CA Payment Security Consulting

CA Risk Analytics – Rules Configuration Best Practices
Version 1.0

ca technologies

Rules Configuration Best Practices

- ✓ Identify the scenarios with generic criteria to catch fraudulent transactions e.g. suspected device id, merchants etc. and write the rules with **DENY** or **INCREASE AUTH** risk advice as appropriate with priority between **EXCEPTION** Rule and Zero Touch rules.

- ✓ Apply UNENROLLED Action, USER/Device Known, Association and Maturity rules with higher priority than Zero Touch rule to challenge the transactions from non/less trust worthy PANs and devices.

- ✓ Apply Velocity rules with higher priority than Zero Touch rules to identify frequent transactions from same PANs or Devices and decline or challenge such transactions

- ✓ Use USERSTATE feature to blacklist PANs identified in High Value Fraudulent transactions and setup a rule to auto decline blacklisted PANs with higher priority than Zero Touch rule.

ca technologies

Rules Configuration Best Practices

- ✓ Use USERSTATE feature to mark PANs as suspect identified in Medium/Low Value Fraudulent transactions and setup a rule to challenge suspected PANs with higher priority than Transparent Authentications.

- ✓ Blacklist untrusted Merchants, Device IDs & IP Addresses identified with more number of high value fraudulent transactions and setup rules with DENY advice and suitable amount/predictive score thresholds.

- ✓ Create gray list of less trustworthy Merchants, Device IDs & IP Addresses identified with more number of medium/low value fraudulent transactions with amount/predictive score thresholds.

- ✓ Any Zero Touch criteria written as separate rule should be configured as lowest priority with risk score 0.

Rules Configuration Best Practices

- ✓ Add new rules with thorough understanding and review of the use-cases.
- ✓ Define the rule criteria and write the same with risk score of **0** to review its performance for few days. If rule performance is satisfactory modify the risk score appropriately for desired risk advice otherwise iteratively revise the rule criteria until desired outcome is achieved.
- ✓ Transactions matching DEFAULT rule escaped matching all rules criteria for catching fraud and genuine transactions and deserve further investigation to identify fraud trends for refining the rules strategy.
- ✓ DENY transactions should be setup for auto-decline by the solution and should result in subsequent decline for sufficient number of days (7 or 14) to allow for fraud investigation.
- ✓ Depending on how issuers' fraud operations are organized configure the case generation for suitable risk advice to begin instant investigations on suspected fraud transactions.

Thank You.

ca technologies