**SAUDI NATIONAL BANK**

**FRAUD INVESTIGATION CASE REPORT**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Case ID:** | CASE\_SA-TXN-0000000013 |
| **Transaction ID:** | SA-TXN-0000000013 |
| **Customer ID:** | SA00000302 |
| **Case Status:** | CONFIRMED\_FRAUD |
| **Priority Level:** | HIGH |
| **Report Date:** | 2025-10-05 00:29 |

**1. EXECUTIVE SUMMARY**

Final Classification: FRAUD  
Confidence Level: 90%  
Transaction Amount: 30,604.76 SAR  
  
Summary:  
Multiple strong fraud indicators present. Immediate action required.

**2. TRANSACTION DETAILS**

|  |  |
| --- | --- |
| **Transaction ID** | SA-TXN-0000000013 |
| **Customer ID** | SA00000302 |
| **Customer Name** | Sarah Ahmed |
| **Date & Time** | 2025-10-03 07:31:59 |
| **Amount** | 30,604.76 SAR |
| **Beneficiary** | Jennifer Silva |
| **Beneficiary Bank** | Medina PLC Bank |
| **Beneficiary Country** | Syria |
| **Transfer Type** | SWIFT Transfer |
| **Transfer Purpose** | Gift |
| **ML Fraud Score** | 0.958 |
| **Nationality** | Saudi |
| **SAMA AML Flag** | YES |

**3. CUSTOMER INFORMATION**

Profile Summary: Customer since 2021-04-19, Risk Level: Low, KYC: Verified

Login Activity: No recent login data

Device Information: 4 devices registered, 4 trusted

**4. RISK ASSESSMENT & CLASSIFICATION**

Initial Classification: FLAGGED

Confidence: 85%

* Risk Factors Identified:
* High ML fraud score: 0.958
* Velocity flag triggered
* Suspicious beneficiary location: Syria

Behavioral Analysis:

• Profile Risk: UNKNOWN

• Login Risk: UNKNOWN

• Device Risk: HIGH

**5. INVESTIGATION FINDINGS**

* Data Sources Analyzed:
* Transaction
* Customer Profile
* Login History
* Device Fingerprints

Detailed Analysis:

HIGH due to high transaction amount exceeding average by 6.6x, indicating a possible large-scale fraudulent activity or money laundering. Additionally, the detection of 1 suspicious device indicates that this account may be associated with malicious intent.  
  
This analysis aims to identify potential risks and threats related to transactions made by an individual customer using their account on our platform. It considers various factors such as the transaction amount, login history, country, and device information. By evaluating these factors, we can determine whether the risk level should be classified as HIGH, MEDIUM, or LOW.  
  
In this case, the high transaction amount and the presence of a suspicious device raise significant concerns about the legitimacy of the transaction and the potential for fraud or money laundering. This analysis suggests that further investigation and monitoring are necessary to mitigate any potential risks.   
  
To address the identified risks, consider implementing additional security measures such as:  
  
\* \*\*Enhanced Authentication\*\*: Implement multi-factor authentication (MFA) or one-time passwords (OTPs) to verify the user's identity.  
\* \*\*Device Monitoring\*\*: Continuously monitor the user's device and location to detect any unusual activity.  
\* \*\*Transaction Review\*\*: Thoroughly review all transactions to ensure they align with the user's expected behavior and financial history.  
\* \*\*Collaboration with Law Enforcement\*\*: If the risk assessment indicates a high likelihood of fraud or money laundering, collaborate with law enforcement agencies to report and investigate the suspected activity.  
  
By taking proactive steps to address these risks, you can help protect your customers' accounts and maintain the integrity of your platform.

* Behavioral Anomalies Detected:
* Transaction amount 30604.76 is 6.6x above average
* 1 suspicious devices detected

**6. SAMA COMPLIANCE & AML REQUIREMENTS**

SAMA AML/CFT Compliance Check:

✓ Large Transaction Reporting: Amount 30,604.76 SAR exceeds SAMA threshold of 20,000 SAR

✓ High-Risk Jurisdiction: Transfer to Syria requires enhanced due diligence

✓ Suspicious Activity Report (SAR): Case requires filing with SAMA FIU

Regulatory Framework:  
• Anti-Money Laundering Law (Royal Decree No. M/31)  
• SAMA AML/CFT Rules 2018  
• FATF Recommendations Compliance

**7. RECOMMENDED ACTIONS**

* Immediate Actions Required:
* 1. Block transaction immediately
* 2. Freeze customer account
* 3. Contact customer for verification
* 4. File fraud report
* 5. Initiate chargeback if applicable

**8. APPROVALS & SIGN-OFF**

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Signature & Date** |
| Fraud Analyst |  |  |
| Team Manager |  |  |
| Compliance Officer |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*CONFIDENTIAL - Saudi National Bank - Fraud Investigation Report  
Generated: 2025-10-05 00:29:45  
This document contains confidential information and is subject to SAMA regulations.*