



Surewin B.V

Linked transaction Detection  
and Escalation Process

## CONTENTS

|                                                                |   |
|----------------------------------------------------------------|---|
| 1. LINKED TRANSACTION DETECTION AND ESCALATION PROCEDURE ..... | 2 |
| 1.1 Linked Transaction Detection Rules .....                   | 2 |
| 1.2 Review Procedure .....                                     | 3 |
| 1.3 Escalation Procedure .....                                 | 3 |
| 1.4 Investigation Outcomes .....                               | 3 |
| 1.5 Record Keeping .....                                       | 4 |
| 1.6 Quality Assurance .....                                    | 4 |
| 1.7 Ongoing Monitoring .....                                   | 4 |
| 1.8 Review Of This Procedure .....                             | 5 |

## 1. LINKED TRANSACTION DETECTION AND ESCALATION PROCEDURE

### Purpose

The Company maintains formal procedures to identify, review and investigate linked, connected or structured transactions that, when viewed individually, may appear below applicable monitoring or due diligence thresholds but, when aggregated, indicate an elevated risk of money laundering, terrorist financing, fraud or other financial crime. This procedure supports the Company's Risk-Based Approach and shall be read together with the AML/CFT Policy, Customer Due Diligence procedures, Enhanced Due Diligence procedures, Ongoing Monitoring procedures and Unusual Transaction Reporting procedures contained within this Operations Manual.

### Definition of Linked Transactions

For the purposes of this Manual, linked transactions are two or more transactions that are connected through a customer, payment instrument, account, device, behaviour or other common characteristic and which, when considered collectively, may indicate an increased level of financial crime risk.

Linked transactions may occur over a short or extended period and shall not be assessed solely by reference to individual transaction values.

#### 1.1 Linked Transaction Detection Rules

Risk Analysts shall assess transactions both individually and cumulatively.

Transactions shall be considered linked where one or more of the following indicators are identified:

- Common customer.
- Common beneficial owner.
- Shared payment card.
- Shared bank account.
- Shared e-wallet.
- Shared payment method.
- Shared IP address.
- Shared device or device fingerprint.
- Shared residential address.
- Shared email address or telephone number.
- Shared withdrawal destination.
- Similar registration details.
- Coordinated gameplay or betting behaviour.
- Common Source of Funds.
- Repeated transactions designed to avoid verification thresholds.
- Any other indicator suggesting common control or coordination.

No single indicator automatically confirms suspicious activity. Investigators shall consider the customer's overall profile, historical activity and cumulative transactional behaviour before reaching a conclusion.

## 1.2 Review Procedure

Where a linked transaction indicator is identified, the Risk Team shall:

1. Review the customer's profile and risk rating.
2. Aggregate all relevant transactions.
3. Review deposits, withdrawals and gameplay.
4. Review KYC documentation.
5. Review payment methods and ownership.
6. Review Source of Funds information where applicable.
7. Determine whether Enhanced Due Diligence is required.
8. Record all findings and supporting evidence.
9. Escalate the matter where required.

## 1.3 Escalation Procedure

Where concerns remain following the initial review, the matter shall be escalated as follows:

| <b>Risk Level</b>   | <b>Escalation</b>                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------|
| Low                 | Record findings and continue monitoring                                                              |
| Medium              | Escalate to Compliance Officer for review                                                            |
| High                | Escalate immediately to the MLRO                                                                     |
| Suspicious Activity | MLRO to determine whether an Unusual Transaction Report (UTR) should be submitted to the FIU Curaçao |

Escalation shall occur immediately where there are reasonable grounds to suspect money laundering, terrorist financing, sanctions breaches, organised fraud or deliberate structuring of transactions.

## 1.4 Investigation Outcomes

Following investigation, one or more of the following actions may be taken:

- No further action.
- Continue enhanced monitoring.
- Request additional KYC documentation.
- Request Source of Funds documentation.
- Request Source of Wealth documentation where appropriate.
- Apply Enhanced Due Diligence.
- Apply a temporary withdrawal hold.
- Restrict account activity.
- Refer the matter to the MLRO.
- Submit an Unusual Transaction Report where determined appropriate by the MLRO.
- Close the customer relationship where required in accordance with the AML/CFT Policy and Terms and Conditions.

## 1.5 Record Keeping

All linked transaction investigations shall be documented within the Company's case management or back-office system.

Records shall include:

- customer reference;
- investigation trigger;
- transactions reviewed;
- supporting evidence;
- actions taken;
- escalation details;
- final outcome; and
- approving officer.

Records shall be retained in accordance with the Company's Record Retention requirements and applicable AML/CFT legislation.

## 1.6 Quality Assurance

Compliance shall periodically review linked transaction investigations to ensure:

- consistent application of this procedure;
- timely escalation of higher-risk cases;
- appropriate documentation of decisions;
- compliance with the AML/CFT Policy; and
- ongoing effectiveness of transaction monitoring controls.

Any material deficiencies identified shall be reported to Senior Management and the Board as part of the Company's AML governance framework.

## 1.7 Ongoing Monitoring

Where a linked transaction investigation does not result in account closure or external reporting, the customer may remain subject to enhanced monitoring. Such monitoring may include increased transaction scrutiny, lower internal review thresholds, periodic Source of Funds reviews, repeat Enhanced Due Diligence, or other proportionate controls based on the customer's assessed risk profile.

## 1.8 Review Of This Procedure

This procedure shall be reviewed at least annually or sooner where there are material changes to applicable legislation, regulatory requirements, the Company's AML/CFT Policy, operational processes or identified financial crime risks. Any material amendments shall be approved in accordance with the Company's governance procedures.