Fraud Prevention

The rules are based on data sets to apply detection intelligence.

Geolocation

Client

Device

White and Black Lists

Detailed Control: Lists, Footprints, and Learning

Black Lists: Block items associated with fraud or previous chargebacks (cards, emails, IPs).

White Lists: Automatically approve trusted users.

Risk: Excessive use of white lists can transfer risk to the merchant, as a fraudulent transaction with a 'trusted' data point would not be stopped. Getnet recommends expert support and continuous monitoring.

Velocity Rules

Contextual Analysis: Identifying Inconsistencies

Mechanism: Filters anomalous patterns of transaction frequency.

Alert: Multiple low-value purchases or repeated charges in very short intervals.

Value: It is crucial to stop Card Testing (automated testing of stolen cards).

Advanced Rules and Continuous Learning

Fraud Prevention Intelligence: Machine Learning

Mechanism: Modern systems combine manual rules with self-learning models (Machine Learning).

The System Learns: Analyzes transactions already flagged as fraud to identify new patterns that escape manual rules (recently created emails, repeated addresses, vertical behaviours).

Chargeback Guarantees: Some advanced tools offer guarantees, but only if the merchant provides complete data.

Re-training

Contextual Analysis: Identifying Inconsistencies

The re-training of fraud prevention rules is carried out under an agile and continuous approach, with one-day self-service re-training sessions that allow for quick and autonomous model updates. Additionally, ad-hoc training can be configured with supervision, adjusting frequency according to fraud behaviour or business needs. The main benefit of this process is to reduce false positives and negatives, optimizing the real detection of risk and increasing the approval rate of valid transactions.