

KYC Policy

Know Your Customer Policy

FarUp Entertainment N.V.

Registration No. 163294

Scharlooweg 39, Willemstad, Curaçao

Licensed and Regulated by Curaçao eGaming | Licence No. OGL/2024/361/0119

April 2026

1. Purpose and Scope

This KYC Policy establishes the framework through which the organisation identifies, verifies, and monitors its customers to mitigate risks related to money laundering (ML), terrorist financing (TF), proliferation financing (PF), fraud, and other financial crime.

The policy aims to ensure compliance with applicable regulatory requirements, issued by the Curaçao Gaming Control Board, and to support a risk-based approach to the organisation's size, structure, and risk appetite.

This policy applies to:

- All brands operated by the organisation:
 1. CasinoFriday
 2. Shotz
 3. BetFriday
- All customers across casino and sportsbook products
- All onboarding, payment, and monitoring systems
- Risk, Fraud, AML, and Compliance function

2. Responsibility

KYC responsibilities are allocated as follows:

- **Customer service agent** Responsible for reviewing KYC documents in low-risk situations, while also identifying and escalating medium to high-risk customers to risk team or the compliance officer.
- **Risk Team**
Performs operational KYC tasks, including customer risk assessments, reviewing due diligence documents and conducting ongoing monitoring, while escalating high risk cases to the compliance officer that require management oversight. Such as potential PEP and Sanction list matches that cannot be successfully disqualified as false positives, customers with potential adverse media, customers risk is difficult to establish, or their due diligence is unusually complex.
- **Compliance officer** Responsible for oversight of the KYC framework, effectiveness of controls, and escalation of organization-wide risks to senior management, review high risk customers for suspicious activity, and when necessary, create a SAR/STR report. Additionally, compliance officer can function as operational assistance when required.
- **Senior Management**
Approves high-risk customer relationships, such as high-risk cases, which might not be acceptable with business risk appetite.

3. Timing of Customer Due Diligence

The organisation applies a risk-based, three-tiered customer due diligence framework, consisting of Customer Due Diligence (CDD), Additional Due Diligence (ADD), and Enhanced Due Diligence (EDD). The level of due diligence applied is determined by the customer's risk profile, transactional behaviour, and identified risk indicators.

3.1 Customer Due Diligence (CDD)

Customer Due Diligence is conducted at the onboarding stage.

At registration, customers are requested to provide customer due diligence documents, before they are able to conduct any withdrawals, and the account will be suspended after they reach the 4000 XCG threshold, if the following due diligence is not provided:

- Proof of identity (ID)
- Proof of address (POA)

CDD aims to verify the customer's identity and establish the basis for the business relationship prior to or at an early stage of account activity.

3.2 Additional Due Diligence (ADD)

Additional Due Diligence (ADD) represents an intermediate control layer applied to customers assessed as Medium Risk, where standard Customer Due Diligence is not sufficient, but Enhanced Due Diligence is not yet warranted.

The objective of ADD is to:

- Better understand the customer's financial profile and background
- Assess whether gambling activity is consistent with declared circumstances
- Mitigate risks arising from anonymity, elevated transaction levels, or insufficient transparency

3.3 ADD Measures

Customers subject to ADD are required to undergo:

a) Source of Wealth / Source of Funds Questionnaire

Collects the following customer information:

- Nationality
- Country of birth
- Occupation
- Annual income
- Primary source of funds used for gambling

b) Open Source / Adverse Media Checks

- Screening of publicly available information to identify potential links to:
- Financial crime
- Fraud
- Sanctions exposure
- Other reputational or regulatory risks

3.4 Triggers for Additional Due Diligence

ADD is triggered where a customer is assessed as Medium Risk, including but not limited to the following scenarios:

1. Threshold-Based Risk Assessment (XCG 4,000)

- A Customer Risk Assessment (CRA) is triggered at XCG 4,000 cumulative deposits
- The customer is assigned Medium Risk due to **product or payment method risk**, where:
- Payment methods are anonymous or lack sufficient transparency, and
- Risk cannot be adequately mitigated through verification of payment method ownership

2. High Velocity Depositing (XCG 10,000 in 24 hours)

- The customer deposits XCG 10,000 within a 24-hour period
- There is **no clear evidence of recycling previously withdrawn winnings**
- The customer is risk rated as Medium Risk following assessment

3. Elevated Activity Over Time (XCG 40,000 in 30 days)

- The customer deposits XCG 40,000 within a 30-day period
- The activity results in a Medium Risk classification based on overall risk assessment

3.5 Outcome of ADD

Following completion of ADD:

- The customer risk profile is reassessed
- If risks are sufficiently mitigated, the customer may remain at Medium Risk with continued monitoring
- Where risks remain unexplained or increase, the case is escalated to Compliance officer to review, where appropriate

3.6 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is applied where a customer is assessed as High Risk.

EDD involves obtaining documentary evidence to verify the origin of funds used for gambling. This includes, but is not limited to:

- Source of funds documentation (e.g. bank statements, payslips)
- Source of wealth documentation (e.g. asset sales, inheritance, business income)

EDD is triggered when:

- The customer is classified as High Risk based on overall risk assessment
- There are concerns regarding the legitimacy of funds
- Transactional behaviour indicates elevated ML/TF/PF risk

The objective of EDD is to mitigate the risk that the customer is funding gambling activity with illegitimate funds.

3.7 Restrictions During Due Diligence

Where any level of due diligence (CDD, ADD, or EDD) requires documentation:

- Customer withdrawals are disabled until the required documentation has been submitted and verified
- Additional restrictions (e.g. deposit or gameplay limitations) may be applied based on risk assessment

This ensures that funds cannot be removed from the platform prior to completion of required verification.

3.8 Failure to Provide Documentation

Where a customer fails to provide requested documentation:

- The customer is issued reminders and follow-up requests
- Account restrictions remain in place during this period

If documentation is not provided within 30 days:

- The business relationship is terminated
- The account is fully restricted, including:
 1. Suspension of deposits
 2. Suspension of gameplay
 3. Suspension of withdrawals

Termination decisions are documented and, where applicable, escalated to the Compliance officer for further review, including consideration of reporting obligations.

4. Documents and Information Requested

The organisation requests documents and information as part of its risk-based customer due diligence framework, with requirements proportionate to the customer's risk classification (CDD, ADD, EDD).

4.1 Types of Documents and Information

Depending on the level of due diligence applied, the organisation may request:

a) Identity and Address Verification (CDD)

- Government-issued identification (e.g. passport, national ID card, driver's licence)
- Proof of address (e.g. utility bill, bank statement, or government-issued document)

b) Payment Method Verification (ADD)

- Evidence confirming ownership of payment instruments used, including:
 1. Redacted copies of payment cards
 2. Screenshots of e-wallet accounts
 3. Bank statements linking the customer to the payment method

c) Source of Wealth Questionnaire

- Customer-provided information via questionnaire, including:
 1. Occupation
 2. Income level
 3. Source of funds used for gambling
- Supporting documentation where required, including:
 1. Payslips or employment contracts
 2. Bank statements
 3. Proof of asset sales, inheritance, or business income

d) Supporting Documentation (EDD)

Where Enhanced Due Diligence is applied, additional independent documentation may be required to verify:

- Origin of funds
- Financial profile consistency
- Legitimacy of transactions

4.2 Timing of Requests

Documents and information are requested at the following stages:

- At onboarding (Customer Due Diligence)
- At defined thresholds triggering Additional or Enhanced Due Diligence (e.g. XCG 4,000 and above)
- Upon detection of risk indicators, inconsistencies, or unusual activity
- During withdrawal processing, where verification of payment method ownership is required

4.3 Review and Verification Process

- All documentation is reviewed by trained Risk Team analytic or customer service agent
- Reviews include:
 1. Authenticity checks
 2. Consistency with customer profile and activity
- Cases involving elevated risk or uncertainty are escalated to the compliance officer

4.4 Refresh and Re-Verification

Customer information and documentation are subject to ongoing review:

- Documentation is **periodically refreshed** based on customer risk level
- Immediate re-verification is required where:
 - Customer information becomes outdated
 - Activity deviates from expected behaviour
 - New risk indicators are identified

5. Customer Due Diligence Criteria

The organisation applies a risk-based approach to customer due diligence, whereby customers are assessed and assigned a risk rating (Low, Medium, High) based on a combination of factors. These criteria are evaluated both at onboarding and throughout the customer relationship.

Customer risk assessments are conducted using a combination of automated controls, predefined alerts, and manual review.

5.1 Core Assessment Criteria

The following factors are considered when assessing customer risk:

a) Identity and Customer Profile

- Verification of identity and age
- Consistency of personal details (name, date of birth, address)
- Nationality and country of residence

b) Geographic Risk

- Customer's country of residence
- IP location and geolocation data
- Jurisdiction risk (including high-risk or restricted countries)
- Mismatches between declared residence and activity location

c) Payment Method Risk

- Type of payment method used (e.g. bank transfer, card, e-wallet, prepaid, cryptocurrency)
- Use of **anonymous or semi-anonymous payment methods**
- Verification of payment method ownership
- Indicators of **third-party usage**

d) Transaction Behaviour

- Deposit and withdrawal patterns
- Velocity of transactions (rapid or repeated deposits)
- Structuring behaviour (multiple smaller deposits to avoid thresholds)
- Use of multiple payment methods
- Attempts to withdraw to alternative payment methods (non-closed loop behaviour)
- High-value or unusual transaction activity

e) Financial Profile and Affordability

- Declared occupation and income level
- Source of funds / source of wealth (where applicable)
- Alignment between financial profile and gambling activity
- Indicators of activity inconsistent with expected affordability

f) Customer Activity and Behavioural Risk

- Gaming behaviour (e.g. rapid betting, minimal risk betting patterns)
- Recycling of funds (re-depositing winnings)
- Bonus abuse or exploitation patterns
- Sudden changes in activity levels

g) PEP and Sanctions Exposure

- Politically Exposed Person (PEP) status
- Links to sanctioned individuals or entities
- Ongoing screening results and alerts

h) Adverse Media and Open-Source Information

- Negative news or public information linking the customer to:
 - Fraud
 - Financial crime
 - Regulatory breaches
 - Other reputational risks

i) Linked Accounts and Technical Indicators

- Detection of multiple accounts linked to the same individual
- Shared devices, IP addresses, or payment instruments
- Indicators of account manipulation or collusion

5.2 Risk Rating and Outcomes

Customers are assigned a risk rating based on the combined assessment of the above factors:

- **Low Risk**
 - Standard monitoring applies
 - Simplified or standard due diligence may be sufficient
- **Medium Risk**
 - Additional Due Diligence (ADD) is applied
 - Increased monitoring and review frequency
- **High Risk**
 - Enhanced Due Diligence (EDD) is required
 - Subject to Compliance officer review and enhanced monitoring

Risk ratings are:

- Assigned at onboarding or at first risk trigger
- Updated dynamically based on customer activity and new information

5.3 Trigger-Based Risk Assessment

Customer risk assessments are triggered by, but not limited to:

- Reaching defined thresholds (e.g. XCG 4,000, XCG 10,000, XCG 40,000)
- Detection of unusual or suspicious transaction patterns
- Changes in customer behaviour or activity
- Identification of inconsistencies in customer information
- Alerts generated through internal monitoring systems

6. Ongoing Monitoring

The organisation applies a combined threshold-based and time-based ongoing monitoring framework to ensure that customer activity remains consistent with their risk profile and previously verified information.

Ongoing monitoring is conducted through a combination of automated alerts, predefined thresholds, and periodic reviews, and is proportionate to the customer's assigned risk level.

6.1 Threshold-Based Monitoring

Customers are subject to event-driven monitoring triggers, including but not limited to:

- **XCG 4,000 cumulative deposits**
 1. Triggers initial Customer Risk Assessment (CRA)
 2. Determines whether Additional Due Diligence (ADD) is required
- **XCG 10,000 in 24 hours**
 1. Triggers review for high velocity activity
 2. Assesses whether activity is consistent with prior behaviour or recycling of winnings
- **XCG 40,000 in 30 days**
 1. Triggers enhanced review of customer activity and financial profile
 2. May result in escalation to ADD or EDD depending on risk indicators

These thresholds serve as initial and event-based indicators of risk and are used to establish or reassess the customer's risk profile.

6.2 Transition to Time-Based Monitoring

Once a customer has:

- Undergone a Customer Risk Assessment, and
- Had a customer risk profile established
- Provided sufficient documentation to support their activity

the organisation transitions to a time-based ongoing monitoring approach, recognising that threshold triggers alone are not sufficient indicators of risk once activity has been explained and verified.

6.3 Risk-Based Monitoring Frequency

Customers are subject to periodic review based on their assigned risk level:

- **Low Risk** are reviewed at least once every 12 months
- **Medium Risk** are reviewed at least once every 6 months
- **High Risk** are reviewed at least once every month

Periodic reviews assess:

- Continued consistency between activity and financial profile
- Changes in behaviour or transaction patterns
- New or emerging risk indicators

6.4 Event-Driven Monitoring

In addition to periodic reviews, customers are subject to continuous event-driven monitoring, including:

- Alerts generated through internal monitoring systems
- Detection of unusual transaction patterns
- Changes in payment methods or behaviour
- Identification of inconsistencies in customer information

Event-driven triggers may result in:

- Immediate reassessment of risk
- Escalation to ADD or EDD
- Application of account restrictions where required

6.5 Inactive Customers and Reactivation

Where a customer becomes inactive:

- If no meaningful activity is observed for a period of approximately 2–3 months, the customer is temporarily removed from active ongoing monitoring cycles

Inactive customers are:

- Placed on a reactivation monitoring list

Upon reactivation (e.g. new deposit or resumed activity):

- The customer is automatically flagged
- A new risk assessment is performed as appropriate
- The customer is reinstated into the ongoing monitoring cycle based on their risk level

7. Politically Exposed Person (PEP) Screening

7.1 Timing of PEP Screening

PEP screening is performed:

- At onboarding (registration stage)
- On a periodic basis every 12 months thereafter
- If customer makes a deposit after 90 day inactivity

This ensures that changes in customer status are identified throughout the business relationship.

7.2 Screening Process

- Customers are screened against recognised PEP databases through approved third-party providers
- Screening is conducted automatically and results are reviewed by the Risk Team

Where a potential match is identified:

- The Risk Team conducts an initial review to determine whether the match is likely a false positive, based on available data (e.g. name, date of birth, jurisdiction)

7.3 Escalation and Verification

Where a match cannot be reasonably determined as a false positive:

- The case is escalated to the Compliance Officer
- Additional verification may be conducted, including:
 - Requesting supporting documentation from the customer
 - Reviewing open source and publicly available information

The objective is to confirm whether the customer is:

- A Politically Exposed Person
- A family member or close associate of a PEP

7.4 Outcome and Decision

Following review, one of the following outcomes is reached:

- **False Positive**
 1. The match is documented and cleared
 2. The customer relationship continues under standard monitoring
- **Confirmed PEP**
 1. The customer is classified as High Risk
 2. In line with the organisation's risk appetite, PEP relationships are not accepted
 3. The business relationship is terminated

7.5 Documentation and Recordkeeping

All PEP screening results, reviews, and decisions are:

- Documented and retained
- Available for audit and regulatory inspection

8. Sanctions Screening

The organisation conducts sanctions screening to ensure that it does not establish or maintain business relationships with individuals or entities subject to financial sanctions.

8.1 Timing of Sanctions Screening

Sanctions screening is performed:

- At onboarding (registration stage)
- On a periodic basis every 12 months thereafter
- If customer makes a deposit after 90 day inactivity

This ensures that customers are continuously assessed against updated sanctions lists.

8.2 Screening Process

- Customers are screened against applicable sanctions lists, including:
 1. EU Sanctions List
 2. UN Consolidated Sanctions List
 3. OFAC Sanctions list
- Screening is conducted through approved third-party providers
- Matches are identified through automated systems

8.3 Escalation and Review

Where a potential sanctions match is identified:

- The case is immediately escalated to the Compliance Officer, without preliminary clearance at Risk Team level
- The Compliance Officer conducts a review to determine whether the match is:
 1. A false positive, or
 2. A confirmed match

8.4 Outcome and Action

Following review, one of the following outcomes is reached:

- **False Positive**
 1. The match is documented and cleared
 2. No further action is required
- **Confirmed Sanctions Match**
 1. The business relationship is terminated immediately
 2. The account is fully restricted (deposits, gameplay, withdrawals)
 3. The case is escalated without delay by the Compliance Officer through a Suspicious Activity Report (SAR) to the Financial Intelligence Unit (FIU)

Where applicable, additional measures may include:

- Immediate blocking of funds in accordance with legal obligations
- Internal escalation to senior management

8.5 Documentation and Recordkeeping

All sanctions screening results, reviews, and decisions are:

- Fully documented
- Retained for audit and regulatory purposes
- Maintained in line with applicable recordkeeping requirements

9. Threshold Procedure

The organisation applies defined transactional thresholds as key control points within its customer due diligence and monitoring framework. These thresholds trigger mandatory reviews, escalation, and due diligence actions to ensure that customer activity remains consistent with their risk profile and regulatory expectations.

9.1 Monitoring of Thresholds

Customer activity is continuously monitored through automated systems and internal controls to identify when predefined thresholds are reached.

Key thresholds include:

- **XCG 4,000 (cumulative deposits or withdrawals)**
- **XCG 10,000 within 24 hours**
- **XCG 40,000 within 30 days**

Thresholds are monitored in real time and supported by daily reporting and alert systems.

9.2 Operational Process at XCG 4,000 Threshold

When a customer reaches XCG 4,000:

- A Customer Risk Assessment (CRA) is triggered
- A customer risk profile is established (Low, Medium, or High Risk)
- Appropriate due diligence level is applied:
 1. Low Risk → Standard monitoring
 2. Medium Risk → Additional Due Diligence (ADD)
 3. High Risk → Enhanced Due Diligence (EDD)

Where required:

- Documentation requests are initiated
- Withdrawals are restricted until verification is completed

9.3 Operational Process at Elevated Thresholds

XCG 10,000 within 24 hours

- Customer activity is reviewed for high velocity behaviour
- Assessment is conducted to determine whether:
 1. Activity represents legitimate recycling of winnings, or
 2. Indicates increased risk

Where risk indicators are present:

1. Customer may be assigned Medium or High Risk
2. ADD or EDD is triggered accordingly

XCG 40,000 within 30 days

- A comprehensive review of customer activity is conducted
- Financial profile and source of funds alignment are reassessed

Where risk is identified:

- Escalation to EDD is required
- Additional documentation may be requested
- Account restrictions may be applied

9.4 Restrictions and Controls at Thresholds

Where due diligence is triggered at any threshold:

- Withdrawals are immediately restricted upon request for documentation
- Additional restrictions (deposits, gameplay) may be applied based on risk level

These controls ensure that:

- Funds cannot be withdrawn prior to completion of required verification
- Identified risks are mitigated before further account activity is permitted

9.5 Customer Follow-Up and Responsibility

- The Risk Team is responsible for:
 1. Initiating documentation requests
 2. Following up with customers
 3. Monitoring submission timelines
- Cases involving elevated risk or non-cooperation are escalated to compliance Officer, where appropriate

9.6 Link to Ongoing Monitoring

Once threshold-triggered reviews are completed and a customer risk profile has been established and supported by documentation:

- Customers transition to time-based ongoing monitoring in accordance with Section 6
- Thresholds remain active as event-driven triggers, but are no longer the sole basis for monitoring

10. Missing Documents at Threshold

The organisation applies a structured follow-up and escalation process where required customer due diligence documentation is not provided following a threshold-triggered request.

10.1 Initial Request and Follow-Up

Where documentation is required as part of CDD, ADD, or EDD:

- The customer is formally requested to provide the required information and/or documentation
- Requests are issued through appropriate communication channels (e.g. email, account notification)
- The Risk Team is responsible for monitoring and following up on outstanding requests

Follow-up actions include:

- Automated reminders
- Manual follow-up where necessary

10.2 Account Handling During Pending Documentation

While documentation remains outstanding:

- Withdrawals are restricted and cannot be processed
- Additional restrictions (e.g. deposits or gameplay) may be applied based on the customer's risk profile

These measures remain in place until:

- Documentation is received and verified, or
- The case is escalated further

10.3 Escalation of Non-Compliance

Escalation is applied on a risk-based basis:

- Where a customer is assessed as High Risk and:
 1. Refuses to provide requested documentation, or
 2. Fails to provide documentation within the required timeframe

→ The case is escalated to the Compliance Officer for review
- For Low and Medium Risk customers:
 1. Follow-up continues until the defined deadline is reached
 2. Escalation may occur if additional risk indicators emerge

10.4 Outcome of Missing Documentation

If documentation is not provided within **30 days** of the initial request:

- The business relationship is **terminated**
- The account is fully restricted, including:
 1. Suspension of deposits
 2. Suspension of gameplay
 3. Suspension of withdrawals
- Where applicable (particularly for High Risk cases), the matter is reviewed by the Compliance Officer to determine whether external reporting obligations (e.g. FIU reporting) apply

10.5 Documentation and Audit Trail

All actions related to missing documentation are:

- Recorded in the customer account and internal systems
- Supported by a clear audit trail, including:
 1. Initial request
 2. Follow-up attempts
 3. Escalation actions (where applicable)
 4. Final decision

11. Thirty-Day Follow-Up

The organisation applies a defined decision-making process where required due diligence documentation has not been provided within 30 days of the initial request.

11.1 Review at 30-Day Mark

At the expiry of the 30-day period:

- The case is reviewed by the Risk Team to confirm:
 1. Documentation has not been received
 2. Follow-up actions have been completed in accordance with internal procedures

11.2 Decision and Outcome

Where documentation remains outstanding after 30 days:

- The business relationship is terminated
- The account is fully restricted, including:
 1. Suspension of deposits
 2. Suspension of gameplay
 3. Suspension of withdrawals

This action is applied consistently to ensure that no customer relationship is maintained without completion of required due diligence.

11.3 High-Risk Escalation

Where the customer has been assessed as High Risk:

- The case is escalated to the Compliance Officer for review prior to, or in conjunction with, termination

The review considers:

- Whether the failure to provide documentation increases suspicion
- Whether the case meets the threshold for external reporting (e.g. FIU)

11.4 Documentation of Decision

All decisions taken at the 30-day stage are:

- Clearly documented, including:
 1. Reason for termination
 2. Customer risk level
 3. Any escalation actions taken
- Retained as part of the customer's compliance record for audit and regulatory purposes

12. Termination of the Business Relationship

The organisation applies a defined process for terminating customer relationships where regulatory requirements are not met or where the customer presents an unacceptable level of risk.

12.1 Grounds for Termination

A customer relationship may be terminated where:

- Required due diligence documentation is not provided within the defined timeframe (e.g. 30 days)
- The customer is assessed as High Risk and risks cannot be adequately mitigated
- There are unresolved concerns relating to:
 1. Source of funds or wealth
 2. Transaction behaviour
 3. Payment method ownership
- A confirmed PEP or sanctions match is identified (in line with risk appetite)
- The customer is found to be engaging in:
 1. Third-party payment method usage
 2. Fraud, abuse, or other prohibited activity

Termination decisions are based on a risk-based assessment and aligned with the organisation's defined risk appetite.

12.2 Decision Authority

- Termination decisions are:
 1. Executed operationally by the Risk Team, and
 2. Escalated to the Compliance Officer:
 - A. The customer is classified as High Risk
 - B. Suspicion of ML/TF/PF exists
 - C. Regulatory reporting may be required

12.3 Account Handling Upon Termination

Upon termination:

- The account is fully restricted, including:
 1. Suspension of deposits
 2. Suspension of gameplay
 3. Suspension of withdrawals
- Access to the account is disabled, preventing further use of the platform

12.4 Handling of Customer Funds

Customer funds are handled in accordance with regulatory obligations and risk considerations:

- Where no suspicion exists:
 1. Remaining balances may be returned via the original payment method, where feasible
- Where risk indicators or concerns exist:
 1. Funds may be subject to additional review
 2. Payment may be delayed or restricted pending internal assessment
- Where legally required (e.g. sanctions cases):
 1. Funds may be frozen and not returned

12.5 Escalation and Reporting Considerations

All terminated relationships are subject to review to determine whether:

- The case should be escalated to the Compliance Officer
- A Suspicious Activity Report (SAR) should be filed with the Financial Intelligence Unit (FIU)

This applies particularly where:

- There is suspicion of ML/TF/PF
- The customer has failed to cooperate in a High-Risk scenario

12.6 Documentation and Recordkeeping

All termination decisions are:

- Fully documented, including:
 1. Reason for termination
 2. Customer risk classification
 3. Actions taken on the account
 4. Any escalation or reporting decisions
- Retained in accordance with recordkeeping requirements for audit and regulatory review

13. Freezing of Funds and Reporting

The organisation applies immediate and proportionate measures where legal or regulatory obligations require the restriction of customer funds and reporting to competent authorities.

13.1 Trigger Event

Freezing of funds and reporting obligations may arise where:

- A confirmed sanctions match is identified
- There is a legal obligation to restrict access to funds
- A competent authority requires or directs such action
- There are sufficient grounds to suspect money laundering, terrorist financing, or proliferation financing

13.2 Freezing of Funds

Where a confirmed sanctions match or legal requirement is identified:

- Customer funds are frozen without delay
- The account is immediately restricted, including:
 - Suspension of deposits
 - Suspension of gameplay
 - Suspension of withdrawals

No transactions are permitted on the account while the restriction remains in place.

13.3 Internal Escalation

Upon identification of a trigger event:

- The case is immediately escalated to the Compliance Officer
- Relevant internal stakeholders are informed as required

The Compliance Officer assumes responsibility for:

- Reviewing the case
- Determining appropriate actions
- Ensuring regulatory obligations are fulfilled

13.4 External Reporting

Where required, the Compliance Officer:

- Submits a Suspicious Activity Report (SAR) or equivalent report to the Financial Intelligence Unit (FIU) without delay
- Ensures that reporting is conducted in accordance with applicable legal and regulatory requirements

Reporting obligations apply particularly in cases involving:

- Confirmed sanctions matches
- Suspicion of ML/TF/PF
- Transactions meeting statutory reporting thresholds

13.5 Prohibition of Tipping-Off

At no point is the customer informed that:

- A report has been filed with the FIU
- Their account is under investigation
- Any internal escalation or suspicion exists

All actions are conducted in strict compliance with tipping-off prohibitions.

13.6 Documentation and Recordkeeping

All actions relating to freezing of funds and reporting are:

- Fully documented, including:
 1. Trigger event
 2. Actions taken
 3. Internal escalation
 4. Reporting details
- Retained in accordance with regulatory recordkeeping requirements minimum 10 years
- Made available for audit and regulatory inspection