request (bank statement/utility bill) and in case of a tax bill, this must be issued for the current tax year².
 - ✚ When Dynamik Marketing has knowledge or suspicion that the funds being used are proceeds of criminal activity, irrespective of any threshold.
 - ✚ At appropriate times and on a risk-sensitive basis, including at times when Dynamik Marketing becomes aware that the relevant circumstances have changed.
 - ✚ When doubts arise about the veracity or adequacy of previously obtained customer identification information.

² List of non-exhaustive documents accepted as proof of address:

- bank statement issued within the last three months.
- utility bill issued within the last three months (e.g. gas, electricity, water)
- tax bill for the current tax year.

5.3. The main aim of CDD is to make sure that Dynamik Marketing has effective mechanisms in place to:

- Identify a customer.
- Verify customer identity.
- Keep customer information up to date.
 - Establish the purpose and intended nature of the business relationship along with the customer's business and risk profile.
 - Monitor customer activity on an on-going basis to reduce fraudulent and ML/TF activity during the life cycle of a customer.

5.4. Dynamik Marketing will conduct CDD at REGISTRATION.

5.5. If customers do not cooperate during the CDD process Dynamik Marketing will not start the business relationship and close the pending account.

5.6. Dynamik Marketing during the relationship will follow the customer activity, and on a risk-basis establish the customer's business profile (gathering information about source of wealth and source of funds if 30 000 EUR or equivalent currency threshold applies) so Dynamik Marketing can properly assess a customer's activity if the case applies.

5.7. Dynamik Marketing will screen automatically and/or manually for PEPs, Sanctions and Adverse Media using Creditsafe's People Search solution and not start a business relationship with Customers that are deemed to pose a risk to the integrity of its operations or any events on which bets are accepted. Customers will be screened using *First Name, Last Name, Address, Country, Date of Birth* and only hits 75% or above will be reviewed. The list of databases that Creditsafe screens against is available at <https://help.creditsafeuk.com/en/support/solutions/articles/7000028477-how-to-run-a-compliance-check>.

6. CDD PROCESS: IDENTIFICATION

6.1. The identity of customers is verified using reliable, unexpired, independent source documents, databases (ie. Creditsafe), or information, for example by requesting a copy of a government issued identity document such as a PANCARD, ID card, passport, residence permit, driver's license or through electronic means such as e-ID, bank ID, etc.

6.2. The timing and extent of verification can vary depending on the risk level of the customer. This is done according to local requirements for standards of verification. Verifying personal data provided is done in a robust way, with a trained specialized compliance team (Compliance Team) to ensure reliability.

6.3. As expressed above via the Customer Risk Assessment (CRA) Know Your Customer Risk Rating can be summarized as:

- a) Low Risk** – Standard Due Diligence – Customers who fall into this category pose a low potential risk to Dynamik Marketing and standard or basic Due Diligence will be applied (*proof of id, proof of address, AML screening*)
- b) Medium Risk** – Customers in this category are considered to have a moderate level of risk and therefore, Dynamik Marketing will apply CDD before establishing a business relationship and after any suspicious transactions.
- c) High Risk** – Enhanced Due Diligence (EDD) – These customers have a potential risk, and therefore, Dynamik Marketing will use EDD and a risk-based approach before starting /accepting such a customer. The thorough analysis involves a final approval of Senior Management.

6.4. As expressed above some of the **Risk Rating Factors** that are used to determine the customer's potential risk level are the following:

- Transaction patterns: Dynamik Marketing analyzes the customer's transaction patterns to identify any unusual or suspicious activity, such as a high volume of transactions, large transactions, or frequent transfers.
- Geographic location: Dynamik Marketing evaluates the customer's geographic location to determine whether it is a high-risk area for money laundering or terrorist financing activities.
- Source of funds: Dynamik Marketing evaluates the source of the customer's funds to determine whether they are from legitimate sources. Suspicious sources of funds may include cash deposits or wire transfers from high-risk countries.
- PEPs, Sanctions and Adverse Media: Dynamik Marketing checks on Creditsafe system whether the customer is a PEP, Sanctioned Individual or an Adverse Media subject. PEP refers to individuals who hold prominent public positions. PEPs are considered to pose a higher risk of money laundering and terrorist financing. In any case, Dynamik Marketing will not start a business relationship with Customers that are deemed to pose a risk to the integrity of its operations or any events on which bets are accepted.

7. CDD PROCESS: ENHANCED DUE DILIGENCE

7.1. Where the risk associated with a business relationship are increased, Dynamik Marketing apply enhanced customer due diligence measures (EDD) to manage and mitigate those high risks appropriately (e.g., where transactions are complex, unusually large, and conducted in an unusual pattern).

7.2. In line with the risk-based approach, EDD are extra CDD measures undertaken by Dynamik Marketing to address any heightened customer risk factors, for example: customer, geography, product/service/interface risks. EDD is conducted by The Compliance Team asking customers to provide identity documentation or general information that may be necessary to achieve certain objectives during the customer relationship, such as:

- To additionally verify and validate the customer identity.
- To update more regularly the information held on customer.
- To obtain additional information evidencing customer's location, occupation, source of wealth / funds.
- To obtain additional information on the intended nature of the business relationship.
- To obtain approval from senior management to commence or continue the business relationship.
- To increase the number and timing of controls applied.

8. CDD PROCESS: MONITORING & UPDATE CUSTOMER DUE DILIGENCE

8.1. After The initial satisfactory identification of a new customer, Dynamik Marketing to mitigate ML/TF risks will monitor the customers as the below:

- a) To use reasonable endeavors to ensure documents, data or information held are kept up to date, relevant, and questioning the veracity of the data held whenever any inconsistencies are identified.
- b) To scrutinize the transactions undertaken during the relationship to ensure that they are consistent with Dynamik Marketing's understanding of the customer risk profile.

8.2. Through monitoring of customer transactions and activity, Dynamik Marketing is in a better position to:

- Identify behaviors/transactions, which diverge from the usual pattern, or do not fit with the customer's profile, or are otherwise not in line with what is normally expected from the customer.
- Identify suspicious activity in relation to which a suspicious transaction report ('STR') or suspicious activity report ('SAR') needs to be filed with the MRLO and in the GoAML system (https://portal.fiucuracao.cw/goAMLWeb_PRD/Home)
- Determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within Dynamik Marketing's risk appetite.

8.3. Any unusual activity that departs from habitual patterns of players will be investigated further. *Examples* of this may be unusually large volumes of transactions (if inconsistent with player activity or information that Dynamik Marketing have on the player) or unusually large amounts being deposited (this can also indicate possible concerns relating to problem gambling). Measures, such as obtaining sufficient information and documentation on the matter can be taken when unusual activity is observed. This may also include establishing the customer's source of funds.

8.4. At Dynamik Marketing we understand that CDD is a crucial process for mitigating ML/TF risks. Therefore, the cooperation of customers, as well as their behavior, are also an important factor that should be considered in the risk assessment process. When CDD cannot be completed, the attempts to obtain CDD should be duly documented as well as the reasons for the inability to complete the processes, such as for example, lack of answer by the customer to information requests.

8.5. Each team from Dynamik Marketing understands that non-cooperation during CDD could potentially be an indication of ML and therefore, in each such case the Dynamik Marketing's staff and particularly the Compliance Team should assess if red flags are present. If an indication is found to exist for filing an STR / SAR submission, the case should be escalated to the Senior Management to start an investigation (and to finally conclude if MLRO should be notified).

9. SUSPICIOUS TRANSACTION REPORTING (STR) | SUSPICIOUS ACTIVITY REPORTS (SAR)

9.1. Dynamik Marketing developed an internal channel and process document for reporting the STR/SAR to the Company MLRO: ``Internal Reporting Workflow``.

9.2. MLRO (*Lorenza Godett*) will report, as per AML laws and regulations, the SARs to FIU Curacao through goAML portal, which is an integrated and modular system. The goAML solution works as following: collection, collation, analysis (rule-based, risk score and profiling), case workflow and intelligence dissemination. The data sent goes to a common database and becomes accessible to the FIU analysis staff. The goAML system then permits data for analysis (https://portal.fiucuracao.cw/goAMLWeb_PRD/Home)

9.3. Dynamik Marketing encourages employees to report any suspicions of ML/TF, even when they are not sure, this reporting should be distinguished from reporting any other irregularities that might be in contradiction with local AML/CTF laws. Furthermore, Dynamik Marketing has implemented an internal **Whistleblowing** process for reporting any non-compliant behaviors, actions, and acts within the Company. Within Whistleblowing policy staff are encouraged to report any contravention of applicable AML law internally through a specific, independent, and anonymous channel, proportionate to

the nature and size of Dynamik Marketing. The whistleblowing policy ensures the basic principles and protects individuals from any retaliation, particularly from adverse or discriminatory employment actions, and to provide such whistle-blowers with appropriate protection, particularly regarding their right to protection of personal data and their rights to effective judicial protection and representation.

9.4. Dynamik Marketing is ensuring the confidentiality of the reporting person and confidentiality of the STR/SARs, as well guidance to employees on how to act to avoid tipping-off the player. When submitting STRs/SARs it is crucial that Dynamik Marketing Teams (The Compliance Team, Customer Service Team, Settlement, Financial Department etc. follow procedures issued by Dynamik Marketing.

9.5. Trading department within Dynamik Marketing is monitoring the Customers behavior and send 3 (three) times per week to Managing Director, Compliance Team and Business Manager fund passing investigation records.

10. SPORTS INTEGRITY STANDARDS

10.1. At Dynamik Marketing, we are committed to safeguarding responsible gambling (*as per Dynamik Marketing Responsible Gambling Policy*) and fighting match-fixing.

10.2. Dynamik Marketing is dedicated to safeguarding sports integrity and fighting against match fixing. Match-fixing in many countries is criminalized or sanctioned under other local legal instruments and presents a dishonest and fraudulent practice, which also defrauds gambling operators from funds and must be prevented. Therefore, indications of match-fixing should not be automatically taken as an indication of ML/TF. Dynamik Marketing, however, can find this information of relevance for the Compliance team and therefore Dynamik Marketing is ensuring an adequate process to allow for the internal sharing of such information that might be of importance for other teams.

10.3. Dynamik Marketing Staff are encouraged to report any suspicion of match-fixing internally through a specific, independent, and anonymous channel, proportionate to the nature (the *Whistleblowing Policy*).

11. RECORD-KEEPING REQUIREMENTS

11.1 Dynamik Marketing will maintain, for the duration prescribed in applicable local law, all transaction records necessary to reconstruct individual transactions so that these can be produced as evidence in response to investigations carried out by relevant authorities. These records shall, at least, include:

- Details of how compliance has been monitored by Dynamik Marketing.

- Information or other material concerning possible ML/TF not acted upon by Dynamik Marketing, with reasoning why no further action was taken.
- Customer identification and verification information, supporting records in respect of business relationships and all other relevant data of customer profile.
- Employee training records.
- Internal reports and external STRs. /SARs
- Contact between Dynamik Marketing and the relevant authorities

12. TRAINING

12.1. Dynamik Marketing assures that all relevant employees and staff (the ones working on relevant positions such as transactions execution, AML/Fraud, etc.), undergo AML training in accordance with their position and responsibilities. Generally, relevant employees should be aware that money laundering risks exist and what internal procedures need to be adhered to in the context of fulfilling AML obligations for their specific role and level.

12.2. Specifically, all relevant employees/staff should receive training on:

- The vulnerabilities of the gaming sector to ML/TF.
- The identification of unusual transactions.
- Red flags to consider when detecting and reporting suspicious activities.

12.3. Training is targeted, well planned, and proportionate.

12.4. Training is performed once / year by the Senior Compliance Officers in the training period (Q3 each year), or when Policy changed (or in the first 3 days after starting / new position for new hires). Evaluation questionnaires and attendance forms are kept according to point 12 above.

13. MONITORING AND IMPLEMENTATION OF THE INTERNATIONAL GUIDELINES

13.1. Dynamik Marketing is always keeping an eye on the AML/CFT International Standards, EU AML Standards, FATF etc. and on the local legislation that applies. This policy and other supportive documents are reviewed every 12 months, considering business needs or when changes are made to regulations or applicable laws whichever is the earliest, to ensure that it remains appropriate considering any relevant changes to the law, organizational policies, or contractual obligations.

