



Your source for payments education

The Art of Selective Friction

in Modern Checkout

Devang Gaur · Product Manager, Payments · Google

Sudhee Dwivedi · Team Lead, Implementation Engineering · Adyen

Agenda: Navigating the optimal zone

Strategic roadmap for balancing checkout speed and authorization trust

01

The Telemetry Paradox

Uncovering the hidden revenue leak when "frictionless" leads to issuer distrust.

02

Tracing the Addiction

How UX-first principles evolved into systemic payment risks without proper measurement.

03

The Unseen Leak

Benchmarking false declines and the high cost of losing customer lifetime value.

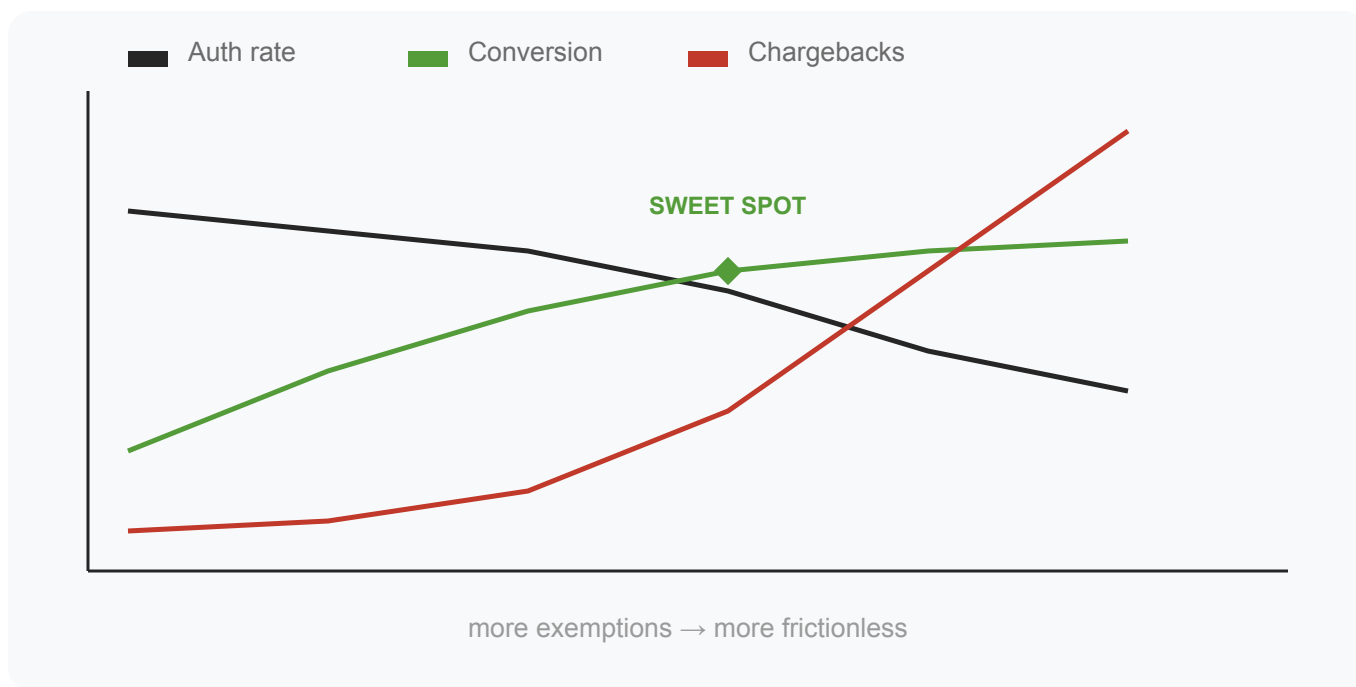
04

The Strategic Dial

A framework for applying TRA and low-value exemptions to protect authorization rates.

The telemetry paradox

Lumen, a subscription-box merchant, did everything right — and revenue still bled out.



Revenue yield peaks

Selective friction is the optimal zone. Going further frictionless hurts yield.

Auth rate quietly drops

Issuers soft-decline as exemptions stack up. No dashboard alert fires.

Chargebacks compound

The frictionless mandate carried a hidden trust cost all along.

Frictionless ≠ optimized. The issuer was never part of the merchant's mental model.

Tracing the frictionless addiction

How a UX principle became a systemic payments risk

01

The UX origin

Amazon One-Click, Apple Pay, and mobile-first thinking trained product teams to treat any added step as a failure.

02

The over-application

Merchants replicated zero-friction logic onto complex, high-risk flows globally — without issuer context.

03

The fallout

Issuer distrust, a spike in soft declines, and rising fraud exposure — none of it visible on the conversion dashboard.

Root cause. Speed was optimized. Trust was never measured. The issuer was never part of the mental model.

The leak you're not measuring

The industry obsesses over abandonment. The expensive leak hides one layer deeper.

70%

Cart abandonment

Everyone watches this dashboard.

1.5–3%

False declines

Of all transactions — yet rarely tracked.

65%

Never come back

Of falsely declined customers, lost for good.

Abandonment is a leak you see.

Over-exemption is a leak you don't.

Two sides of every transaction

Most checkout optimization ignores the entity that actually approves or declines the payment

MERCHANT LENS: Speed & conversion

PRIMARY GOAL

Maximize conversion, minimize abandonment

VIEW OF EXEMPTIONS

Features to maximize at all costs

BLIND SPOT

What the issuer sees on the other side

*trust is
the
currency*

ISSUER LENS: Risk & liability

PRIMARY GOAL

Protect against fraud and liability

VIEW OF EXEMPTIONS

Signals that hide risk and erode trust

BLIND SPOT

Exemptions mean the merchant owns the liability

The cart is not one payment

One “Place Order” click can hide four different authentication and authorization contexts

LUMEN CHECKOUT · ONE CLICK

€184.00 total

 **Wireless headphones**
€129.00 · one-time

 **Annual care plan**
€39.00/yr · subscription

 **Music app (free trial)**
€0.00 today · €9.99/mo

 **Cloud storage add-on**
metered · billed on usage

CIT

Physical good

Customer present. In scope for SCA now — authenticate or apply an exemption.

CIT + MANDATE

Annual subscription

First charge authenticates and sets the recurring mandate. Store the network TID or future bills decay.

MIT

Trial subscription

Nothing captured now. A future merchant-initiated charge fires when the trial converts.

VARIABLE MIT

Usage add-on

Amount unknown at checkout. Variable-amount MITs can fall back into SCA scope.

One click is not one payment. It is four authentication contexts wearing a trench coat.

Each line item has its own friction rule

The same cart resolves to four different SCA, exemption, and liability outcomes

Cart component	SCA scope	Exemption	Liability	What the issuer sees
Physical good	In scope (CIT)	TRA / low-value	Issuer	Fresh authenticated CIT
Annual plan setup	In scope (CIT)	None — authenticate	Issuer	Mandate + stored TID
Trial → recurring	Out of scope (MIT)	MIT / recurring	Merchant	MIT flag + TID lineage
Usage add-on	Can fall back in	Variable MIT	Merchant	Variable amount, weak ID

The trap. Authenticating the cart once may not extend liability protection to the recurring charges it spawns — it depends on network and setup.

Why this demands infrastructure, not rules

A single friction toggle cannot serve Lumen's cart with its four payment lifetimes

ONE FLAT RULE

- ✗ Treats the cart as a single charge
- ✗ One friction decision for every line
- ✗ No memory of credential-on-file state
- ✗ Transaction lineage lost after checkout
- ✗ Re-bills fail silently → involuntary churn

INTENT-AWARE INFRASTRUCTURE

- ✓ Decomposes the cart into payment intents
- ✓ Tags each line with its CIT / MIT status
- ✓ Routes the right exemption per component
- ✓ Persists the network TID across the lifetime
- ✓ Re-evaluates friction at every future bill

Selective friction is not a checkout setting. It is a per-intent decision managed over time.

From signal to decision in 300ms

What the infrastructure actually does in the moment of checkout

01

Ingest

BIN, issuer history, card mix, velocity — the signals issuers weigh.

02

Decide

Set the friction level per payment intent, not per card.

03

Route

Pick the best acquirer; smart-retry on soft declines only.

04

Persist

Store the network TID; carry lineage into the next bill.

THE RETRY IS THE TELL — SOFT DECLINE ≠ HARD DECLINE

SOFT DECLINE

“Try again differently.” Step up to 3DS and recover — **10–25% rescue rate.**

HARD DECLINE

“Stop.” Retrying raises your fraud score. The issuer remembers across all your traffic.

Smart routing lifts auth +2–4% now, 5–10% as it learns. Dumb retries burn issuer trust.

The exemption trap

Each exemption type has a trust cost. Misapplication compounds over time.

TRA

Transaction Risk Analysis

Use: Low-risk, known user flows.

Misuse: Blanket use to force conversion.

TRUST COST

Moderate / high — issuers step up or hard-decline when their risk models disagree.

MIT

Merchant-Initiated Transactions

Use: True subscriptions & recurring billing.

Misuse: Masking unpredictable card-on-file charges.

TRUST COST

High — triggers regulatory scrutiny and cascading soft-decline patterns.

€30

Low-Value Exemption

Use: Micro-transactions; caps at €100 / 5 consecutive.

Misuse: Ignoring velocity; hiding card testing.

TRUST COST

Critical — issuers will block the entire BIN if velocity goes unchecked.

Exemptions are not features to maximize. They are tools that carry an issuer trust cost.

Geographic risk calculus: no global baseline

The same exemption strategy can win in one market and destroy auth rates in another

EU / UK

MANDATED

- PSD2 / SCA strictly enforced by law
- Issuer behavior heavily regulated by baseline rules
- Exemptions must be surgical; consumers expect step-ups

US

VOLUNTARY

- No SCA mandate — frictionless is the baseline
- Issuers rely on proprietary, opaque risk models
- Voluntary 3DS shifts liability but can shock consumers

Japan / India

NEWLY MANDATED

- JCA EMV 3DS mandate in effect since April 2025
- India mandates 3DS on all card-not-present
- Conservative issuer culture — step-ups expected

APAC / LATAM

MIXED

- Brazil: optional for credit, mandatory for debit
- Malaysia: risk-based auth mandate from central bank
- High challenge rates even in frictionless flows

What the data actually shows

Published, anonymized industry data — Adyen, Visa, Mastercard, Stripe

+2.35%

Auth rate delta

Selective friction vs. blanket exemptions

8–10%

Revenue at risk

EU merchants from SCA conversion impact

~5%

Conversion uplift

From smart exemption routing decisions

10–25%

3DS rescue rate

Retrying soft-declined transactions

Network tokenization: the trust bridge

Building issuer confidence without adding consumer friction

KEY METRICS

+3% **Adyen**
auth rate uplift

+4.6% **Visa**
approval increase

+2.1% **Mastercard**
auth rate uplift

-30% **Visa**
fraud reduction

HOW IT WORKS

- 1 Replace PAN with token**
Static card number becomes a dynamic, merchant-specific token. Non-reversible without the network key.
- 2 Cryptogram per transaction**
Every charge generates a one-time cryptogram. Replay attacks become impossible.
- 3 Lifecycle management**
Token auto-updates when the card expires or reissues. Zero involuntary churn for subscriptions.
- 4 Issuer sees higher trust**
Token + cryptogram is a stronger signal than raw PAN + CVV. Fewer false declines.

The AI engine: staying in the sweet spot

Authorization is not an on/off switch. AI keeps you in the optimal zone, permanently.

01

Intelligent authorization signals

Enriches 150+ data fields per transaction — device, behavior, velocity — so issuers authorize confidently.

+2.2% revenue lift; up to +13% auth for enterprise merchants.

02

Network-wide shopper recognition

Recognizes shoppers new to you but proven safe elsewhere, converting unknowns into trusted knowns.

Recognizes 80%+ of “new” shoppers, lifting first-purchase auth.

03

Real-time fraud suppression

Suppresses fraud signals in real time — frictionless need not mean chargeback exposure.

98% chargeback reduction alongside auth gains.

The sweet spot is not a setting. AI holds it by optimizing signals, recognizing trusted shoppers, and suppressing fraud at once.

The friction dial

Not an on/off switch — a continuously tuned, market-specific decision model

GREEN

Exempt

Friction adds no value here.

KEY SIGNALS

- Low transaction value
- Known / returning customer
- Non-mandated market
- Strong historical approval BIN

→ Frictionless flow

AMBER

Selective step-up

Challenge to preserve issuer trust.

KEY SIGNALS

- Mid-value transaction
- Mixed customer history
- Issuer showing soft declines
- Unusual velocity patterns

→ Step-up challenge

RED

Full authentication

Exempting here is actively harmful.

KEY SIGNALS

- High value / new customer
- Heavily mandated market
- Elevated dispute category
- Complex cross-border routing

→ Mandatory 3DS

Key takeaways

Three things to carry back to your checkout strategy

01

Frictionless is not the goal. Trust is.

Optimizing purely for speed hides issuer distrust, soft declines, and fraud exposure that never show up on the conversion dashboard. The right friction protects revenue.

02

Treat exemptions as tools, not trophies.

TRA, MIT, and low value each carry a trust cost. Apply them by transaction context and by market, because the same strategy that wins in the US can sink auth rates under PSD2.

03

Tune the dial with data, not defaults.

Friction is a per intent decision managed over time. Segment traffic, feed issuers transparent signals, and test continuously to balance speed, security, and compliance.

The final word

Frictionless is a **UX goal**.

Selective friction is a **revenue strategy**.

FOR MERCHANTS

Stop treating exemptions as a high score. Calibrate your logic based on business and regional market.

FOR NETWORKS & ACQUIRERS

Protect the trust bridge. Segment traffic to feed issuers the transparent signals they need.

Q&A

Please don't forget to submit your **session evaluation**.

DEVANG GAUR

Product Manager, Payments



SUDHEE DWIVEDI

Team Lead, Implementation Engineering

