PAYMENTS · DATA · AI · COMPLIANCE

Card Payments (Debit, Credit and Prepaid) Delivery and Support Runbook

Issuing and acquiring, from requirements to live L1, L2 and L3 support: authorization, clearing, settlement, disputes, PCI DSS, network certification, live pilot, fraud controls, alerts, disaster recovery and audit.

SP Sankar · Payment Product Consultant

sp@paymentconsultant.top · paymentconsultant.top · linkedin.com/in/spsankar

Version 2026 · Always confirm current rules with the card networks, the PCI Security Standards Council and your processor.

Contents

1. Purpose and how to use this runbook
2. Planning vs delivery alignment
3. Card basics for the team
4. Rules and regulations
5. The nine kinds of work, step by step
6. Exit criteria and sign-off: E2E and UAT
7. Proving it in production
8. Controls that run across every card payment
9. Security, certificates and certification
10. Production support: L1, L2 and L3
11. Operational runbooks for common card incidents
12. Disaster recovery
13. Internal and external audit
14. Measures to watch
15. Go-live checklist
16. Sources

Purpose and how to use this runbook

This runbook takes a card change from idea to live production and support. It covers both sides of a card payment:

- **Issuing:** the bank or fintech that gives the card to the customer (debit, credit or prepaid), approves purchases and handles disputes.
- **Acquiring:** the bank or processor that lets a merchant accept cards, sends purchases to the networks and pays the merchant.

It is written for product managers, delivery leads, engineers, testers, operations, fraud and compliance teams.

Cards differ from bank transfers in three ways: **a purchase is approved in about a second but settled later**, the **card networks set many of the rules** (and change them twice a year), and **card data must be protected under PCI DSS** at every step.

Golden rules for Agile card delivery

- Work in sprints, but never skip the hard gates: network certification, PCI DSS sign-off, E2E and UAT exit criteria, and a live pilot with real cards.
- Plan around the networks' release cycles; mandates have fixed effective dates you can't move.
- Never let raw card numbers into logs, test data or analytics. Use tokens.
- Treat authorization speed and uptime as features: a slow or failed authorization is a lost sale or a declined customer.
- Test the money after the approval: clearing, settlement, fees, chargebacks and reconciliation.

Planning vs delivery alignment

Card projects have more outside fixed dates than most: Visa and Mastercard release mandates (usually twice a year), processor releases, network certification slots, PCI DSS assessment dates, and the retail peak season, when most banks and merchants freeze changes (often from mid-November to early January).

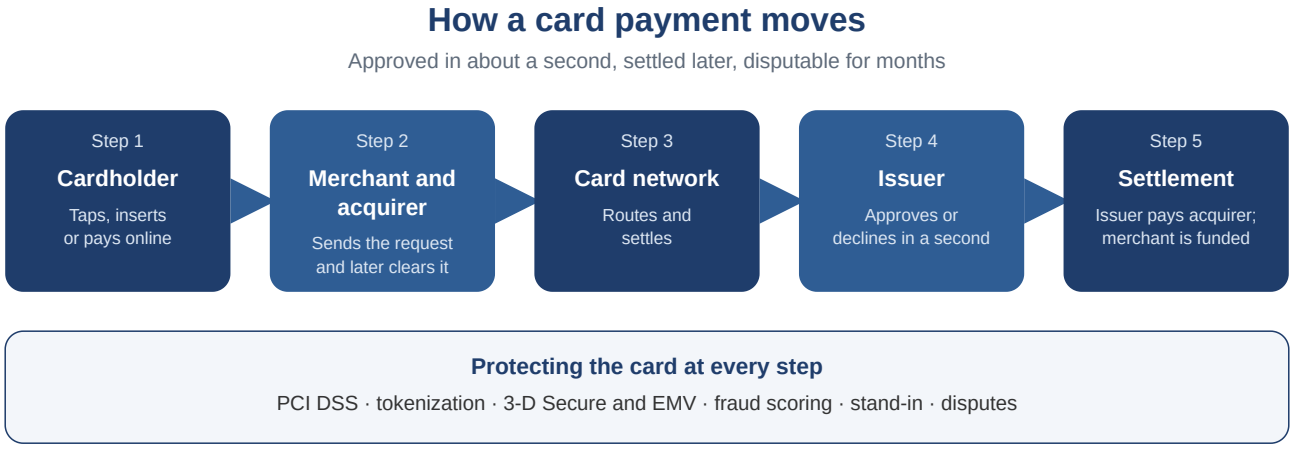
Level	What it holds	Who owns it	Reviewed
Product roadmap	Card products, network mandate dates, PCI assessment, peak-season freeze	Product manager	Quarterly
Release or PI plan	Features committed, certification slots, processor dependencies	Product manager, delivery lead	Every planning increment

Level	What it holds	Who owns it	Reviewed
Sprint plan	User stories for 2 weeks	Product owner and team	Every sprint
Release calendar	Deployment dates, peak freeze, processor release windows	Release manager	Weekly

- **Mandates first:** list every network mandate that applies in the next 12 months and plan backwards from its effective date.
- **Plan to real capacity** with 15 to 20% buffer for production support and disputes work.
- **Track outside dependencies:** networks, processor, card manufacturer, token service, fraud vendor.
- **Measure it:** say/do ratio, feature predictability, scope change and milestone status, reported weekly.

Card basics for the team

Cards are the most used way to pay in the US by number. The Federal Reserve Payments Study found that in 2024 there were 120.6 billion debit card payments and 67.1 billion credit card payments. Cards made up 79% of all noncash payments by number but only about 8% by value. Credit card payments grew faster than debit for the first time in a three-year period since 2000 (Federal Reserve, July 2026).



How a card payment moves

> **How to read this picture:** Read left to right: Steps 1 to 4 are the authorization, which takes about a second. Step 5, settlement, happens later, usually in 1 to 2 days. The band at the bottom lists the protections that apply at every step, from the tap at the till to a dispute months later.

Who is involved

Party	Role
Cardholder	The customer who pays with the card
Merchant	The business that accepts the card
Acquirer and processor	Connects the merchant to the networks and pays the merchant
Card network	Visa, Mastercard, American Express, Discover, plus debit networks; routes and sets rules
Issuer and issuer processor	Approves or declines, bills or debits the cardholder, handles disputes
Program manager (prepaid and fintech)	Runs the card program for a fintech with a sponsor bank issuer

The life of a card payment

Step	What happens	When
Authorization	Merchant asks the issuer through the network: approve or decline	About a second
Clearing	Merchant's acquirer sends the final purchase details	Usually the same or next day
Settlement	Money moves from issuer to acquirer through the network, less fees	Usually 1 to 2 days
Funding	Acquirer pays the merchant	Per merchant agreement
Dispute (chargeback)	Cardholder disputes a charge; issuer can charge it back to the acquirer	Weeks to months, under network rules

Debit, credit and prepaid

Type	Money comes from	Main consumer rule
Debit	The customer's bank account	Regulation E
Credit	A credit line the customer repays later	Regulation Z (Truth in Lending)

Type	Money comes from	Main consumer rule
Prepaid	Money loaded onto the card in advance	Regulation E, including the Prepaid Rule

Rules and regulations

Rule	What it means for delivery
Card network rules (Visa, Mastercard and others)	Authorization, clearing, disputes, fees, branding and security; updated in regular releases
PCI DSS v4.0.1	Protect card data everywhere it is stored, processed or sent; future-dated requirements became mandatory on March 31, 2025
PCI PIN and PCI 3DS	Security of PINs and of 3-D Secure online checks
Regulation E	Debit and prepaid: error resolution, liability limits, disclosures
Regulation Z	Credit: billing error disputes, disclosures, fee limits
Regulation II (Durbin)	Debit: interchange limits for large issuers and the rule that debit cards must support at least two unaffiliated networks, including for online payments
BSA/AML and OFAC	Customer checks, monitoring and sanctions screening
State money transmission and privacy laws	Especially for fintech and prepaid programs

The nine kinds of work, step by step

These are not waterfall phases. In sprints they overlap; the gates are what matter.

Phase 1: Requirements

- Product: debit, credit or prepaid; consumer or business; physical, virtual or both; digital wallets.
- Authorization rules: limits, merchant category blocks, country blocks, stand-in rules if the issuer system is down.
- Fraud and authentication: 3-D Secure for online, card-present EMV, tokenization for wallets.
- Disputes and chargebacks process, fees, statements and notifications.
- Network mandates in scope with their dates.

Exit: requirements signed by product, operations, fraud, disputes, compliance and the processor.

Phase 2: Design

- Message flows: ISO 8583 (most card authorizations today) and network-specific formats; clearing files and settlement reports.
- Response time budget for authorization; stand-in processing when your system is unavailable.
- Card data: where card numbers live, tokenization, encryption keys and HSMs; keep the PCI scope as small as possible.
- Reconciliation design: authorizations to clearing to settlement to the general ledger.

Exit: architecture, security and PCI scope reviews passed.

Phase 3: Development

- Build to the processor's and networks' specifications.
- No real card numbers in code, logs or lower environments; use test cards and tokens.
- Code review, static analysis and dependency scanning on every change.

Phase 4: Unit testing

- Authorization rules, limits, response codes, fee and interest calculations, statement logic.
- Message building and parsing for every message type.

Phase 5: Performance testing

- Peak authorizations per second (Black Friday, holiday season, payday).
- Response time with fraud scoring on; behaviour under processor or network slowdowns.

Exit: peak load at 2 times expected volume inside the response time budget.

Phase 6: End-to-end (E2E) testing

- Authorizations, reversals, refunds, partial approvals, incremental authorizations, offline and stand-in.
- Clearing, settlement, fees and reconciliation to the ledger.
- Disputes and chargebacks through to resolution.
- 3-D Secure, tokenized wallet payments, EMV chip and contactless.
- Network certification test scripts with the processor and networks.

Phase 7: User acceptance testing (UAT)

- Operations, disputes and customer service run real cases.
- Customer journeys: card activation, PIN set, wallet provisioning, card lock, disputes in the app.

Phase 8: Release management

- Change approval, release notes, rollback plan; respect the peak-season freeze.
- Coordinate with the processor's release calendar and network mandate dates.

Phase 9: Deployment

- Deploy, smoke test, then a live pilot with real cards (see "Proving it in production").
- Hypercare for the first weeks; watch approval rates and declines closely.

Exit criteria and sign-off: E2E and UAT

E2E exit criteria

- [ ] Network and processor certification scripts passed and signed off
- [ ] 100% of planned test cases run; at least 95% passed; no open Severity 1 or 2 defects
- [ ] Authorization response times inside budget at peak load
- [ ] Clearing, settlement and reconciliation balanced end to end
- [ ] Disputes and chargebacks tested end to end
- [ ] No real card numbers found in logs or test environments (scan evidence)

UAT exit criteria

- [ ] Business scenarios signed by the business owner
- [ ] Disputes, fraud and service procedures tested by the people who use them
- [ ] Customer journeys, notifications and statements checked

Sign-off matrix

Who signs	What they confirm
Product owner	Features meet acceptance criteria
QA lead	Exit criteria met, evidence stored
Operations and disputes heads	Teams trained, procedures ready
Fraud	Rules and models tuned and live
Compliance	Reg E, Reg Z, Reg II and AML requirements met
Information security / PCI	PCI DSS controls in place for the new scope
Change manager	Release approved

Proving it in production

1. Issue a small number of real cards to employees (a "friends and family" pilot).
2. Make real purchases: card present (chip and contactless), online with 3-D Secure, and in a digital wallet.
3. Make a refund, a reversal and an ATM withdrawal if in scope.
4. Raise and resolve a test dispute.
5. Check clearing, settlement, fees, statements and the general ledger for every pilot transaction.
6. For acquiring: process real low-value sales and refunds at a pilot merchant and confirm merchant funding.
7. Watch approval and decline rates daily before widening the rollout.

Exit: all pilot transactions settled and reconciled; sign-off by product, operations, fraud and compliance.

Controls that run across every card payment

Control	What good looks like
PCI DSS	Card data protected, scope kept small, assessment passed every year
Tokenization and encryption	Card numbers replaced by tokens; keys in HSMs with dual control
Real-time fraud scoring	Every authorization scored; rules and models tuned weekly
3-D Secure and EMV	Strong checks for online and in-store payments
Limits and controls	Spend, cash and country limits; customer card lock in the app
Stand-in processing	Safe approvals when the issuer system is unavailable, with limits
Dispute handling	Disputes worked within network and Reg E or Reg Z time limits
Reconciliation	Authorizations, clearing, settlement and ledger balanced every day

Security, certificates and certification

- **Access:** least privilege, quarterly reviews, PAM for privileged access, NIST SP 800-63B for passwords and multi-factor authentication. Access to card data only for named roles with a business need.
- **Keys and HSMs:** key ceremonies with dual control and split knowledge; track key and certificate expiry; alert 60, 30 and 7 days before.
- **Network and processor certification:** required for new products, new channels and after major changes; keep the signed results.

- **PCI DSS assessment:** a yearly assessment (or self-assessment for smaller entities) plus quarterly scans; update the scope before each release.
- **Vendors, licences and open source:** track versions, support dates and licences; scan dependencies on every build; review processor SOC reports and PCI attestations yearly.

Production support: L1, L2 and L3

Level	Who	What they do	Target
L1	Card operations, service desk and fraud desk (24/7)	Monitor approvals, handle customer calls, card blocks, first triage	Acknowledge within 15 minutes
L2	Application and processor support	Diagnose declines, failed files, stand-in issues; manage incidents	Respond within 30 minutes
L3	Engineering, processor and network	Code fixes, hotfixes, root cause	Engaged within 1 hour for Sev 1

Severity levels

Severity	Example	Response
Sev 1	Authorizations failing, approval rate drops sharply, processor down	Bridge within 15 minutes, any time of day
Sev 2	One channel or BIN range affected, clearing file late	Within 30 minutes
Sev 3	Single card or transaction issue	Next business day

Alerts and notifications

- Real-time alerts to Slack or Teams and paging for: approval rate below normal, decline codes rising, response time above budget, stand-in active, clearing or settlement file missing, key or certificate expiry.
- Email updates to stakeholders for Sev 1 and Sev 2 every 30 minutes.
- Customer messages in the app for wide outages.

Escalation: L1 to L2 at 15 minutes; L2 to L3, the processor and the incident manager at 30 minutes; senior leaders for any Sev 1.

Hotfixes: emergency change with a named approver, peer review, test in a lower environment, PCI impact check, and a review within 5 business days.

Operational runbooks for common card incidents

1. Approval rate drops suddenly

1. Check decline codes: is it one network, one BIN range, one merchant type or all?
2. Check the processor and network status pages and your fraud rules (a new rule can block good customers).
3. Roll back the last change if it lines up with the drop.
4. Tell customer service what to say.

2. Issuer system down

1. Confirm stand-in processing is active with the processor and the limits are right.
2. Fix and fail back; then reconcile stand-in approvals against balances.

3. Clearing or settlement file missing or wrong

1. Contact the processor; do not post partial files twice.
2. Reconcile once the file arrives; correct the ledger.

4. Suspected card data breach

1. Follow the incident response plan; involve security, legal and the networks as their rules require.
2. Contain, preserve evidence and decide on card reissue with fraud and the networks.

5. Surge in fraud on a BIN range

1. Tighten rules for the affected range; block and reissue cards if needed.
2. Report to the networks as required; watch disputes over the next weeks.

Disaster recovery

Item	Example target
Recovery time objective (RTO)	Minutes for authorization (with stand-in covering the gap); hours for batch jobs

Item	Example target
Recovery point objective (RPO)	Zero for authorizations and balances

- [ ] Backup site connected to the processor and networks and tested
- [ ] Stand-in limits agreed and tested with the processor
- [ ] HSMs and keys available at the backup site
- [ ] DR test at least once a year, with evidence
- [ ] After failover, reconcile authorizations, balances and stand-in activity

Internal and external audit

Internal audit checklist

- [ ] Card policies and procedures current and approved
- [ ] PCI DSS assessment current; scope matches reality
- [ ] Authorization rules, limits and stand-in settings reviewed and approved
- [ ] Fraud rules changes approved and tested before release
- [ ] Disputes worked within network and Reg E or Reg Z timeframes (sample cases)
- [ ] Key management ceremonies documented with dual control
- [ ] Access to card data reviewed quarterly; no direct database changes without approved tickets
- [ ] Daily reconciliation balanced; breaks closed
- [ ] DR test in the last 12 months

External audit and exam checklist

- [ ] Evidence index linking each control to its evidence
- [ ] PCI Report on Compliance or self-assessment and attestation
- [ ] Transaction and dispute population lists ready to sample
- [ ] Change records with approvals, certification and pilot evidence
- [ ] Access lists and review sign-offs
- [ ] Incident records and root cause reviews
- [ ] Processor and vendor SOC reports and PCI attestations
- [ ] Open findings tracker with owners and dates

Measures to watch

Measure	Why it matters
Approval rate	The single best sign that cards work for customers
Authorization response time	Slow responses become declines at the till
Fraud loss rate	Losses as a share of spend
Dispute and chargeback rate	Customer harm and cost; networks watch this too
Stand-in usage	How often your system was not available
Reconciliation breaks	Must be zero at end of day

Go-live checklist

- [ ] Network and processor certification complete
- [ ] PCI DSS controls in place for the new scope
- [ ] E2E and UAT exit criteria met and signed
- [ ] Live pilot transactions settled and reconciled
- [ ] Fraud scoring, 3-D Secure and limits live
- [ ] Stand-in tested
- [ ] 24/7 alerts, on-call and escalation tested
- [ ] DR path tested
- [ ] Disputes and service teams trained

Sources

- Federal Reserve: 2025 Federal Reserve Payments Study, initial findings (July 2026)
- PCI Security Standards Council: PCI DSS v4.0.1
- Regulation E (including the Prepaid Rule), Regulation Z, Regulation II
- Visa and Mastercard published rules (check the current editions)