FRAUD DETECTION RULES & REPORTING SYSTEM IMPLEMENTATION REPORT

OBJECTIVE:

This report outlines the rules we can setup to detect fraud in our payment system and stop these fraudulent activities before the cause harm. I will use rules such as transaction thresholds, IP address monitoring, behavioral patterns, and other key indicators that could signal fraudulent activity. By setting these rules, the system will help mitigate risks and protect both customers and the platform.

TOOLS USED: Excel.

FUNCTIONS:

CountIF – Used to aggregate the data to generate summary.

Pivot Table – Used to analyze user behavior by summarizing number of alert triggered by each user.

FRAUD DETECTION RULES

1. **Failed Payments Thresholds**:

Rule: Transactions should be flagged if there are two or more failed payment attempts from the same account within a short time frame (e.g., 24 hours). For example: A user attempts to process three failed payments in 24 hours this should trigger the fraud alert.

Action: If this threshold is met, the transaction should be blocked automatically, and an alert sent to the fraud prevention team for manual review.

2. **Large Transactions**:

Rule: Any transaction above 50% of a user's average transaction amount should be flagged as potentially suspicious. Example: If a user who typically spends between 10,000 to 20,000 Naira now attempts to transfer 100,000 Naira, this should trigger an alert.

Action: The system should automatically trigger a review and block the transaction until further verification is completed by the user.

3. **Repeated Transactions**:

Rule: If a user makes the same transaction repeatedly (e.g., same amount, same beneficiary) within a short time span like 15 minutes, the system should flag the transaction as suspicious.

Action: The system should block these repetitive transactions and flag them for investigation.

4. **Unusual Time of Transaction:**

Rule: Transactions made during off-hours example late night or early in the morning should be flagged as suspicious unless proven otherwise.

Action: The system should trigger a temporary block, and the user will be required to authenticate themselves before proceeding.

5. **Multiple Accounts from Same IP**

Rule: Flag accounts with multiple registrations from the same IP address. Detect two or more accounts registered from the same IP address in a short time.

Action: Flag accounts for manual review or limit the number of accounts allowed per IP address.

6. **Suspicious Payment Method Usage**

Rule: Flag suspicious payment methods or multiple failed attempts with specific cards. When there is an increased use of prepaid or virtual cards, or card payment failures greater than 3 times in one month.

Action: Require additional verification steps or review the payment method.

7. **Multiple Withdrawals in Short Time Period**

Rule: Flag drivers or customers making multiple withdrawals from wallets in a short time. More than two payouts within 24 hours.

Action: Temporarily block additional withdrawals and trigger a review of the account.

MOCK DATASET REPORTING

In the generated 100 transactions, the fraud detection rules successfully flagged 49 alerts, resulting in an Alert Rate of 49%.

The primary focus areas for immediate investigation and rule tuning are the top three alert categories, which collectively account for over half of all flags.

1. **Multiple Accounts from Same IP (8 Alerts):** This is a critical red flag, often associated with fraudulent users creating multiple accounts to exploit sign-up bonuses or other incentives.
   Recommendation: Prioritize the Action of flagging these accounts for manual review or implementing a hard limit on new accounts allowed per IP address, as suggested in the rules document.
2. **Repeated Transaction in a Short Time (8 Alerts**): This velocity rule is detecting rapid, potentially automated transactions.
   Recommendation: Review the time window (e.g., 15 minutes) and consider implementing an automatic block of repetitive transactions to prevent financial loss, as detailed in the rules document.

3. **Multiple Failed Attempts (6 Alerts):** This indicates users potentially cycling through payment methods (card testing) or issues with the payment gateway integration.
   Recommendation: Ensure the Action to automatically block transactions after the failed payment threshold is implemented to prevent further attempts.

RECOMMENDATION

User Behavior Analysis: Use the data from the Pivot Table to identify users (U12, U2, U8) that have triggered multiple types of alerts, indicating high-risk accounts requiring immediate attention.

Performance Monitoring: Begin tracking all metrics against a weekly or monthly baseline to identify positive or negative trends in the Alert Rate.

Refine Rules & Actions: Collaborate with the Product Management and Cybersecurity teams to review and potentially tighten the thresholds (e.g., velocity rules) and implement the prescribed automatic actions (e.g., blocking repetitive transactions or limiting accounts per IP) to proactively reduce exposure to financial loss.