Merchant and Payment Service Provider (PSP) VAMP compliance checklist

1. Baseline and monitoring setup

- [ ] Pull monthly CNP transaction, fraud, and non-fraud dispute data
- [ ] Build a dashboard showing daily and 30-day rolling VAMP ratio vs. thresholds (30bps, 50bps)
- [ ] Calculate your enumeration ratio (VAAI-based) if you exceed 300,000 authorizations per month

2. Fraud prevention controls

- [ ] Enforce 3DS v2 for all CNP payments; optimize for a frictionless pass rate above 80%
- [ ] Deploy device fingerprinting, IP geolocation checks, and velocity limits (e.g., 5 authorizations per minute/200 authorizations per hour)
- [ ] Layer CAPTCHA or step-up challenges after 2–3 failed attempts

3. Dispute and chargeback automation

- [ ] Automate evidence collection: order history, shipping proof, and customer communications
- [ ] Define SLAs to respond to representment requests within 5 business days
- [ ] Track dispute reason codes and win rates in a centralized case management tool

4. Bot and enumeration mitigation

- [ ] Monitor authorization success/failure patterns to spot credential testing spikes
- [ ] Implement rate-limiting on authorization endpoints and throttle suspicious IP ranges
- [ ] Leverage machine learning to flag abnormal credential flows

5. Standard operating procedures (SOPs), training, and governance

- [ ] Document VAMP definitions, thresholds, alerts, and remediation steps in your SOP manual
- [ ] Train fraud, customer service, and dev teams on new workflows and metrics
- [ ] Schedule monthly “VAMP health” reviews with internal stakeholders and your acquirer

6. Acquirer collaboration

- [ ] Share your VAMP dashboard snapshot and a brief “scorecard” deck each month
- [ ] Agree on escalation paths (email, calls, or joint workshops) before any threshold is breached
- [ ] Solicit feedback on your dispute-handling playbooks and iterate continuously