PSD2 Implementation Guide for Prepaid Issuers

Strong customer authentication, dynamic linking, and exemption flow patterns — mapped to the architecture prepaid and gift card issuers actually run.

Working draft · 2026 | Compliance | ogloba.com

EXECUTIVE SUMMARY

The EU's second Payment Services Directive (PSD2) reshaped the security baseline for electronic payments in Europe — and prepaid issuers are squarely in scope wherever their instruments function as payment instruments. Closed-loop gift card programs are comparatively light on regulatory burden versus open-loop prepaid, but they are not free: PSD2 in Europe, alongside KYC/AML rules and consumer-protection regimes, still applies and should be planned for up front.

This guide walks through what PSD2 asks of a prepaid issuer — strong customer authentication (SCA) and dynamic linking — the exemption flows worth engineering for, the anonymous-prepaid ceilings that constrain program design, and how each requirement maps onto issuer platform architecture. It closes with an implementation checklist oriented around what reviewers and auditors actually look at. This document is a working draft for business and legal review; it is not legal advice.

1. What PSD2 asks of a prepaid issuer

Scope: when prepaid is a payment instrument

PSD2 applies to payment services and payment instruments in the EU/EEA. Open-loop prepaid cards sit clearly in scope. Closed-loop programs may fall under limited-network exclusions, but that assessment is market-by-market and program-by-program — reloadability, redemption network breadth, and cross-border acceptance all move the analysis. The practical planning posture Ogloba recommends to program owners: treat the PSD2 control set as the design baseline, then relax where counsel confirms an exclusion, rather than the other way round.

Strong customer authentication

SCA requires authenticating the payer using at least two independent factors drawn from knowledge (something the user knows), possession (something the user has), and inherence (something the user is), whenever the payer accesses a payment account online or initiates an electronic payment. For prepaid issuers this touches cardholder portals, balance and history views, top-up and reload journeys, and online redemption.

Dynamic linking

For remote electronic payment transactions, the authentication code must be dynamically linked to the specific amount and the specific payee. Any tampering with either must invalidate the code. Architecturally, this means the authentication service must receive amount and payee at challenge time — a requirement that breaks bolt-on authentication designs where the challenge is issued before the order is final.

2. Exemption flows worth engineering for

PSD2's regulatory technical standards define exemptions that let issuers skip SCA where risk is demonstrably low. Exemptions are where compliance and conversion meet: every exemption correctly applied is checkout friction removed. The categories that matter most to prepaid programs:

- **Low-value transactions** — below thresholds set in the RTS, subject to cumulative value and transaction-count counters since the last SCA.
- **Recurring transactions** — same amount, same payee after an initial SCA; relevant to subscription-style reloads.
- **Trusted beneficiaries** — payees the cardholder has whitelisted under SCA.
- **Transaction risk analysis (TRA)** — exemption tied to the provider's measured fraud rates staying under reference thresholds, which makes fraud-rate monitoring a first-class compliance artefact, not just a loss-prevention metric.

> Engineering implication: exemption counters (cumulative value, consecutive transaction counts) and per-channel fraud-rate telemetry must live in the transaction pipeline itself. If they sit in a reporting silo, the issuer cannot claim the exemption in real time.

3. KYC ceilings and the anonymous-prepaid squeeze

PSD2 does not operate alone: the EU's AML framework caps what anonymous prepaid can do, and the direction of travel has been tightening since the European Commission's February 2016 Action Plan on terrorist financing, whose key theme was better identifying the holders of prepaid cards.

- EU law has permitted prepaid cardholders to reload a maximum of €2,500 over one year without undergoing any KYC, and single-use cards to be loaded with up to €250 anonymously — ceilings a program must enforce in its load and redemption logic, not merely in its terms.
- Enforcement varies sharply by member state and sector. Prepaid card and bank account packages have been sold in France through some 25,000 independent tobacco shops with minimal ID checks, while Saudi Arabia checks even prepaid mobile accounts against the Al Elm national database in real time — a reminder that multi-country programs need per-market KYC configurations, not one global setting.
- Money-transfer flows carry extended KYC duties. Ogloba's platform collects required ID information and communicates with central applications of the largest money transfer companies; in Belgium, chipped resident ID cards can be read directly at the EFTPOS to confirm the sender's identity.

The design takeaway: build KYC escalation into the customer journey. A card that starts anonymous within legal ceilings should be able to step up to identified status — with document capture and verification —

without forcing the customer into a different product.

4. Mapping requirements to issuer architecture

PSD2 compliance is ultimately an architecture property. The reference posture below is how the Ogloba platform is engineered; issuers running their own stack can use it as a comparison baseline. Ogloba designs its platform to support customer compliance with the laws applicable to gift card, prepaid, and loyalty programs in each market — including PSD2 (EU), PCI-DSS where card data is processed, GDPR, the UK Data Protection Act, and local consumer-protection regimes.

Millisecond
Per-transaction fraud screening — a rules engine plus ML models inspect each transaction before it settles

PCI DSS L1
Certified compliant with PCI DSS v4.0.1 at Service Provider Level 1 — the highest tier of payment-card data security

Tier-IV
Data centers with encryption at rest and in transit, and role-based access control

Full audit logs
Every balance- or settlement-touching action recorded; mandatory approval flows enforce separation of duties

- **Real-time screening as the TRA backbone.** Because a rules engine and machine-learning models inspect each transaction in milliseconds — blocking suspicious patterns before they settle and learning from new fraud vectors automatically — fraud rates can be measured and evidenced continuously, which is precisely what exemption claims require.
- **Separation of duties by construction.** Granular permissions assign each back-office user a role down to specific tasks; mandatory approval flows govern any operation that touches balances or settlements; full audit logs record who did what. This is what lets enterprise programs pass internal and regulatory review while still moving fast on day-to-day issuance, reloads, and refunds.
- **A single source of truth for evidence.** The platform processes and stores client data in a dedicated Transaction Data Warehouse (TDW), so reconciliation, incident investigation, and audit evidence all draw on the same records — down to the individual card, terminal, merchant, channel, and timestamp.
- **Multi-market configuration.** KYC thresholds, VAT reporting, and consumer-protection specifics are configured per market on one platform — the pattern proven by European retail groups running multi-country programs from a single back office.

5. Implementation checklist

AREA	WHAT REVIEWERS LOOK FOR	WHERE IT SHOULD LIVE
SCA orchestration	Two-factor challenge on account access, reloads, and online redemption; factor independence documented	Authentication service in front of portal and payment initiation
Dynamic linking	Authentication code bound to final amount and payee; tamper invalidates the code	Challenge issued at order-final stage of the checkout flow

Exemption counters	Cumulative value and transaction-count tracking since last SCA, per instrument	Transaction pipeline (real-time), not batch reporting
Fraud-rate telemetry	Measured fraud rates per channel to support TRA exemption claims	Rules engine + ML screening layer with continuous reporting
KYC ceilings	Anonymous load/reload caps enforced in code; step-up KYC journey available	Load/reload logic with per-market threshold configuration
Audit trail	Who did what on any balance- or settlement-touching operation; approval flows	Back office with RBAC, mandatory approvals, full audit logs
Data protection	Encryption at rest and in transit; PCI-aligned card-data handling; GDPR posture	Hosting and platform layer (Tier-IV, PCI DSS Level 1)

Map PSD2 onto your program

Ogloba's team can walk through your issuance and redemption flows, show where SCA, dynamic linking, and exemption logic sit on the platform, and help you scope a per-market compliance configuration.

Talk to the Ogloba team → ogloba.com/contact

This working draft consolidates material previously published on ogloba.com — capability pages, the gift card benefits guide, the KYC overview, and legal/compliance pages — together with a general description of the PSD2 framework. It is not legal advice; regulatory thresholds are set by the applicable RTS and national implementations. Final content pending business and legal review.