1 . Defence-in-Depth Architecture

Layer	How It Reduces Shared-factor Risk	Key Evidence
Multi-Factor Engine	• Enforcement logic runs in a hardened MFA service; success of **all factors is required** and no factor can be bypassed or replayed	PCI-DSS v4 §8.5.1
Factor Isolation	• “Knowledge” (password) is stored only as Argon2id hashes in an HSM cluster. • “Possession” (WebAuthn/FIDO2 credential or TOTP secret) is stored in a **separate vault** and wrapped by a distinct key hierarchy (KEK ≠ DEK)	Key-management controls
Out-of-Band Challenges	• Password resets must be completed **in-app** with WebAuthn *or* a TOTP proven on the trusted device; an e-mail link alone is never sufficient.	Internal reset policy (maps to PCI-DSS §8.3.3)

Step-Up & Risk Scoring	• Device fingerprint, IP reputation and behavioural signals throttle or block suspicious logins even when the right factors are presented	PSD2-aligned risk engine
Administrative Hardening	• All staff and moderator portals are gated by MFA, with RBAC and immutable audit logs	Compliance Statement §10.2

---

2 . Technical Safeguards & Algorithms

Control	Parameter / Standard	Purpose
Password hashing	Argon2id, 0.5 GB-RAM, ≥ 3 iterations	GPU-hard; prevents offline hash reuse if DB leaked
MFA secrets	Stored only inside FIPS-140-2 HSM; wrapped with 256-bit KEK	Ensures compromise of the application DB ≠ compromise of possession token
Transport	TLS 1.3 with forward secrecy	Stops session hijack / MITM attacks

Data at rest	AES-256-GCM	Uniform crypto baseline across PII & auth data
Factor replay defence	WebAuthn challenge-response (ECDSA P-256) + TOTP time-window ±30 s	Makes recorded OTPs or signatures useless

---

3 . Recovery & Reset Hardening

1. **Identity re-proofing before changes** – any request to change password, e-mail, phone, payout account or 2FA device invokes the same KYC tiering used for high-risk payments; selfie-and-document checks via Stripe Identity / Onfido where needed.

2. **24-hour cooling-off window** – critical credential changes are queued; we send alerts via two independent channels (original e-mail *and* in-app push).

3. **Audit-logged approvals** – support agents can approve resets only through an RBAC-controlled console protected by MFA; every action is immutable-logged for five years.

4. **Lockout & throttling** – ten failed attempts trigger a 30-minute lockout, rate-limited at the WAF and app tiers (PCI-DSS §8.3.4).

---

4 . Additional Operational Controls

- **Password policy** – 12-character minimum, mixed case/number, no last-4 reuse .

- **Session binding** – JWTs include device hash & rotating key ID; replay on another device forces re-authentication.

- **Continuous anomaly detection** – real-time model blocks logins if geovelocity or device-change risk spikes (links to PSD2 TRA exemptions).

- **Security headers & WAF** – OWASP Top-10 protections and per-IP rate limiting stop credential-stuffing cascades .

Bottom line

By storing each factor in **separate cryptographic domains**, enforcing out-of-band step-up challenges, and subjecting resets to the **same (or stronger) verification than production logins**, we break the attack chain where compromise of, say, an e-mail inbox would also yield the second factor. Combined with strong crypto, stringent lockouts and real-time risk analytics, the design keeps the user, the platform and downstream payment flows safe even when one element is breached.