NovaPay – Document 08: Fraud Prevention & Identity Verification

Version: Content-Only | Generated: 20 Oct 2025 | Company: NovaPay (UK)

Purpose
Set the framework for preventing and detecting fraud, protecting customers and NovaPay while aligning fraud controls with AML/CTF requirements.

Identity Verification
Onfido provides document verification and biometrics (liveness, face match). Threshold failures trigger manual review in 24 hours. Single■provider dependency acknowledged; secondary vendor evaluation planned.

Fraud Detection Tools
Sift Science provides device fingerprinting, velocity/behavioral analytics, and anomaly scoring; rules pushed to payment gateway for pre■authorization checks.

Fraud Types Monitored
Account takeover, identity theft, payment fraud/card■not■present, first■party (friendly) fraud, synthetic identities, mule accounts, and merchant collusion.

Alert Volumes and Performance (Q3 2025)
~1,200 fraud alerts/month with ~15% confirmed fraud; chargeback rate 0.8% (industry 0.5–1.0%); average time to containment 6 hours; account recovery initiation within 24 hours of confirmation.

Customer Authentication
2FA (SMS/app) and biometrics for high■risk actions; step■up authentication for device anomalies; session risk scoring integrated with Sift.

Account Recovery
Secure re■verification, device reset, password rotation, and transaction reimbursement decisioning per FCA DISP and Visa/MC rules; Action Fraud (UK) reporting for confirmed external frauds.

Integration with AML
Fraud alerts shared with AML via weekly file drop; however, there is no unified view. Fraud patterns (e.g., mule networks) are not consistently fed to TM scenarios.

Weaknesses
(1) Limited integration—fraud and AML operate in silos; (2) No unified customer risk score across systems; (3) Reliance on a single IDV provider; (4) Limited synthetic identity detection; (5) 40% of fraud alerts require manual review, increasing latency.

Improvements
Data hub to join fraud/AML/KYC profiles (Q3 2026); evaluate secondary IDV (Q2 2026); dedicated synthetic ID module (Q1 2026); automated alert exchange with TM (Q2 2026).

KPIs
Containment within 8 hours (actual 6h); recovery initiated <24h (actual 21h); manual review ≤30% (actual 40%); confirmed fraud rate 10–20% (actual 15%).

Governance
Monthly Fraud Risk Committee; quarterly Board reporting; incident post■mortems for losses >£25k; collaboration with card schemes and law enforcement.

Conclusion

Fraud tooling is strong, but integration with AML and multi■vendor resilience need improvement to reduce manual load and enhance detection of synthetic identities.