

Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Policy

Disrupt Entertainment Limited N.V.

Effective Date: April 10, 2025

Version: 2.0

1. POLICY STATEMENT

Disrupt Entertainment N.V. ("the Company") is committed to preventing its operations from being used for money laundering (ML), terrorist financing (TF), or proliferation financing (PF) purposes. This policy ensures compliance with:

- National Ordinance on Identification when Rendering Services (NOIS)
- National Ordinance on Reporting Unusual Transactions (NORUT)
- Sanctions National Ordinance
- Kingdom Sanction Act
- GCB Regulations for Combating ML/TF/FP (January 2025)

This policy applies to all directors, management, employees, and third-party contractors.

2. RISK-BASED APPROACH

2.1 Business Risk Assessment (BRA)

The Company conducts an annual Business Risk Assessment to identify and assess ML/TF/FP risks considering:

- **Customer risk factors:** Multiple income sources, irregular income streams, PEPs, high spenders, casual customers

- **Geographical risk factors:** High-risk jurisdictions per FATF/CFATF lists, sanctioned countries, high-corruption countries
- **Product/service risk factors:** Cash transactions, anonymous payment methods, peer-to-peer gaming, cryptocurrency
- **Distribution channel risk factors:** Non-face-to-face interactions, third-party involvement

The BRA is documented, approved by the Board of Directors, and reviewed at least annually or when significant changes occur.

2.2 Customer Risk Assessment (CRA)

For each customer, the Company performs a Customer Risk Assessment to categorize ML/TF/FP risk as:

- **Low Risk**
- **Medium Risk**
- **High Risk**

The CRA determines the appropriate level of Customer Due Diligence (CDD) to be applied.

2.3 Customer Acceptance Policy (CAP)

The Company maintains a Customer Acceptance Policy that defines:

- Customer types presenting higher-than-average ML/TF/FP risk
- Risk indicators for low, medium, and high-risk classifications
- Level of CDD measures required for each risk category

- Circumstances warranting service refusal

3. CUSTOMER DUE DILIGENCE (CDD)

3.1 When CDD is Required

CDD measures are required when:

- Financial transactions equal or exceed NAf. 4,000
- Carrying out occasional transactions above NAf. 4,000
- Suspicion of ML/TF/FP exists
- Doubts about previously obtained customer identification data arise

3.2 CDD Measures

a) Identification and Verification of Customer

At account opening, collect minimum information:

- Full name
- Permanent residential address
- Date of birth
-

When the NAf. 4,000 threshold is reached, additionally collect and verify:

- Place of birth
- Nationality
- Identity number

Verification must use reliable, independent sources (government-issued ID documents, utility bills not older than 6 months, etc.).

b) Beneficial Owner Identification

Customers must declare they are playing on their own behalf. If beneficial owners exist (e.g., syndicates), identify and verify:

- Natural persons holding $\geq 25\%$ shares/voting rights
- Persons exercising ultimate effective control
- If no natural person identified, the senior managing official

c) Purpose and Nature of Business Relationship

Understand the customer's:

- Source of wealth (origin of accumulated money)
- Source of funds (how funds for specific transactions were obtained)
- Expected level of activity

Use statistical data or customer declarations appropriate to risk level.

d) Ongoing Monitoring

- Keep identification data accurate and up-to-date
- Monitor transactions for consistency with customer profile
- Investigate deviations from expected behavior
- Review customer risk assessment when patterns change

3.3 Timing of CDD

- Collect minimum identification at account opening
- Complete full CDD verification within 30 days of reaching NAf. 4,000 threshold

- If threshold reached by deposit: freeze further deposits/withdrawals until CDD complete
- If threshold reached by withdrawal: freeze account entirely until CDD complete
- Terminate relationship if CDD not completed within 30 days

3.4 Simplified Due Diligence (Low Risk)

For low-risk customers:

- Limit identification to name, address, date of birth
- Reduce ongoing monitoring frequency
- Verify identity after establishing business relationship (if permitted by risk assessment)

3.5 Enhanced Due Diligence (High Risk)

For high-risk customers:

- Obtain additional customer information (occupation, previous addresses)
- Obtain additional information on intended nature of relationship
- Request source of funds/wealth documentation
- Obtain senior management approval to establish/continue relationship
- Conduct enhanced ongoing monitoring
- Require first payment through reputable jurisdiction account

3.6 Politically Exposed Persons (PEPs)

For all PEPs (foreign, domestic, international organization):

1. Screen at onboarding and regularly during relationship
2. Obtain senior management approval to establish/continue relationship

3. Take reasonable measures to establish source of wealth and source of funds
4. Conduct enhanced ongoing monitoring

Apply same measures to PEP family members and close associates.

If existing customer becomes PEP, implement measures within 30 days or terminate relationship.

3.7 Sanctions Screening

Screen all customers against:

- UN Sanctions List
- EU Sanctions List
- Local sanctions lists (if published)

Screening conducted:

- At account opening
- Before each withdrawal
- Regularly during business relationship

If match found:

- Freeze account immediately
- Report to FIU
- Follow "Process for Freezing of Resources"

3.8 Termination of Business Relationship

Terminate relationship if:

- Unable to complete CDD within required timeframe
- Customer refuses to provide required information
- Risk becomes unacceptable

Return funds through same channel received unless ML/TF/FP suspicion exists. Report to FIU if suspicion exists.

4. REPORTING UNUSUAL TRANSACTIONS

4.1 Unusual Transactions - Objective Indicators

Report transactions $\geq$ NAf. 5,000 per gaming day:

- Cashless transactions (transfers from casino bank to customer bank)
- Deposits or withdrawal requests
- Sale of chips/tokens/credits to customer
- Cash outs
- Credit card and e-wallet transactions

4.2 Unusual Transactions - Subjective Indicators

Report transactions where:

- Reported to Police/Department of Justice for ML/TF connection
- Customer on sanctions list
- Presumption of ML/TF/FP exists based on:
 - Inconsistency with customer profile
 - Financial transactions significantly greater than normal pattern
 - Gaming transactions inconsistent with normal pattern
 - Payment to blacklisted country bank account
 - Deposits/withdrawals to/from sanctioned person

4.2 Reporting Process

1. **Internal Reporting:** Employees report unusual transactions immediately to Compliance Officer with supporting documents
2. **External Reporting:** Compliance Officer reports to FIU via goAML portal without delay
3. **Documentation:** Maintain records of all reported and non-reported unusual transactions with rationale

4.3 Prohibition of Disclosure

No employee may disclose to customer or third parties:

- That unusual transaction report has been filed
- That FIU has requested information
- Any details related to ML/TF/FP investigation

4.4 Account Blocking

Internal procedures determine when unusual transaction reporting leads to account blocking, considering tipping-off risk.

RECORD KEEPING

Maintain for minimum 5 years:

Customer Records:

- Identification documents (copies of passports, ID cards, utility bills)
- CDD information and risk assessments
- Account files and business correspondence
- Evidence of beneficial ownership

Transaction Records:

- All customer transactions (domestic and international)
- Records sufficient to reconstruct individual transactions
- Source and recipient of payments

Reporting Records:

- Internal unusual transaction reports
- External reports to FIU
- Rationale for non-reporting decisions

Records available to competent authorities upon appropriate legal request.

5. AML/CFT/CFP COMPLIANCE PROGRAM

5.1 Compliance Officer

Appointment: Senior officer at management level, independent from gaming operations

Responsibilities:

- Design and implement AML/CFT/CFP program
- Verify compliance with laws and regulations
- Review adherence to policies and procedures
- Organize staff training
- Analyze and review unusual transactions
- Report unusual transactions to FIU via goAML
- Maintain reporting records
- Update program as needed
- Monitor ML/TF/FP developments
- Prepare periodic reports to senior management/Board

Current Compliance Officer: Adrian Toshkov

5.2 Policies, Procedures and Controls

The Company maintains written, Board-approved:

- AML/CFT/CFP policies
- Customer Acceptance Policy
- CDD procedures
- Transaction monitoring procedures
- Reporting procedures
- Record-keeping procedures
- Risk management measures
- Sanctions screening procedures
-

Policies reviewed annually and updated as needed.

5.3 Employee Screening

All employees undergo criminal background checks before hiring.

5.4 Training Program

New Employees:

- Nature and process of ML/TF/FP
- Internal policies and procedures
- ML methods and trends in gambling sector
- CDD requirements
- Objective and subjective reporting indicators

Role-Specific Training:

- **Dealers/Cashiers:** Front-line ML detection, transaction monitoring

- **Supervisors/Managers:** Comprehensive ML/TF/FP oversight
- **Compliance Staff:** Specialized AML/CFT/CFP training
- **Senior Management/Board:** Reputational risk awareness

Ongoing Training:

- Refresher training at regular intervals
- Updates on new ML/TF/FP trends and techniques
- Regulatory changes

Training Records Maintained:

- Training content
- Attendee names and dates
- Test results
- Ongoing training plan

5.5 Independent Audit

Annual independent audit of AML/CFT/CFP program by:

- Internal audit department (if adequately resourced and independent), OR
- External qualified auditor

Auditor Qualifications:

- Minimum 2 years AML/CFT compliance experience
- Relevant degree
- Recognized AML certification (CAMS, CAMS-Audit, or AMLFC)

Audit Scope:

- AML/CFT/CFP manual adequacy

- Compliance management effectiveness
- Transaction testing
- Training adequacy
- Legal/regulatory compliance
- Record retention adequacy
- System ability to identify unusual activity
- Employee interviews
- Unusual transaction sampling

Audit Documentation:

- Scope of testing
- Testing results
- Identified deficiencies
- Corrective action recommendations
- Management responses
- Implementation deadlines

Deficiencies reported to senior management and Board with corrective action requirements.

6. PHYSICAL ESTABLISHMENTS (if applicable)

If the Company uses physical establishments to extend customer reach:

- Ensure physical establishment applies Company's AML/CFT/CFP policies
- Verify operator is of good standing
- Identify and verify operator
- Monitor operator's account activity
- Regularly verify policy implementation
- Document all compliance measures

7. BRANCHES AND SUBSIDIARIES

Foreign branches and subsidiaries must implement AML/CFT/CFP measures consistent with Curaçao requirements.

8. GOVERNANCE

8.1 Board Approval

This policy is approved by the Board of Directors and reviewed annually.

8.2 Policy Updates

Policy updated when:

- Regulatory changes occur
- BRA identifies new risks
- Audit identifies deficiencies
- New products/services/delivery channels introduced

8.3 Communication

Policy communicated to all employees through:

- Training sessions
- Internal announcements
- Accessible policy repository

9. REGULATORY EXAMINATION

The Company provides to GCB upon request:

- Written AML Compliance Program
- Business Risk Assessment records
- Compliance Officer identification and job description

- Unusual transaction reports (internal and external)
- Frozen account records
- Training records
- Independent audit reports
- Customer files (risk assessments, CDD, acceptance, transaction information)

10. DEFINITIONS

Business Risk Assessment (BRA): Assessment of ML/TF/FP risks the Company's business is generally exposed to

Customer Due Diligence (CDD): Process of identifying customers and verifying their identity, understanding purpose of relationship, and ongoing monitoring

Customer Risk Assessment (CRA): Customer-specific assessment categorizing ML/TF/FP risk as low, medium, or high

Enhanced Due Diligence (EDD): Additional CDD measures for higher-risk situations

Financial Intelligence Unit (FIU): Curaçao FIU receiving unusual transaction reports

Financial Transactions: Deposits, withdrawals, and account funding (not gambling transactions)

Politically Exposed Person (PEP): Individual entrusted with prominent public function (foreign, domestic, or international organization)

Simplified Due Diligence (SDD): Reduced CDD measures for lower-risk situations

Source of Funds: How funds for particular transaction were obtained

Source of Wealth: Origin of all money customer has accumulated over lifetime

Unusual Transaction: Transaction meeting objective or subjective indicators per NORUT

12. POLICY REVIEW AND APPROVAL

Version	Date	Approved By	Next Review Date
2.0	Adrian Toshkov Compliance Officer	08.10.25	

Signature: _____

Name: [Board Member Name]

Title: [Title]

Date: _____

END OF POLICY

APPENDIX A: SANCTIONS LISTS RESOURCES

- **UN Sanctions:**
<https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>
- **EU Sanctions:** <http://www.sanctionsmap.eu/#/main>
- **FATF Lists:** www.fatf-gafi.org
- **CFATF Statements:** www.cfatf-gafic.org
- **Transparency International Corruption Index:**
www.transparency.org

APPENDIX B: INDICATORS CHECKLIST

Objective Indicators (≥NAf. 5,000 per gaming day):

- ☐ Cashless transaction
- ☐ Deposit or withdrawal request
- ☐ Chip/token/credit sale
- ☐ Cash out
- ☐ Credit card transaction
- ☐ E-wallet transaction

Subjective Indicators:

- ☐ Reported to Police/Justice for ML/TF
- ☐ Customer on sanctions list
- ☐ Transaction inconsistent with customer profile
- ☐ Significantly greater transaction value than normal
- ☐ Gaming pattern inconsistent with normal
- ☐ Payment to blacklisted country
- ☐ Transaction with sanctioned person