B2B Gift-Card Fraud — a Controls Playbook

Velocity, device, behavioural, and human-in-the-loop controls for bulk gift-card orders — and how to enforce them in the platform rather than in a spreadsheet.

Working draft · 2026 | Best Practices | ogloba.com

EXECUTIVE SUMMARY

B2B and bulk gift-card orders are the highest-leverage fraud surface in most programs: a single order concentrates the value of hundreds of consumer purchases, the product is delivered digitally in seconds, and gift cards are liquid — easy to resell and hard to claw back once redeemed. When a fraudulent bulk order settles on a stolen payment credential, the chargeback lands on the program.

This playbook lays out the layered control stack Ogloba applies to B2B order flows — velocity rules, device fingerprinting, behavioural signals, and human-in-the-loop review — the patterns that have cut B2B gift-card chargebacks at Ogloba clients. It then covers how those controls are enforced at platform level (a rules engine plus ML models screening every transaction in milliseconds, mandatory approval flows, full audit logs) and the operating cadence that keeps them effective.

1. Why B2B orders are a distinct fraud surface

Consumer gift-card fraud is retail-scale; B2B fraud is wholesale-scale. Four properties make bulk orders different:

- **Value concentration.** One approved order can move as much value as a month of consumer sales — so a single missed signal is expensive.
- **Digital delivery speed.** Bulk digital codes fulfil in seconds. Unlike physical shipment fraud, there is no delivery window in which to catch and cancel.
- **Resale liquidity.** Gift cards are quasi-cash on secondary markets. Fraudsters do not need to use the cards — they need only sell them faster than the chargeback arrives.
- **Legitimate lookalikes.** Genuine B2B behaviour — new corporate customers placing large first orders under deadline pressure — is exactly what fraud looks like. Blunt blocking rules kill real revenue, which is why layered, graduated controls matter.

> Design goal: raise the cost and delay for the attacker without adding friction for the repeat corporate buyer whose ordering pattern the platform already knows.

2. The layered control stack

Layer 1 — Velocity rules

Velocity is the cheapest strong signal in bulk fraud. Ceilings on order value and order frequency — per account, per payment credential, and per destination — catch the "many orders, short window" pattern that precedes most bulk fraud events. The platform's promotion machinery already thinks in these terms (frequency limitations per card, day, week, or month; maximum caps), and the same primitives apply to order risk: limits are configuration, not custom code.

Layer 2 — Device fingerprinting

Stolen credentials are cheap; clean devices and clean network histories are not. Device fingerprinting ties orders to the hardware and environment placing them, so an account that suddenly transacts from a new device — or many accounts transacting from one device — surfaces before settlement.

Layer 3 — Behavioural signals

Every B2B account accumulates a normal shape: typical order sizes, denominations, cadence, and delivery destinations. Deviation from that shape is a signal even when each individual order looks plausible. This is where reporting granularity pays off — the platform records activity down to the individual card, terminal, merchant, channel, and timestamp, giving the fraud model and the human reviewer the same evidence trail.

Layer 4 — Human-in-the-loop review

Above a risk threshold, automation should stop and a person should decide. First orders from new corporate accounts, orders that breach velocity ceilings, and orders flagged by the model route to a review queue backed by mandatory approval flows — the same separation-of-duties machinery that governs any operation touching balances or settlements. The reviewer approves, declines, or requests verification; every decision lands in the audit log.

3. Enforcing the stack at platform level

Controls that live in a spreadsheet or a weekly export are advisory. On Ogloba they are properties of the transaction pipeline:

Millisecond
Per-transaction screening — a rules engine plus ML models block suspicious patterns before they settle and learn new fraud vectors automatically

Every transaction
Sanctions screening, velocity limits, and fraud rules applied on each transaction, tuned to the corridors and amounts in the program

Full audit logs
Mandatory approval flows and granular role-based permissions on every balance- or settlement-touching operation

Modular
A fraud module can be switched on as program risk grows — without re-platforming

- **Screening before settlement.** Real-time fraud checks and PCI-grade validation run at activation — cards go live the moment they are sold, but only after the checks pass.

- **Rules plus models.** The rules engine encodes the controls you can articulate (velocity ceilings, corridor limits); the ML models catch the patterns you cannot, and learn from new fraud vectors automatically.
- **Separation of duties by construction.** Granular permissions assign each user a role down to specific tasks, so no single operator can both raise and approve a high-risk order.
- **One evidence trail.** The Transaction Data Warehouse gives fraud, finance, and support the same single source of truth for investigating any incident or reconciling any settlement.

4. The operating cadence

Fraud controls decay: attackers adapt, promotions change order patterns, and thresholds tuned for last quarter mis-fire this quarter. Programs that stay ahead treat fraud as an operating discipline with a fixed cadence, owned by a named program owner:

RITUAL	PURPOSE	CADENCE
Issuance / redemption review	Spot anomalies in volume, denominations, and channel mix while they are days old, not months	Weekly
Fraud review	Re-tune velocity ceilings and review-queue thresholds against measured chargeback and decline outcomes	Monthly
Continuous monitoring	24/7 monitoring and fraud analytics on platform infrastructure, with AI-powered anomaly detection in production	Always on
Support loop	24/7/365 hotline able to query card status and block, replace, refund, or reload cards — with every action audit-logged	Always on

5. Controls checklist

- Velocity ceilings per account, credential, and destination — enforced in the pipeline, reviewed monthly.
- Device fingerprinting on every B2B order, with device-to-account anomaly flags.
- Behavioural baseline per corporate account; deviation scoring feeding the review queue.
- Human-in-the-loop approval for first orders and threshold breaches, with mandatory approval flows.
- Sanctions screening and fraud rules on every transaction, not sampled subsets.
- Full audit logs and separation of duties across the order-to-settlement path.
- A named program owner and a weekly/monthly review rhythm that actually happens.

Working draft — pending final review. © Ogloba 2026

Pressure-test your B2B order flow

Bring a real order pattern and Ogloba's team will walk through it against the control stack — where velocity, device, behavioural, and human-in-the-loop checks would fire, and what the platform enforces out of the box.

Talk to the Ogloba team → ogloba.com/contact

This working draft consolidates material previously published on ogloba.com — technology, back-office, and transport & money-transfer capability pages, the gift card benefits guide, and the Ogloba blog. All claims are as published there and remain subject to final business review.