**SAUDI NATIONAL BANK**

**FRAUD INVESTIGATION CASE REPORT**

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

|  |  |
| --- | --- |
| **Case ID:** | CASE\_SA-TXN-0000000011 |
| **Transaction ID:** | SA-TXN-0000000011 |
| **Customer ID:** | SA00000044 |
| **Case Status:** | SUSPECTED\_FRAUD |
| **Priority Level:** | MEDIUM |
| **Report Date:** | 2025-10-05 00:22 |

**1. EXECUTIVE SUMMARY**

Final Classification: SUSPICIOUS  
Confidence Level: 70%  
Transaction Amount: 73,324.81 SAR  
  
Summary:  
Significant suspicious activity. Enhanced monitoring recommended.

**2. TRANSACTION DETAILS**

|  |  |
| --- | --- |
| **Transaction ID** | SA-TXN-0000000011 |
| **Customer ID** | SA00000044 |
| **Customer Name** | Turki Fahad |
| **Date & Time** | 2025-09-27 06:36:59 |
| **Amount** | 73,324.81 SAR |
| **Beneficiary** | Fahad Salem |
| **Beneficiary Bank** | Henderson-Bernard Bank |
| **Beneficiary Country** | UAE |
| **Transfer Type** | SWIFT Transfer |
| **Transfer Purpose** | Loan Repayment |
| **ML Fraud Score** | 0.239 |
| **Nationality** | Expatriate |
| **SAMA AML Flag** | YES |

**3. CUSTOMER INFORMATION**

Profile Summary: Customer since 2023-03-07, Risk Level: Medium, KYC: Verified

Login Activity: 10 recent logins from 3 countries: Saudi Arabia, Pakistan, Turkey

Device Information: 3 devices registered, 3 trusted

**4. RISK ASSESSMENT & CLASSIFICATION**

Initial Classification: FLAGGED

Confidence: 70%

* Risk Factors Identified:

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 Risk due to the unusually high transaction amount and presence of suspicious devices, indicating potential malicious activity. The device information suggests an attempt to bypass security measures or hide identity.   
  
Recommendation:  
Investigate transactions for money laundering and proceed with account freezing until further analysis.   
  
Additional Notes:  
Device Information - 4 unique IPs and 2 mobile devices reported; IP addresses are from 3 different countries, with 2 of them being known hotspots for fraud. Mobile devices used for login appear to be compromised or stolen, suggesting an attempt to disguise user's location. The majority of these devices are not registered to any legitimate account holder.   
  
Note: Device Information might have been removed from this analysis as it may be considered sensitive information.  
  
Based on the system output:  
The customer has a low risk profile given their age (942 days) and previous lack of fraudulent activities (Prev Fraud: 0). However, there are concerns raised by the large transaction amount and suspicious device data.  
To mitigate risks, I would recommend investigating the transaction and potentially freezing the account until further analysis can determine the legitimacy of the transaction.  
In addition, monitoring the device information to identify any potential security breaches or unauthorized access to the account.   
To ensure compliance with regulatory requirements, conducting thorough background checks on all accounts with high-risk profiles.  
Given the situation, a more detailed review of the device information is warranted to better understand its implications.  
The customer’s account should be flagged for further investigation into the unusual transaction activity.  
Monitoring and tracking the account for potential future suspicious activity is essential to maintaining the integrity of the financial institution and preventing potential losses.  
The customer's age indicates that they are likely an adult, which could suggest a higher likelihood of legitimate financial activity; however, the device data raises red flags regarding potential security threats.  
Further investigation is necessary to clarify the legitimacy of the transaction and to assess whether the customer is aware of the device usage and can confirm their identity.   
In conclusion, while the customer appears to be at lower risk based on their age, the anomalies detected warrant further scrutiny. A comprehensive review of all available data is needed to make an informed decision about the account's status.   
To prevent potential losses, additional monitoring and reporting are recommended for this account.   
It is highly recommended to collaborate with other departments such as IT and Law Enforcement to gain a deeper understanding of the device information and its implications for the case.  
Given the findings, it is advisable to temporarily freeze the account pending further review and collaboration with relevant authorities to address potential security concerns.   
Due to the potential security threat posed by the suspicious devices, I recommend a comprehensive review of all available data and a collaboration with law enforcement agencies to investigate the matter thoroughly.  
Based on the system output, the customer’s account does not seem to pose an immediate significant risk, but there are several red flags that require attention.  
A full review of the account's history and current activity is required to assess whether the transaction was legitimate or if there were any other suspicious

* Behavioral Anomalies Detected:
* Transaction amount 73324.81 is 23.7x above average
* 1 suspicious devices detected

**6. SAMA COMPLIANCE & AML REQUIREMENTS**

SAMA AML/CFT Compliance Check:

✓ Large Transaction Reporting: Amount 73,324.81 SAR exceeds SAMA threshold of 20,000 SAR

✓ 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. Place temporary hold on account
* 2. Request additional customer verification
* 3. Monitor account closely for 48 hours
* 4. Review with fraud specialist

**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 00:22:45  
This document contains confidential information and is subject to SAMA regulations.*