

ABC Interactive NV

Next Way Ltd

Anti-Money Laundering Policy

Table of Contents

Table of Contents	1
Management Overview	4
Company Statement	4
The Compliance Officer	4
Management	5
Staying up to date	5
Staff Training	6
Monitoring	7
Approach	7
Record Keeping	8
Business Risk Assessment	10
Company AML/CFT Risk Matrix	10
1. 10	
A) Inherent Risk (IR) – what the risk exposure is before controls:	10
B) Control Effectiveness (CE) – strength of controls: how well the controls reduce Inherent Risk (IR)	10
C) Residual Risk (RR)	11
2. 12	
1) Customer / Player Base (Weight 25%)	13
2) Products / Games (Weight 10%)	15
3) Payments / Transactions (Weight 15%)	16
4) Interface / Delivery (Weight 15%)	16
5) Geography / Markets (Weight 20%)	17
6) Employee / Insider (Weight 10%)	17
7) Unusual Activity Monitoring (Weight 5%)	18
Overall Company Residual Risk	18
Customer Acceptance Policy	20
Introduction	20
New Customer Account Registration Acceptance	20

New Customer Account Registration Restrictions	20
Customer Risk Assessment, CDD and Risk Levels	22
Customers with which a business relationship is terminated or declined:	24
Deposit and Withdrawal Management Procedures	27
Player Account Balance	27
Payment Methods	27
Player Deposits	27
Player Withdrawals	28
Withdrawal Payouts	28
Customer Risk Assessment	29
1. Customer Risk (Who) 30%	29
2. Jurisdiction Risk (Where) 20%	30
3. Payment Method Risk (What) 20%	30
4. Game Risk (What) 15%	30
5. Interface/Delivery Channel Risk (How) 5%	31
6. Supporting Behavioral Analysis 10%	31
CRA Calculation	32
Final Risk Band Mapping	33
On-Going Monitoring	34
Identification and Verification (KYC) Policy	35
1. Purpose & Scope	35
2. Regulatory Basis	35
3. Definitions	35
4. Player Identification	35
5. Player Verification	36
5.1 Documents Standards	36
Acceptable Documents	36
Non-Documentary Verification Methods:	36
5.2 Verification Timing & Triggers	37
5.3 Verification Outcomes & Actions	37

6. Record-Keeping & Audit Trail:	38
Enhanced Due Diligence	39
Meaning of Source of Funds	39
Meaning of Source of Wealth	39
PEP and Sanctions Screening	40
Politically Exposed Persons (PEPs)	40
PEP Classification Duration & De-classification	42
Reporting of unusual transactions	43
Red Flags	43
Reporting unusual transactions to compliance officer	44
Submitting a report of unusual transaction/s to the Authorities	45
Prohibition of Disclosure (Tipping off)	45
Internal Fraud Management	47
Internal Controls	47
Authorisation controls	47
Segregation of duties	47
Checks on performance	48
Employment Screening	48
Whistle Blowing Procedures	48
Education	48
Fraud Investigation	
Player Fund Segregation Policy	48
Restricted Jurisdictions Policy	51
Version History	53

Management Overview

Company Statement

ABC Interactive will conduct business in accordance with all applicable laws, rules and regulations which apply to our operations (NORUT - National Ordinance on the Reporting of Unusual Transactions; NOIS - National Ordinance on Identification of Clients when rendering Services; Kingdom Sanctions Act - The National Ordinance also known as the "Rijkssanctiewet"; Sanctions National Ordinance; AML/CFT/CFP Regulations for online gaming-regulations for Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation of weapons of mass destruction for the online gaming sector of Curacao issued by Gaming Control Board).

The Company AML policies are designated to prevent our company from being used or abused by individuals for the laundering of their criminally acquired funds or for any other unlawful or illegal activity, and to mitigate all possible risks relating to money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes.

ABC Interactive applies a risk-based approach which allows us for our resources to be invested and applied where they are most required. Where the risks are higher enhanced measures must be taken.

The risk-based approach involves the followings stages

- Identifying the relevant AML/ CFT risks such as customer risk; geographical risk; product, service and transaction risk; interface risk
- Designing and implementing policies, procedures and controls to manage and mitigate the risks
- Ongoing monitoring and improvement
- Keeping records of all actions taken with reason

The Compliance Officer

The company has appointed a Compliance Officer responsible for the detections and deterrence of money laundering and terrorist financing including designing and implementing the AML program, reviewing all internal reports of unusual transactions, preparing external reports of unusual transactions, external reporting of the unusual transactions to the FIU as per article 11 of the NORUT.

To ensure that the AML/ CFT compliance officer is able to fulfill their role effectively, the management will make sure:

- The compliance officer is able to act independently
- The compliance officer must be independent from the games operations.
- The compliance officer has timely access to customer identification data, customer due diligence information, transaction records, and any other relevant information.
- The MLRO has no conflicting responsibility which may pose a conflict of interest.
- The MLRO has sufficient time, resources and information to fulfill their responsibilities.

Management

The Compliance Officer will have overall responsibility for ongoing regulatory compliance, as well as anti-money laundering procedures.

The Compliance Manager will be responsible for the following:

- AML Program:
 - Design and implement the AML program
- Compliance:
 - To verify compliance with local AML/ CFT laws and regulations
 - Review compliance with company's policies and procedures
- Verification and KYC
 - Sourcing third party verification systems and services.
 - Implementing and managing KYC verification processes
 - Defining CDD / EDD processes
- Back Office
 - Managing and monitoring the Back Office processes for KYC, fraud, and money laundering, etc.
- Money Laundering reporting
 - Point for escalation of unusual transaction reporting, and responsible for reporting these to the relevant bodies
 - Keep records of internally and externally reported unusual transactions.

Staying up to date

The company is aware that the requirements and guidance, as well as external fraud trends can and will change, and that its policies and procedures and procedures must be kept up to date.

Therefore the measures will be implemented to ensure the company is kept up to date:

- Key personnel will subscribe to various relevant mailing lists offered and will join relevant forums.

In the case of an update, the following steps will be taken, as necessary:

- Update company policy documentation and training material.
- Inform all relevant staff by email regarding the updates, meet with relevant team managers, and ensure they update their teams appropriately.
- Update email communication templates and chat canned responses.
- Update website policies, maintaining a version number and 'last update' date.
- Update the Terms and Conditions as needed.

Staff Training

Training will be given to all staff, whether employed by the company directly or in-directly through a service provider.

Relevant training material will be prepared for all teams based on the company policies.

Training will be conducted as follows:

- Training material based on the finalised and approved policies will be prepared, in the form of documents and presentations.
- Training will be provided to existing management and staff in a class setting.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should we find that some issues are not clear we will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in policy will be communicated in a group email and through ad-hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- Existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements;
- Their personal obligations under the money laundering and terrorist financing requirements;
-
- The company's identification, verification, record-keeping and other procedures to prevent money laundering and the financing of terrorism;
- The recognition and handling of unusual transactions;
- Their personal liability for failure to report information or suspicions in accordance with the money laundering and terrorist financing requirements and the licence holder's internal procedures; and

- New developments, including information on current techniques, methods and trends in money laundering and the financing of terrorism.

Monitoring

- Training will be followed by tests to ensure the material was understood.
- Supervisors in both the Support and Back Office teams will monitor all activities within their teams.
- Randomly selected support chats and emails will be reviewed for quality assurance.
- Where an issue is seen, we will (a) review other chats and emails by the staff member and (b) review other chats and emails on the same issue. This will be done to determine if this is a once off issue, an issue with the particular employee or a general misunderstanding of the topic.
- Player complaints will be reviewed in order to identify any shortfalls.

Where it is found that an employee has not abided by the policies set by the company:

- The employee will be given an official warning in writing.
- The employee will be required to re-do any appropriate training and tests.
- The employee will be put under a probationary period, which will include closer monitoring of their activity.
- If the employee continues to breach the company policies, they will be terminated in line with local HR regulations.

Note that the Compliance Officer will be actively involved in the training process:

- Review all training material, and ensure all relevant aspects of the requirements are covered.
- Ensure that any updates in the requirements are incorporated into the training material, and all relevant staff are updated with the new requirement.
- Ensure that training is conducted with all new and existing employees, according to this training plan.

Approach

- The AML/ CFT Compliance Officer together with other senior management will be fully engaged in defining and managing the processes needed to prevent money laundering and other fraudulent activity.
- We will use a threshold approach to due diligence about when to verify a player electronically.
- The AML program is risk-based, and designed to mitigate the money laundering and terrorist financing risks the company may encounter, and
- We will monitor all transactions and activity.

- We will pay back to source wherever possible, and when not feasible, we will have controls in place to manage the risk of money laundering.
- We will continuously monitor these risks and processes.
- We will ensure that all relevant employees are trained on AML and CTF policies and procedures, and emphasise the importance of being alert to these risks.

Record Keeping

As part of our record keeping procedures, we will collect and retain, for at least five years after the business relationship is ended with the customer:

- Necessary records on transactions sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for prosecution of criminal activity
- All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents)
- All correspondence with the customers

We will also retain all records of reports and enquiries related to AML/CFT activity. These records will include:

- Date;
- Nature of the enquiry;
- Name of the authority;
- Name of the enquirer;
- Powers being exercised;
- Participants about whom the enquiry was made;
- Transactions that were involved.

Such record keeping will always follow any applicable Data Protection and Privacy guidelines, and can be amended accordingly in line with applicable laws and regulations.

The following information and documentation will be kept which may be required to be provided to GCB (Gaming Control Board) upon their request:

- Written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation
- Records of BRA
- Names of the AML/ CFT compliance officer and job description
- Records of unusual transactions which required closer investigation.
- Records of blocked accounts

- Schedule of the training regarding money laundering, terrorist financing and proliferation of weapons
- The assessment reports by the internal audit department or an external auditor
- Customer records, including CDD, customer risk assessment, transactions information.

Business Risk Assessment

The company has prepared a Business Risk Assessment (BRA), and continues to review and update the BRA as necessary.

Company AML/CFT Risk Matrix

This section provides an overview of our enterprise-wide AML/CFT risk profile based on the factors, weightings, and scores in the Company AML/CFT Risk Matrix. It explains the method and presents the calculated Residual Risk (RR) per pillar and overall RR for the company.

1. Scoring & bands (company-level)

A) Inherent Risk (IR) – what the risk exposure is before controls:

- 1 = Low – Limited exposure; low value/velocity; traceable flows.
- 2 = Low–Moderate – Mostly low risk with a few riskier pockets.
- 3 = Moderate – Mixed exposure (some higher-risk elements present).
- 4 = Moderate–High – Several higher-risk drivers material and recurring.
- 5 = High – Systemic exposure (cash-like instruments, high-risk geographies, strong ML typologies).

B) Control Effectiveness (CE) – strength of controls: how well the controls reduce Inherent Risk (IR)

- Residual risk is computed as: $RR = \text{round}(IR \times (1 - CE/6), 1)$; (keeps a non-zero floor even for strong controls).

CE	Reduction factor (1 - CE/6)	Description
----	--------------------------------	-------------

1	0.833	Weak / ad-hoc. Controls exist on paper or sporadically; gaps in design/coverage; little or no evidence they run.
---	-------	--

2	0.667	Basic / developing. Controls designed and operating in core areas but inconsistent; limited assurance. suitable for controls that are present but not yet consistently performed or evidenced.
3	0.500	Moderate / partially effective. Controls run routinely with minor misses; coverage mostly complete; partial but usable evidence.
4	0.333	Strong. Well-embedded and automated where sensible; full coverage; regular t testing; timely fixes.
5	0.167	Very strong / embedded & evidenced. Mature, automated, tested; continuous monitoring; swift corrective action; minimal residual risk but never zero. acknowledges efficient control maturity while still leaving non-zero residual risk

C) Residual Risk (RR)

- Residual Risk (RR) is the risk that remains after controls are applied. It reflects both the underlying exposure (Inherent Risk, IR) and the strength of our controls (Control Effectiveness, CE).
- Formula: $RR = \text{round}(IR \times (1 - CE/6) / 1)$

What each term means

- IR (Inherent Risk): Exposure before controls (1–5 scale).
- CE (Control Effectiveness): How strong the controls are (1–5).
- $(1 - CE/6)$: The reduction factor. CE is divided by 6 on purpose so even CE=5 doesn't drive risk to zero. It recognises that some residual risk always remains.

Worked examples

- If IR=4, then:
 - CE=2 → $RR = \text{round}(4 \times (1 - 2/6) / 1) = \text{round}(4 \times 0.667, 1) = 2.7$
 - CE=3 → $RR = \text{round}(4 \times 0.5 / 1) = 2.0$
 - CE=4 → $RR = \text{round}(4 \times 0.333 / 1) = 1.3$
 - CE=5 → $RR = \text{round}(4 \times 0.167 / 1) = 0.7$

Residual Risk Bands:

Band	Meaning	Required actions
Low (1.0–1.9)	Residual risk is controlled and within appetite. Controls are effective; only minor optimisation opportunities.	Maintain current controls; continue routine; implement minor improvements; review on normal cadence.

Medium (2.0–3.4)	Material residual risk; tolerable with mitigation but outside target state. Some gaps in coverage/evidence or control execution.	Increase management review frequency; enhance QA/spot tests. Add automation: reduce manual steps that cause misses (scheduled data pulls, automated alerts, etc)
High (3.5–5.0)	Elevated/unsustainable vs appetite; control design/operation or evidence is insufficient for the exposure.	Consider temporary risk-reducing measures (limits/restrictions); escalate to MLRO; schedule frequent reviews

2. Risk Pillars

Our Business-Wide AML/CFT Risk Matrix groups risk into seven pillars, each weighted to reflect its relative impact on our gaming business model. These weights drive the overall Residual Risk (RR) calculation and help management prioritise controls, assurance, and remediation.

- **Customer / Player Base — 25%.**
The largest driver. Covers who our players are and how they behave: KYC quality/recency, High value depositors/VIP exposure, multi-accounting risk, PEP/sanctions exposure, and consistency of activity with stated profile and Source of Funds. A higher weight is warranted because even robust products and payments can be misused if customer risk is not well controlled.
- **Geography / Markets — 20%**
Jurisdictional exposure (FATF listings, sanctioned/restricted countries), and discrepancies between residence, access IP, and payment origin. Geography materially affects both ML/TF typologies and sanctions risk; hence the second-highest weight.
- **Payments / Transactions — 15%**
Funding and withdrawal rails (bank/cards, e-wallets, vouchers), pay-back-to-source discipline, settlement flows, and anomaly patterns (rapid deposit–withdrawal loops). Payment channels are a core conduit for ML/TF and therefore carry significant weight.
- **Products / Games — 10%**

Intrinsic risk of offered games (e.g., slots/scratch = lower; table games = moderate). Product design and features can enable or limit misuse; weight reflects that product risk is meaningful but generally mediated by Customer/Payments controls.

- **Interface / Delivery — 15%**

Remote onboarding and play (non-face-to-face), VPN/proxy/device risks. Because gaming is fully remote, the integrity of the digital interface is a key control area and merits equal weight to Payments.

- **Employee — 10%**

Staff access, potential collusion, segregation of duties, and training/awareness. While less frequent, insider weaknesses can amplify other risks; a steady, non-trivial weight keeps assurance focused here.

- **Unusual Activity Monitoring — 5%**

The detection layer across all pillars: rules/alerts, information provided to MLRO, escalation and STR decisions. It is a cross-cutting safeguard with a modest standalone weight because its effectiveness is already reflected within other pillars' residuals.

How the pillars work together

- **Aggregation:** Each pillar's Residual Risk (RR) is calculated from its Inherent Risk (IR) and Control Effectiveness (CE). The overall company RR is the weighted sum of the seven pillar RRs using the weights above.
- **Risk appetite & governance:** We apply Low/Medium/High bands to each pillar and to the overall score to set escalation paths, decide on targeted improvement plans, determine review frequency

1) Customer / Player Base (Weight 25%)

Sub-factor	What could go wrong	Key controls (from BRA)	IR	CE	RR
Unverified / impersonated accounts	False data or third party opening → unknown counterparty.	KYC at thresholds or red flags; block if KYC is not completed within 30 days; no withdrawals pre-identity verification.	4	3	2
High-value depositing customers	Rapid HVD patterns masking proceeds of crime.	MLRO monitors HVD; open source check + EDD when necessary.	4	3	2

Sub-factor	What could go wrong	Key controls (from BRA)	IR	CE	RR
PEP exposure	Corruption/bribery proceeds funding play.	PEP screening at threshold	3	4	1.0
Sanctions exposure	Prohibited persons attempt to transact.	Sanctions screening	3	4	1.0
Dormant accounts withdrawals	Time-distancing after minimal/no play.	Verification reviews all payouts; escalate unusual/large requests to MLRO.	3	3	1.5
Source of funds/wealth for HVC	Spend not aligned to income/wealth.	MLRO review; SoF/SoW evidence on risk basis.	4	3	2.0
Multiple payment methods	Attempting to structure deposits to avoid detection.	Ongoing Monitoring; withdrawals back to source.	3	3	1.5
Corporate/3rd-party cards	Unauthorised use; laundering via business cards.	T&Cs prohibit; monitoring; 3D secure on transactions; block/return to source.	4	3	2.0
Multi-accounting (same operator)	multiple accounts using different names, making it difficult to verify the real account holder and/or the source of the funds.	Device recognition; manual review of new accounts	4	3	2.0
Multi-operator dispersion	Activity split across operators reduces signals.may result in customer activity levels with single operators falling below internal reporting thresholds in accordance with the risk-based approach	The company does monitor its customers across all sites it operates, however is unable to track a customer's activities on other operators' sites.	3	2	2.0

Sub-factor	What could go wrong	Key controls (from BRA)	IR	CE	RR
VIP upgrades	Upgrading a customer onto loyalty/reward schemes without having undergone proper due diligence may potentially increase the risk	VIP works with MLRO/Verifications; ongoing monitoring; RG emphasis.	3	4	1.0

2) Products / Games (Weight 10%)

Sub-factor	Risk	Controls	IR	CE	RR
Slots & scratchcards	Lower manipulation risk but bonus abuse can raise risk.	Bonus abuse monitoring by Risk team.	2	4	0.7
Blackjack/baccarat/roulette	Hedging/covering outcomes → layering.	Analyst review of low-risk betting; MLRO escalation/STRs.	3	4	1.0
Withdraw without play / minimal play	Deposit/withdraw loops to cleanse funds.	T&Cs admin fees; verification review; STRs when warranted.	4	4	1.3
P2P/poker	Collusion/soft-play (higher risk) — not offered .	Not applicable; control = product not available.	1	5	0.2

3) Payments / Transactions (Weight 15%)

Sub-factor	Risk	Controls	IR	CE	RR
Bank transfers / cards	Traceable; pay-back-to-source. Low .	Pay-back-to-source; ownership verification + anti-fraud monitoring..	2	4	0.7
EEA e-wallets (Skrill/Neteller/ecopayz)	Medium; some anonymity/mobility.	Ongoing monitoring; return to source where possible.	3	3	1.5
Prepaid cards / vouchers/ Crypto	High : cash-like, non-refundable.	EDD; winnings paid only to the account in the player's name after checks or return to source where possible	5	3	2.5

4) Interface / Delivery (Weight 15%)

Sub-factor	Risk	Controls	IR	CE	RR
Non-face-to-face onboarding	Identity theft/forgery at scale.	selfie/video; if verification fails block; if suspicious activity STRs raised to FIU	4	3	2.0
Disguised location (VPN/shared IP)	Group/device fraud; jurisdiction evasion.	VPN detection & blocks at registration/login; IP/device review.	4	3	2.0

Non-face-to-face transactions (layering)	Moving funds via third parties/banks.	Verifications & MLRO monitor; investigate; STRs.	4	3	2.0
Affiliates (traffic origination)	Affiliate fraud/abuse risk.	Monitoring for abuse	3	3	1.5

5) Geography / Markets (Weight 20%)

Sub-factor	Risk	Controls	IR	CE	RR
Activity outside registered country	location mismatch; High Risk country logins.	Block FATF-blacklisted; monitor High Risk countries activity.	4	3	2.0
Residence vs card/bank mismatch	Cross-border disguise of origin/destination.	Verify country matches; request info; STR if warranted.	4	3	2.0
High-risk jurisdictions	Strategic AML/CFT deficiencies.	Block FATF blacklisted; High Risk countries customers auto high risk + EDD	4	3	2.0

6) Employee / Insider (Weight 10%)

Sub-factor	Risk	Controls	IR	CE	RR
Collusion / manipulation	Influence outcomes or records.	No ability to affect bet outcomes; restricted access; two-person review for payouts.	3	4	1.0

Staff knowledge & escalation	Missed red flags	Training at hire and regular cadence; direct access to MLRO/management; monitoring activities of staff.	3	4	1.0
------------------------------	------------------	---	---	---	-----

7) Unusual Activity Monitoring (Weight 5%)

Sub-factor	Risk	Controls	IR	CE	RR
Missed unusual patterns	Failure to detect/escalate across areas.	automated reports reviewed by AML team; red flags escalation and cross-team communications (support/verification).	3	4	1.0

Overall Company Residual Risk

Pillar	Weight	Avg RR (calc.)	Reporting band
Customer / Player Base	25%	1.64	Low
Products / Games	10%	0.80	Low
Payments / Transactions	15%	1.57	Low
Interface / Delivery	15%	1.88	Low
Geography / Markets	20%	2.00	Medium
Employee / Insider	10%	1.00	Low

Unusual Activity Monitoring	5%	1.00	Low
-----------------------------	----	------	-----

Overall Company Residual Risk (weighted): 1.56 — Low.

Our weighted Overall Residual Risk (RR) is 1.56 (Low) and remains within risk appetite. Most controls are rated CE=3 (Moderate), which reduces inherent risk by about half but leaves a modest margin to the Medium band. Several pillars are positioned near the upper end of Low.

Customer Acceptance Policy

Introduction

The Customer Acceptance Policy defines the criteria by which the company may or not accept potential customers, the level of customer due diligence measures to be applied according to the customer's risk.

New Customer Account Registration Acceptance

- To deposit and play on a company's site, a customer must first register on the site.
- To register an account with us, a customer must be identified. The customer provides the following personal information and contact details at account registration:
 - Username
 - Email address
 - Password
 - First Name and Last Name
 - Date of Birth
 - Gender
 - Language
 - Address and country of Residence
 - Mobile number
- Registration is limited to individuals who are over eighteen years of age and reside in jurisdictions allowed by the company.
- Customers may have only one account per site.

New Customer Account Registration Restrictions

- Individuals under 18 years of age are not permitted to register on the site.
- Individuals from countries where we are unable to accept players due to local gambling regulations.
- Individuals from FATF blacklisted countries are not permitted to register on the site. These countries are not included in the available countries on registration, and login from related IPs will be blocked.
- Existing customers who have an existing exclusion on the site.

Customer Risk Assessment, CDD and Risk Levels

The customer acceptance is based on the risk level assigned to the customer.

All the customers are categorized in three categories: low, medium and high risk.

At onboarding stage, the risk associated with a customer will be based on the personal information provided by customers during account registration, for example the players from high-risk jurisdictions may be considered as high-risk customers. At this stage, a provisional risk rating will be assigned based on the initially collected information. While a single factor may increase the risk associated with a particular player, this does not mean that the player is automatically classified as high risk as other contributing factors and information are also taken into consideration. As such, each factor is measured against the player's profile holistically. For example, a customer from a high-risk jurisdiction without any financial activity will not be deemed high risk unless the account activity changes.

At account opening, all customers are being screened against sanctions lists, and for PEP status.

Upon registration, all new accounts are monitored for red flags to identify unusual or suspicious activity that may be indicative of high risk of ML/FT:

- Inconsistencies in the data and information previously obtained from customer
- Doubts about veracity customer identification information, data or documentation
- Using bank accounts, bank cards or e-Wallets held or issued in the name of third parties
- Using IPs or payment methods that are from high-risk jurisdictions, or do not match the details on the account.
- Using VPNs, remote servers, etc., that may disguise or hide their actual location.
- Changing deposit methods and withdrawing to different methods
- Higher than expected deposit volume
- A dormant account suddenly becomes active
- Adverse media found on the customer
- Customer does not cooperate in the carrying out of CDD
- Links to other accounts.
- Deposits with minimal bets followed by withdrawal request
- Unreasonable reluctance to provide information or documents requested for verification purposes, etc.

In line with Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation of weapons of mass destruction (AML/CFT/CFP Regulations) for the online gaming sector of Curacao, when a customer engages in financial transactions equal to or above four thousand

NAF (NAf 4,000) since the account opening, the CDD measures has to be conducted and customer risk assessment must being carried out within 30 days the Naf 4,000 threshold was reached, assigning a player low, medium or high-risk level, together with the screening of the customer for PEP status.

The Customer Due diligence measures are to be applied when:

- The player engages in financial transactions equal or above Naf 4,000
- There is suspicion of money laundering
- We have doubts as to the veracity of the information/ documentation collected from the player

The level of CDD measures is applied according to the risk level assigned to the player.

The customer risk assessment is based on the following risk pillars:

- Payment methods
- Game play
- Jurisdiction
- Customer Risk
- Interface Risk

Upon a player reaching the deposit threshold, the account is immediately scored and assigned to a risk level. Scoring then re-runs on key events (e.g, new adverse media/PEP hits).

Pillar Weights

Pillar	Weight (%)
Customer Profile	30%
Jurisdiction	20%
Payment Method	20%
Game / Product	15%
Interface / Delivery Channel	5%
Behavioural / Monitoring	10%

Risk Categories and Actions

CRA Score	Category	Actions
0–40	Low	Standard KYC; routine monitoring.
41–70	Medium	Targeted KYC (e.g., SoF summary, recent statements); closer monitoring; review payment methods.
71–100	High	EDD (SoF/SoW request); enhanced ongoing monitoring; withdrawal/limits subject to senior review; investigate and consider STR as applicable.

The customer due diligence measures will be applied according to the customer risk level:

Customer Due Diligence Type:

- **Simplified CDD:** customers identification by collecting personal and contact details. Applied to customers which did not reach the Naf. 4,000 threshold and whose activity were not flagged as suspicious or unusual, or customers which have not requested a withdrawal.
- **Standard CDD:** verification of personal details using documentation: ID document and proof of address; we may collect additional personal information, we may obtain source of income/ funds, occupation information. Applied to all customers who reached the Naf. 4,000 threshold or have requested a withdrawal request.
- **Enhanced CDD:** verification of personal details using documentation: ID document and proof of address; collection of additional personal information; obtaining source of income/ funds, occupation information and documentation; taking additional measures to mitigate the risk. Applied to players who reached Naf. 4,000 thresholds assigned with high risk level such as PEPs, or players whose activity was flagged out as suspicious or unusual

Customers with which a business relationship is terminated or declined:

- Customers for which we are unable to complete the CDD within 30 days the Naf. 4,000 threshold has been reached
- Customers confirmed to be on a sanctions list

- Customers with negative adverse media relating to financial crime in large amounts, and serious crime
- Customers which we know, suspect or have reasonable grounds to suspect of ML/FT
- High risk customers where cannot be applied effective risk mitigating measures and falls outside company risk appetite
- Customers whose activity was flagged as suspicious or unusual, and which were unresponsive to our request for additional information, clarification, documentation within reasonable timeframe, or did not provide sufficient or reasonable explanation
- Customers with sufficient reasons to indicate that they may have problem gaming problem
- Customers which were in breach of our Terms and Conditions
- Customers suspected of fraud including chargebacks
- Customers sharing similar behavior suspected of abuse with significant evidence to indicate that the customers are unnaturally connected (matching deposit methods, game choice, bet amount choice, same Internet provider, account formatting)
- Customers which transactions were reported as fraudulent by the issuer
- Customers which provided false or misleading information without a reasonable explanation
- The customers which are either Politically Exposed Persons (“PEPs”), their family members or close business associates and we were unable to complete the EDD measures, and /or did not receive management approval

Customers which may be considered higher risk:

- Politically Exposed Persons (“PEPs”), their family members or close business associates
- Customers from high-risk jurisdictions, or linked to a high-risk jurisdiction by place of birth or nationality, source of funds/ wealth
- Customers with unusually large deposits, and unusual patterns of transactions
- Customers with adverse media relating to their suspected involvement in illegal activities and crimes, or customers known to be under investigation
- Customers with irregular source of income or multiple source of income

Risk Factors

When assessing the ML&TF risks relating to types of customers, jurisdictions, and services used by the customer, transactions and interface risks, various risk factors within the risk categories are being considered. The risk factors, either separately or in combination, may increase or decrease the potential risk posed by a customer or a business relationship, thus affecting the appropriate level of CDD measures

Below are risk factors that should be considered as indicative of potentially lower risk, medium risk and higher risk:

Low Risk:

Type	
Customer Risk	• Customers who are employed or with a regular source of income from a known source which supports their activity with us (this includes benefit recipients) • Customers with a long-term and active business relationship with us
Payment method	• Bank transfers, Debit, credit cards issued by banks
Game Play	• Slots, scratchcards
Country	• EU countries • Third countries with effective systems for preventing and combating money laundering and terrorist financing.

Medium Risk

Type	
Customer Risk	• Self-employed individuals (small business owners such as builders; shop owners) • Customers which are not specifically identified as potentially low risk or high risk.
Payment method	• EEA licensed e-wallets (Skrill, Neteller, ecopayz) • Non-EEA licensed e-wallets and methods that allow cash funding
Game Play	• Blackjack, baccarat, roulette
Country	• Non - FATF "grey list": Jurisdictions under Increased Monitoring

High Risk

Type	
Customer Risk	• Politically Exposed Persons ("PEPs"), their family members or close business associates • Customers from high-risk jurisdictions

Payment method	• Prepaid cards and vouchers
Game Play	• We do not offer high risk games (P2P)
Country	• FATF "grey list": Jurisdictions under Increased Monitoring

Deposit and Withdrawal Management Procedures

Player Account Balance

Each player has a gaming account from which bets are deducted and winnings added.

All funds deposited by the player are credited to the player's corresponding gaming account with balance updating accordingly

The player can top up the funds in his account by depositing through the deposit section on our online casino platform deposit section on our site, and then use these funds to place bets.

Bets are deducted from his account balance, and winnings are added to the account balance.

Withdrawals of available funds in the player's balance can be withdrawn by the player.

We do not offer credit to players.

Funds may not be transferred from one player to another.

Payment Methods

Payments shall only be accepted and made from accounts held with licensed financial institutions or through licensed payment providers notified to the Authority, and which the Authority has not instructed the licensee to refrain from using.

No cash deposits/withdrawals will be effected between the company and its players.

Player Deposits

After registering, a player may then deposit funds into their account through the deposit section on our online casino platform.

The company offers a variety of popular deposit options including credit and debit cards, FSA-approved e-wallets (such as Neteller and Skrill), online bank transfers and vouchers.

Players can deposit in a number of currencies, and if a player chooses to deposit in a currency different to the currency of his account, he will be shown the amount that he will receive prior to depositing.

In order to facilitate these deposits, the company has integrated with a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself.

The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the player's balance.

The client is then able to bet on the site with his/her available balance.

Player Withdrawals

A player with an available balance will be able to request a withdrawal of the funds via the withdrawal section on the site.

The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

The Verifications Team reviews the request which includes:

- verification of KYC documentation,
- manual check for duplicate accounts,
- requesting additional KYC documentation if needed, and
- review for breaches of terms and conditions.

Once the payout request is approved by us, the payout request will then be processed and submitted to the PSP.

Withdrawal Payouts

In remitting funds to the player, we will, where possible, remit the funds directly into the account where the funds originated from.

Provided that where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

Customer Risk Assessment

The Customer Risk Assessment (CRA) is developed in accordance with regulatory requirements.

Customer risk assessment is carried out to detect any unusual activity during the business relationship.

Once a player engages in financial transactions equal to or more than Naf. 4,000, we do a Customer Risk Assessment, assigning a player as low, medium or high risk. The Naf. 4,000 threshold is to be calculated daily taking into account all deposits and withdrawals made by the player since the establishment of the business relationship.

The CRA is based on core risk categories:

- Customer Risk
- Geographical Risk
- Product, Service and Transaction Risk
- Delivery Channel (Interface) risk

The CRA framework uses a weighted risk-scoring methodology, combining quantitative scoring where each risk factor is given a numerical score and weight, while also allowing for qualitative review to capture risks that may not be fully reflected by numbers alone.

The model is dynamic:

- Step 1: Weighted Base Risk Score (each risk pillar is scored on a 0–100 scale and weighted by importance).
- Step 2: Risk Adjustments (fixed-point additions for red flags).
- Step 3: Tiered Overrides (automatic High Risk for mandatory high-risk situations).

1. Customer Risk (Who) 30%

This pillar assesses the inherent risks linked to the customer's identity and profile.

Factors:

- KYC Verification
- Declared occupation and income; Source of Wealth (SoW) information
- Source of wealth (SoW) supporting documentation
- PEP and Sanctions screening
- Adverse Media

- “*Activity vs Expected*”: alignment of activity with the Anticipated Behaviour Profile - ABP (or Declared Income Band)
- Strong unexplained deviations from expected customer activity (unusual deposit spikes)

Important: Significant anomalies trigger Automatic High-Risk Override

2. Jurisdiction Risk (Where) 20%

This pillar assesses the risks arising from the customer’s country of residence, nationality, and place of birth. It considers exposure to FATF grey- blacklisted jurisdictions and other high-risk countries.

Factors:

- Customer country of residence
- Nationality; Place of birth
- FATF status (grey list / blacklist) and EU “high-risk third countries”

3. Payment Method Risk (What) 20%

Payment method risk considers the type of payment methods used (bank transfers, cards, e-wallets, vouchers), whether the account or card belongs to the customer, and the level of traceability.

Factors:

- Payment method type (Bank transfers, cards, e-wallets, prepaid vouchers) - volume and frequency by method:
 - Bank transfers, cards - Low Risk
 - E-wallet (Skrill, Neteller, ecopayz, etc) - Medium Risk
 - Prepaid cards/vouchers such as Paysafecard (anonymous & hard-to-trace method due to limited audit trail) - High Risk
- Account ownership:
 - Manual checks that the payment account name matches the customer’s name
 - Third-party usage is flagged as high risk

4. Game Risk (What) 15%

Game/product risk considers the types of games played, betting amounts, and potential abuse or misuse of products for layering funds.

Key Factors:

- Game Type - bet frequency and amounts:
 - Fixed odds games without hedging (e.g., slots) - low medium
 - Fixed odds games where hedging is possible (blackjack, baccarat, roulette; crash games) - medium risk
- Wins and Bets Ratio

5. Interface/Delivery Channel Risk (How) 5%

It measures risks associated with non-face-to-face onboarding and remote transactions. While interface risk tends to be more uniform across customers than other pillars (customer, geography, and payment method/ game risks usually fluctuate more between individuals), it remains relevant.

Factors:

- Device intelligence at registration:
 - Device fingerprinting (ThreatMetrix) and risk rating
 - Detection of proxy or VPN use - (ThreatMetrix) blocks account automatically at registration
- The use of VPNs or proxies to conceal a customer's true location/device, as well as duplicate or multi-accounting across the same brand, which may be used to bypass controls

6. Supporting Behavioral Analysis 10%

This layer assesses dynamic risks that emerge from customer behavior over time.

Factors:

- Withdrawal history and patterns:
- Abnormal withdrawal patterns
- Etc.

CRA Scoring Methodology

The Customer Risk Assessment (CRA) combines a weighted base score, dynamic adjustments, and tiered overrides to ensure risk ratings are consistent, and aligned with regulatory expectations.

CRA Score Range per Risk Category:

- 0 – 40 Low Risk
- 41 – 70 Medium Risk
- 71 – 100 High Risk

Pillar Weights and Rationale

Pillar	Weight (%)	Rationale
Customer Profile	30%	Customer background, occupation/income, SoW documentation, alignment of activity with the Anticipated Behaviour Profile - ABP and PEP/adverse media status are the most significant determinants of inherent ML/TF risk.
Jurisdiction	20%	Residence, nationality, and country of birth strongly influence risk, especially where linked to FATF grey/blacklist jurisdictions.
Payment Method	20%	Certain payment types (e.g., prepaid) carry higher risk due to limited traceability and ownership checks.
Game / Product	15%	Some game types, especially those allowing hedging add risk
Interface / Delivery Channel	5%	Generally uniform across customers (all customers use the same platform and channel), but risks remain from VPN/proxy use (hiding true location/device).To mitigate these risks, the company uses ThreatMetrix (TMX), a third-party system integrated into the registration process
Behavioural / Monitoring	10%	Captures dynamic risk from transactional behaviours

CRA Calculation

- Each pillar contains specific risk factors, which are individually scored on a 0–100 scale.
- Within each pillar, factors may carry sub-weights that contribute to the pillar's overall risk score.
- To ensure the final CRA score reflects both the level of risk and the importance of that risk, the calculation is performed in two stages:

1. Pillar Score Calculation => Pillar Score = $\sum$ (Factor Score × Factor sub-weight)

2. Weighted Pillar Contribution => Total Pillar Contribution = Pillar Score × Pillar Weight

3. Total CRA Risk Score. The overall CRA score is the sum of all weighted pillar contributions:

- Total Risk Score = $\sum (Pillar\ Score \times Weight)$
- Scoring model. CRA Total Score = (Who × 0.30) + (Where × 0.20) + (Payments × 0.20) + (Product/Game × 0.15) + (How × 0.05) + (Behaviour × 0.10) + Dynamic Adjustments + Tiered Overrides

Final Risk Band Mapping

CRA Score Range	Risk Category	Action Required	Rationale
0 – 40	Low Risk	Standard CDD	Low Risk = minimal risk → standard controls: Customer profile, jurisdiction, product, payment method, and behavioural indicators suggest minimal exposure to ML/TF risk. Standard due diligence is sufficient.
41 – 70	Medium Risk	Enhanced monitoring	Medium Risk = moderate factors → monitoring + info validation: One or more moderate risk factors are present (e.g., unusual payment patterns, game/product risk profile). This category requires closer ongoing monitoring and, where appropriate, the collection of additional information or documentation to validate the customer's activity.
71 – 100	High Risk	EDD, Source of Wealth (SoW) documentation, MLRO oversight & approval	High Risk = → EDD Significant inherent or residual risk is present (e.g. PEP status, adverse media, high-risk jurisdiction, or strong deviations from expected activity). Requires Enhanced Due Diligence, documented Source of Wealth/Funds, senior-level approval, and closer monitoring.

On-Going Monitoring

The Company conducts ongoing due diligence on every customer relationship and scrutinises transactions to ensure they are consistent with our knowledge of the customer and their risk profile. Monitoring is risk-sensitive: higher-risk customers receive more frequent and deeper reviews; all customers receive baseline oversight.

This includes:

- Obtain fresh identification when existing documents have expired. (on a risk-sensitive basis)
- Question the data and information we have whenever inconsistencies are noticed.
- And in general review and update from time to time, on a risk sensitive basis.
- Scrutinizing the customer's transactions by comparing the actual level of the player's account activity against the profile of an average player or the information provided by the customer through a declaration or documentation
 - If unusual transactions were identified, collect information and if necessary supporting documentation and source of funds, and the MLRO shall determine whether to report an STR to the FIU

Identification and Verification (KYC) Policy

1. Purpose & Scope

This policy sets out the mandatory requirements for identifying and verifying players.

2. Regulatory Basis

This Policy implements the obligations on identification and verification of players, including:

- Collection of personal data sufficient to establish identity (identification); and
- Confirmation of those details using reliable, independent sources such as documents (verification), applying a risk-based approach (RBA).

Primary regulatory source (Curaçao):

- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction — Applicable to Curaçao casinos and providers of other online games, issued by the Gaming Control Board / Curaçao Gaming Authority (GCB/CGA).

3. Definitions

- Identification: Collection of personal details to establish a player's identity.
- Verification: Confirmation of the collected details via reliable, independent documents/ data.
- Reliable independent source: Government-issued records; regulated financial institutions; trusted utility providers; qualified digital identity providers
- Document standard : Minimum quality and authenticity criteria a document must meet to be accepted.

4. Player Identification

At account opening the following personal information is collected to identify the player:

- Full name and surname
- Residential address
- Date of birth

Additional data may be collected for High risk situations: place of birth, nationality, identity number

5. Player Verification

5.1 Documents Standards

Acceptable Documents

Purpose	Primary examples	Alternative examples	Validity / Recency
Photo ID	Passport; National ID card	Driving Licence (photo); Residence permit	Unexpired; photo clear; full page/front&back
Proof of Address (PoA)	Utility bill; Bank/credit statement;	Tenancy/lease agreement; Insurance letter; Government benefits letter; Tax letter	Issued ≤ 6 months
Proof of ownership of payment account used on our site	Bank statement or online banking page showing account holder name, , and recent transaction(s) with our merchant	Card copy (front & back) with PAN masked (first 6/last 4 only), name and expiry visible; e-wallet account page (e.g., Skrill/Neteller) showing registered name/email and/or recent transaction(s); Payment provider/bank confirmation letter	Issued ≤ 6 months (or covers the most recent deposit). CVV fully covered; signature strip visible; no third-party accounts

- **Quality Criteria:** unobstructed, full edges visible, no glare/blur, readable MRZ/ID number, consistent metadata (names, dates, address). Foreign documents require extra care and, where necessary, translation.
- **Rejection Reasons (non-exhaustive):** Cropped/blurred; expired; altered; mismatch with account data; third-party documents; screenshots of mobile banking without issuer; unverifiable providers; suspected forgery

Non-Documentary Verification Methods:

- Geolocation/IP/device fingerprint: Consistency checks vs. declared country/address.

- Registry/database checks: Electoral roll, credit reference data, company registries, telephone directories.
- Contact: Phone call or secure message to corroborate facts.
- Video: Where enabled, biometric face-match with liveness to confirm that the person presenting the ID is the same individual and physically present.
- Any other reliable methods that reasonably confirm the identity of the player

5.2 Verification Timing & Triggers

- Onboarding: Identification initiated at registration (collect personal details: name and surname, permanent residential address and date of birth);
- Complete identity verification before first withdrawal or upon risk trigger—whichever occurs first.
- Threshold trigger: Complete verification when engaging in financial transactions (deposits and/or withdrawals) equal to or in excess of NAF 4,000. All CDD measures must be completed no later than 30 calendar days from the moment the threshold is reached.
- Event-driven triggers / red flags (pre-threshold): If any ML/TF red flags arise before the threshold (e.g., unusual device/geo, third-party payment indicators, inconsistencies in identity data, tampered documentation; PEP/sanctions match; geo anomalies; fraud indicators, etc), apply CDD and, where appropriate EDD regardless of value.

5.3 Verification Outcomes & Actions

Outcome	Description	Account status / next steps
Verified	Documents/data meet documents acceptance standards; match to account; checks passed	Full access; standard monitoring
Partially Verified	Verified identity but other documents are incomplete or missing (e.g., PoA expired; payment ownership pending)	Access allowed; pending withdrawals; obtain missing items
Not Accepted	Failed consistency checks (expired/forged/altered; data mismatch); suspected forgery	May suspend or restrict; consider EDD/ SAR as

appropriate; request additional information/ clarification

Unresponsive	No response or uploads after KYC request(s) within defined timeframe	Re-initiate; set final deadline; suspend or maintain restrictions per risk; consider account closure if persistent
---------------------	--	--

Escalation: Any High-risk case or repeated failures is escalated to the CDD & AML Team and the MLRO for review.

6. Record-Keeping & Audit Trail:

- Store copies of KYC documents in the player’s folder
- Retain for 5 years (or longer if required by law/regulator). Apply access controls.
- Maintain records of CDD on player’s account: what was checked, by whom, exceptions and approval

Enhanced Due Diligence

The Enhanced Due Diligence has to be conducted where the risk of ML/TF are higher

EDD may include:

- Obtaining additional information on the customer such as occupation
- Obtaining information on the source of funds or source of wealth of the player
- Obtaining information on the reason of a performed transaction
- Obtaining management approval to commence or continue the business relationship
- Conduct enhanced ongoing monitoring

As part of EDD, we may ask for documentation showing Source of Funds and/or Source of Wealth.

- Source of Funds declaration, together with supporting documents
- Bank statements
- Salary slips
- Other documentation as relevant.

These documents are reviewed to ensure that we are able to trace the source of the funds used on our site.

Meaning of Source of Funds

Our understanding of Source of Funds is that this refers to the origin of the particular funds being used to deposit on our site.

Meaning of Source of Wealth

Our understanding of Source of Wealth is this refers to the origin of the entire body of wealth (i.e. total assets) of the client:

The information that should be obtained should give an indication as to the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

PEP and Sanctions Screening

Screening for PEP status and sanctions screening must be carried out before establishing the business relationship, once the Naf. 4,000 threshold is reached, and on a regular basis.

Politically Exposed Persons (PEPs)

- Foreign PEPS are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
- Domestic PEPS are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
- Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Targeted Financial Sanctions:

- Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities
- Before doing business or performing an occasional transaction for the first time with a player, the casino should check published lists of known or suspected terrorists or other sanctioned persons
- We are required to freeze without delay and without prior notice, the funds or other assets of designated persons in line with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curacao on the basis of the Kingdom Sanctions Act.
- If Curacao publishes a local list with designated persons and organizations, the casino should also take that local list into account. The casino must ensure it does not do business with customers that are subject to international sanction

Watchlists Covered:

- United Nations Security Council Consolidated Sanctions List;
- European Union Consolidated Financial Sanctions list;
- United States (OFAC U.S. Treasury) - OFAC Consolidated Sanctions list; OFAC Specially Designated Nationals (SDN) list;
- UK Sanctions List (FCDO) and OFSI Consolidated List of Asset Freeze Targets;
- INTERPOL Wanted List;
- World Bank List of Debarred Firms and Individuals
- International Monetary Fund- Offshore Financial Centers;
- Iraq- ISIL (Da'esh) & Al-Qaida Sanctions List;
- Sanctions – Canada; Sanctions - Ireland; Sanctions - New Zealand;
- Europe's Most Wanted Fugitives; Wanted- Royal Canadian Mounted Police

True Matches and False Positives

- Any match between a player's details and a record on sanctions or PEPs lists, is not necessarily an indication that this is the actual sanctioned individual or the PEP.
- Additional review of the account is necessary to eliminate the false positive.
 - The AML & CDD team will try to confirm if the player is actually a PEP or a sanctioned individual. Where there is a false positive, the label and block will be removed from the player's account.
- Where there is a match on the lists, and open-source checks do not rule out the player being sanctioned or PEP:
 - PEP match:
 - We initiate the EDD which must be completed within the thirty-day window
 - Obtain senior management approval to service the PEP
 - Establish their source of wealth and, where applicable, their source of funds
 - Conduct enhanced on-going monitoring of the customer's activity.
 - Sanctions match:
 - A report must be filed with the FIU, and the casino has to take the 'Process for the freezing of resources' into account so the sanctioned individual cannot remove money from an account
- It's important that the player's details are up-to-date and complete. Incomplete or inaccurate data will result in a lot of false positives.

PEP Classification Duration & De-classification

- Initial classification: from the time a PEP role is identified (including family members/close associates).
- After leaving office: the individual remains classified as a PEP for a minimum of 12 months.
- De-classification: permitted only after a documented risk assessment concludes the risk of influence/misuse of former position has sufficiently diminished (consider recency of role, seniority, ongoing influence, jurisdictional corruption risk, adverse media, and transaction behaviour).
- Family members/close associates: follow the same minimum 12-month rule and risk-based extension where warranted.
- All de-classification decisions require compliance officer approval and a recorded justification.

Reporting of unusual transactions

We are required to monitor for suspicious and unusual activity and transactions, and report any suspicious or unusual activity and transactions.

Unusual Transactions

The following transactions or intended transactions are deemed unusual as per NORUT (Decree Indicators Unusual Transactions) legislations:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice
- Transactions by sanctions individual, adopted by virtue of the Sanctions National Ordinance
- Transactions in the amount of NAf. 5,000 or more
- Transactions or activity where there is suspicion of money laundering (ML), funding of terrorism (FT) or that the funds being used on our site are the proceeds of criminal activity.

Red Flags

The following are examples of red flags which may be indicative of ML/FT (but are not definite proof of ML/FT).

Red flags are not intended to automatically result in filing a STR but are merely indicators that should lead us to question the player's behaviour. If there is no reasonable explanation for the red flags then an internal report must be made to the MLRO.

The following is a list of possible red flags which should be considered:

- Player does not cooperate in the carrying out of CDD.
- Player attempts to register more than one account on a site.
- Player deposits considerable amounts during a single session by means of multiple prepaid cards.
- Player deposits funds well in excess of what is required to sustain usual betting patterns.
- Player makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Player makes frequent deposits and withdrawal requests without any reasonable explanation.

- Noticeable changes in the gaming patterns of a player, such as when the player carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Player enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Player carries out transactions which seem to be disproportionate when seen in the context of what is known about the Player's wealth, income or financial situation.
- Player seeks to transfer funds to the account of another Player or to a bank account held in the name of a third party.
- Player requests a withdrawal to an account he never deposited with.
- Player displays suspicious behaviour in playing games that are considered as high risk
- Complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose

Reporting unusual transactions to compliance officer

All employees have a duty to report suspicious and unusual transactions without delay. If an employee has any suspicion about a Player or transaction, it must be reported to the compliance officer immediately.

All employees are expected to report suspicious and unusual transactions to the compliance officer.

Note: The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the MLRO to determine if the information available can be considered as sufficient for a STR to be made to the Authorities

Internal reports of unusual and suspicious transactions must be submitted to the compliance officer via email.

The following information should be included:

- Account details
- Detailed reason for suspicion

The compliance officer will:

- acknowledge receipt of the report and review and investigate further as required.
- make an assessment based upon all the information and decide whether the matter needs to be reported to FIU.
- If it does, they will submit a Report to the FIU without delay in line with article 11 of the NORUT.
- If internally reported transaction is not reported to the FIU by the casino, the reason shall be adequately documented and signed off by the compliance officer and/or management

- The compliance officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.
- The report with the details of the unusual transaction/s must be submitted to the FIU by means of the goAML reporting portal.

Submitting a report of unusual transaction/s to the Authorities

Once the compliance officer has received an internal report, the compliance officer will decide if a report should be submitted to the Authorities.

When making this decision, the compliance officer should consider that AML legislation is intended to address and attack serious crime which usually either involves amounts that are not minimal or circumstances which show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

For example identity fraud and chargebacks may give rise to ML but a licensee will only be subject to reporting obligations if they result in funds derived from these activities being deposited with or held by the licensee.

However, we should not report single instances involving small amounts but should consider whether we can detect a bigger pattern or scheme.

The compliance officer should consider whether an internal report gives rise to a suspicion of ML by taking into account all relevant information which would include considering whether there are common denominators between repeated instances of chargebacks or identity fraud. These may include common or related persons, common IP addresses etc.

If the compliance officer decides that a report need not be submitted to FIU, the reasons for this decision must be recorded.

goAML reporting portal after validation by the FIU

Prohibition of Disclosure (Tipping off)

It is important not to knowingly or inadvertently tip off the Player that a report has been submitted.

We are not permitted to disclose information to the customer nor to third parties

This includes informing the player that an report was submitted or taking any action that may tip him/her off.

Any action we take following the submission of a report to FIU must be properly considered to determine whether this may prejudice the analysis being conducted by the Authorities. Therefore we must be careful when closing an account or blocking additional transactions after filing a report or receiving an enquiry from the Authorities, as this may tip off the player. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

Internal Fraud Management

We will actively take steps to prevent both internal and external fraud, and will always endeavour to keep abreast of new fraud methods.

The prevention framework for preventing internal fraud will consist of the following:

- Implementation of control measures and policies in order to prevent fraud;
- Adoption of surveillance and other means for the purposes of detection of fraudulent behaviour;
- Investigation of suspicious conduct or activities;
- Coherent and efficient whistle blowing policies and procedures.

Internal Controls

Management will implement a number of internal controls and general procedures which will be used on a day-to-day basis in respect of managing and running the daily operations of the business. These internal controls will mainly focus on the following principles:

Authorisation controls

Certain actions shall require the approval or authorisation of senior management personnel prior to being able to be carried out by employees. Furthermore, a system of levels of access shall be implemented throughout the Company, whereby access to data and other inside information owned by the Company shall only be granted to selected employees. Such access and the extent to which it is granted shall be determined according to the role and position of the relevant employee. At all times, no employee shall have any access which is in excess of his needs in order to be able to perform the work which is expected of him through his role and position.

Segregation of duties

Duties to be performed by employees shall be allocated in such a manner that no one employee shall have full and sole control over an entire process or an entire area. This prevents fraudulent behaviour from being undertaken by employees as a result of the level of power they are granted over a particular section of the operation. In cases where it would not be beneficial for the Company to have a particular duty or task split between different employees, it shall be ensured that the employee who is given full control over such process or area shall be adequately supervised in proportion with the fraud risk level that such process or area may pose.

Checks on performance

Senior level personnel shall carry out checks on employees on a regular basis; or whenever the need for such checks to be performed is felt by the Company. In particular, such checks shall be carried out when a suspicion arises in relation to the behaviour of specific employees. These checks may be carried out through surprise spot checks, inventory counts or other procedures which will enable such personnel to verify whether employees are complying with the policies and procedures that are in place.

Employment Screening

Prior to engaging employees, we shall carry out relevant integrity checks, in-line with their position, responsibilities and access levels. We will not employ any persons who are not deemed to be fit and proper. Once a person is employed, screening shall still be carried out on an ongoing basis as required. The frequency and extent of screening which shall be carried out shall be proportionate to the risk level posed by the employee.

Whistle Blowing Procedures

We will implement a whistle blowing procedure whereby employees may report suspicious activity, fraudulent or unethical behaviour or irregularities to particular members of senior management. All reports lodged by employees will be treated with strict confidence. Under no circumstances will the identity of the reporting employee be disclosed to any other employee, least of all, to the reported employee/s. Such reports shall be made to the Compliance Officer. Once a report is lodged by an employee, this will be treated seriously by the Company. All reports shall undergo checks and investigations in order to determine their veracity. Any suspicion of fraud or corruption shall be taken very seriously and will be examined and analysed with precision. Where a report is deemed to be frivolous or unwarranted, this shall also be investigated.

The results of any investigation will be written in a report which will be retained by the Company. The report will include an explanation of the findings, providing the reasons for any actions were taken or otherwise.

Education

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

Fraud Investigation

When an investigation has uncovered evidence of fraud or corruption, management will decide whether the matter is serious enough to be reported to the regulators and the relevant law enforcement authorities, and take the necessary action against the employees in question. This may be either written warnings or termination of employment, depending on the severity of the case.

Player Fund Segregation Policy

1. Purpose

This policy outlines the Company's procedures and commitments to ensure that customer funds are fully protected through the segregation of player funds from the Company's operational funds.

The purpose of this policy is to maintain transparency, trust, and financial integrity, in full compliance with applicable laws, regulations, and gaming licence conditions.

It establishes clear principles and controls to safeguard player balances, winnings, and pending withdrawals at all times.

2. Scope

This policy applies to:

- All player funds deposited with the Company, including but not limited to player balances, winnings, and pending withdrawals;
 - All bank accounts, e-money, or PSP wallets used by the Company to receive, hold, or settle player funds;
-

- All employees, departments, and third-party service providers involved in handling financial operations, payments, or reconciliations.
-

3. Key Definitions

- **Player Funds / Liabilities:** The total amount owed to players at any given time, including balances and pending withdrawals.
 - **Customer Funds Account(s):** Bank accounts or wallets designated solely for holding player funds.
 - **Operational Account(s):** Accounts used for Company revenues and expenses, including payroll, suppliers, marketing, and taxes.
 - **Reconciliation:** The process of verifying that the total balance of Customer Funds Accounts matches or exceeds total player liabilities.
-

4. Segregation of Funds

The Company will maintain separate bank accounts to ensure that customer funds are strictly segregated from the Company's operational accounts.

Specifically:

- **Customer Funds Account(s):** All deposits, winnings, and any funds belonging to customers will be held in designated Customer Funds Accounts.
- **Operational Account(s):** All company-related funds (revenues, expenses, salaries, and supplier payments) will be held in separate Operational Accounts.

Under no circumstances will customer funds be used for operational purposes. The balances of Customer Funds Accounts will always be sufficient to meet the Company's total player fund liabilities.

5. Procedures

5.1 Fund Deposits

Upon receipt, all customer deposits are placed directly into the Customer Funds Account. These funds are never used for operational or investment purposes and remain available to fulfil player withdrawal obligations.

5.2 Withdrawals

When a customer requests a withdrawal, the corresponding amount is deducted from the Customer Funds Account and transferred to the customer's payment method within the applicable legal or regulatory timeframe. Withdrawals are processed in accordance with AML and CDD requirements and subject to standard verification procedures.

5.3 Reconciliation

Weekly reconciliation processes are undertaken by the Finance Department to ensure that the balances in the Customer Funds Accounts accurately reflect the aggregate balances of all customer accounts.

Any discrepancy or shortfall is reported immediately to the Finance Director and Compliance Officer and rectified without delay by transferring funds from operational reserves to the Customer Funds Account.

5.4 Access Control

Access to Customer Funds Accounts is restricted to authorized financial personnel only. All movements between Customer and Operational Accounts require dual authorization and are recorded for audit and compliance purposes.

5.5 Audit and Oversight

Periodic internal and external audits are conducted to verify compliance with this policy and to ensure ongoing integrity of fund segregation practices. Reports are reviewed by senior management and retained for inspection.

6. Regulatory Alignment – Curaçao (CGA / LOK)

The Company operates in accordance with the conditions of the Curaçao Gaming Control Board (GCB) and Curaçao Gaming Authority (CGA), including compliance with the **National**

Ordinance on Games of Chance (LOK – PB 2024, no. 157).

The Company will promptly implement any new conditions or requirements relating to the separation, safeguarding, insurance, or payout of player funds, and will maintain evidence of compliance for regulatory and banking reviews.

7. Governance and Record Keeping

The Finance Director and Compliance Officer are jointly responsible for the implementation and monitoring of this policy.

All records relating to player fund segregation - including reconciliation reports, bank statements, and authorization logs - are retained securely for at least five (5) years and made available to regulators or financial partners upon request.

Restricted Jurisdictions Policy

1. Policy Statement

ABC Interactive N.V. (hereinafter “the Company”) restricts access to its online casino platforms, including but not limited to:

- <https://www.imperialwins.com>
- <https://www.slotsventura.com>

This policy ensures compliance with:

- Curaçao Licensing Obligations
 - International Anti-Money Laundering (AML) and Counter-Terrorism Financing Standards
-

- Responsible Gambling Requirements
- The Regulatory and Compliance Frameworks of Our Payment Service Providers (PSPs)

The Company applies a risk-based approach to determine prohibited jurisdictions, subject to ongoing regulatory updates and legal assessments.

2. Restricted Jurisdictions

Access to the Company's services is restricted in countries deemed high-risk or non-permissible under the frameworks described above, including but not limited to the following:

Afghanistan, Abkhazia, Albania, Austria, Australia, Bahamas, Barbados, Barthele, Belgium, Botswana, Bulgaria, Burundi, Cambodia, Cameroon, Cayman Islands, Central African Republic, Chad, Croatia, Cuba, Cyprus, Czech Republic, Democratic Republic of the Congo, Denmark, Djibouti, Eritrea, Estonia, Ethiopia, France, French Guiana, French Polynesia, French Southern Territories, Georgia, Germany, Gibraltar, Greece, Government and non-government controlled Ukrainian territory, Guadeloupe, Guernsey, Haiti, Hungary, Iran, Iraq, Israel, Italy, Jamaica, Jersey, Lebanon, Libya, Lithuania, Mali, Malta, Martinique, Mauritius, Mayotte, Moldova, Mongolia, Mozambique, Myanmar (Burma), Netherlands, New Caledonia, Nicaragua, North Korea (DPRK), Pakistan, Palestine, Palestinian Territories, Panama, Paraguay, Portugal, Reunion, Romania, Russian Federation, Saint Martin, Saint Pierre and Miquelon, Senegal, Sierra Leone, Slovakia, Slovenia, Somalia, South Ossetia, South Sudan, Spain, Sudan, Sweden, Switzerland, Syrian Arab Republic, The Crimea Region (Ukraine), Transdniestria, Turkey, Uganda, United Kingdom, United States, United States Minor Outlying Islands, Venezuela, Virgin Islands (British), Virgin Islands (U.S.), Wallis and Futuna, Yemen, Zimbabwe, and other contested territories not internationally recognised.

3. Enforcement Measures

The Company maintains technical and procedural measures to block access and prevent transactions from the above jurisdictions, in alignment with AML/CTF standards and PSP compliance requirements.

Version History

Version	Date	Record of Changes
1.0	2021/08/01	Initial Version
2.0	2021/11/29	Addition of Screening for PEP/Sanctions; SAR investigation and reporting; MLRO
3.0	2024/11/25	Update of the AML policies and procedures in line with the New AML/CFT/CFP Regulations by Gaming control Board
4.0	2025/09/09	PEP and Sanctions – added watchlists; PEP Classification Duration; Business and Customer Risk Assessment Scoring Update; update identification and verification policy
4.0	2025/10/23	Latest check

Signed by:

Maya Baroud
Director

Signature: _____

