Categorical fields:

| **Field** | **Why It’s Important** |
| --- | --- |
| **authentication** | Indicates whether the user was verified. For example, M (manual) is often riskier than P (biometric). A lack of authentication (N) in large transactions is a major fraud indicator. |
| **processingChannel** | Reveals how the transaction was routed (ATM, mobile app, API, etc.). Fraudsters often prefer remote channels (A, R) due to lower scrutiny. |
| **merchantCategoryCode** | Certain MCCs (e.g., gift cards, ATMs) are more prone to fraud. Fraud detection models weigh some categories as high-risk. |
| **accessChannel** | Represents the user's interface: e.g., C (Call center), P (POS), U (App). Fraud tends to exploit less monitored channels. |
| **deliveryChannelId** | Indicates delivery/transaction method (gateway, direct debit). Some IDs correlate with specific fraud types (SIM swaps, social scams). |
| **scamFlag** | Pre-labeled flag showing a known scam pattern. Even if it’s not always present, it’s valuable as a reinforcement feature. |
| **typeOfLoss** | Encodes known fraud types (FRAUD\_GEN, SOCIAL, etc.). Helps the model identify patterns that are already tagged as fraud-confirmed. |

These fields **capture real-world fraud signals** across biometric, device, behavioral, and channel dimensions — making them excellent inputs for decision tree learning and rule generation.

[ New JS Rule ] ─┬─▶ [ Run Rule on Past Transactions ]

│

└─▶ [ Collect Matches / Misclassifications ]

│

▼

┌─────────────────────────────┐

│ Evaluate Performance (TP, FP, FN, TN) │

└────────────┬──────────────────────────┘

▼

┌───────────────────────────────────────┐

│ Fine-tune model OR update training set │

└───────────────────────────────────────┘