CloudWalk Technical Case – Understanding the Industry

Data Analyst - Risk Analyst I

Daniel Sousa

1. Money Flow, Information Flow, and Roles of Main Players

The payment ecosystem is a network of financial institutions and services that work together to move funds and data securely from a customer to a merchant.

- **Money Flow**
    1. **Customer → Issuer**: The customer's bank ("issuer") fronts the transaction amount when a purchase is made.
    2. **Issuer → Card Network**: The issuer debits the customer's account and sends funds to the card network (e.g., Visa, Mastercard).
    3. **Card Network → Acquirer**: The network routes the funds (net of interchange fees) to the acquiring bank.
    4. **Acquirer → Merchant**: The acquirer deposits the settlement (after its own fees) into the merchant's account. (Stripe, 2025)
- **Information Flow**
    1. **Authorization**: At purchase, transaction data (card number, amount, merchant ID) travels from merchant → gateway → processor → network → issuer.
    2. **Response**: The issuer approves/declines and returns the decision back through the same path.
    3. **Capture & Settlement**: Once approved, the merchant "captures" funds, then at batch close the acquirer and issuer reconcile and settle transactions on a scheduled cycle. (Kalem, 2025)
- **Roles**
    - **Issuer**: Bank that issues card, holds customer accounts, authorizes transactions.
    - **Card Network**: Runs the payment rails, sets standards, and routes authorizations and settlements.
    - **Acquirer**: Bank or financial institution that supports the merchant's account, receives funds from networks, and pays out merchants. (Kagan, 2024)
    - **Payment Processor**: Manages technical messaging between gateways, networks, issuers, and acquirers.
    - **Gateway**: Securely transmits transaction data from the merchant's point-of-sale or website to the processor.

---

2. Differences Between Acquirer, Sub-acquirer, and Payment Gateway

Feature	Acquirer	Sub-acquirer (PSP/Payfac)	Payment Gateway
Definition	Bank or FI contracting directly with merchants to process and settle card payments. (Kagan, 2024)	A service provider that aggregates multiple merchants under a single primary merchant account, then routes transactions to an acquirer. (Stripe, 2025)	Technology service that encrypts and routes transaction data between merchant and processor. (Stripe, 2023)
Risk & Liability	Holds financial risk for chargebacks and non-payment.	Shares or sub-delegates risk from the acquirer; often offers simplified onboarding at higher PSP fees.	No financial risk—focuses solely on data transport and security.
Contractual Model	One-to-one contract with each merchant.	One master contract covers multiple small merchants.	Service subscription or integration contract.
Flow Changes	Funds: Card Network → Acquirer → Merchant Data: Merchant → Gateway → Processor → Network → Issuer.	Funds: Card Network → Acquirer → PSP → Merchant Data: Merchant → Gateway (often bundled) → PSP → Processor → Network.	Data: Merchant → Gateway → Processor → …; Funds unaffected.

---

3. Chargebacks vs. Cancellations and Their Connection to Fraud

- **Chargeback**
    - A **chargeback** is a forced reversal started by the cardholder disputing a settled transaction with their issuer. The issuer withdraws funds from the merchant's account and returns them to the customer. (Stripe, 2025)
    - **Lifecycle**: Dispute filed → issuer investigates → provisional credit to cardholder → merchant may show evidence → final decision.
- **Cancellation**
    - A **cancellation** is a merchant- or customer-initiated reversal **before** settlement (i.e., before funds move from issuer to acquirer). No formal dispute occurs, and typically no fees or penalties are incurred.
- **Connection to Fraud**
    - **Fraud-driven chargebacks** occur when stolen cards, cloned data, or "friendly fraud" (legitimate customers falsely claiming non-receipt) trigger disputes. (Stripe, 2025)
    - They impose direct monetary loss (sale amount + fixed fees) and indirect costs (higher processing rates, reserve requirements, or termination risk for merchants/acquirers).

---

4. What Is Anti-Fraud and How an Acquirer Uses It

- **Definition**
  An **anti-fraud solution** combines rules-based engines, machine-learning models, behavioral analytics, and global fraud intelligence to assess transaction risk in real time and post-authorization. (Rupp, 2022)
- **Usage by Acquirers**
  1. **Pre-Authorization Screening**: Transactions are scored against block lists (e.g., high-risk IPs, BIN ranges) and custom merchant rules.
  2. **Real-Time Monitoring**: Machine-learning models analyze patterns (velocity, anomalies) as transactions flow; suspicious ones are held for manual review or declined. (Mastercard, 2022)
  3. **Post-Authorization Analysis**: Ongoing screening for chargeback risk triggers alerts for high-risk merchant portfolios, enabling acquirers to intervene (e.g., tightening thresholds, requesting more KYC).
  4. **Chargeback Mitigation**: By flagging at-risk transactions early, acquirers reduce the volume of costly disputes and keep compliance with network monitoring programs (e.g., Visa Acquirer Monitoring Program).