PAYMENTS · DATA · AI · COMPLIANCE

Zelle (Person-to-Person) Payments Delivery and Support Runbook

For banks and credit unions, from requirements to live L1, L2 and L3 support: enrolment and tokens, network certification, scam and fraud controls, live pilot, 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 Early Warning Services, your processor and your own bank policies.

Contents

1. Purpose and how to use this runbook
2. Planning vs delivery alignment
3. Zelle 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 payment
9. Security, certificates and certification
10. Production support: L1, L2 and L3
11. Operational runbooks for common 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 Zelle change, for example joining the Zelle network, adding Zelle for small business, request-to-pay, or new fraud controls, from idea to live production and support. It is written for product managers, delivery leads, engineers, testers, operations, fraud and compliance teams at a bank or credit union.

Zelle is a bank-owned person-to-person network that lives inside the bank's own app. Three things shape every Zelle project:

- **Speed.** Money between enrolled users usually arrives in minutes, and once sent it can't be pulled back.
- **Identity by email or phone.** Customers send to a token (a US mobile number or email address), not an account number, so enrolment and token checks are critical.
- **Scams.** Most losses come from customers being tricked into sending money themselves. Fraud prevention and customer warnings are as important as the payment flow.

Golden rules for Agile Zelle delivery

- Work in sprints, but never skip the hard gates: Zelle network certification, E2E and UAT exit criteria, fraud sign-off and a live pilot.
- Build fraud controls and warnings into the first release, not later.
- Test enrolment, token changes and limits as hard as the payment itself.
- Support must cover evenings and weekends, because customers send money then.

Planning vs delivery alignment

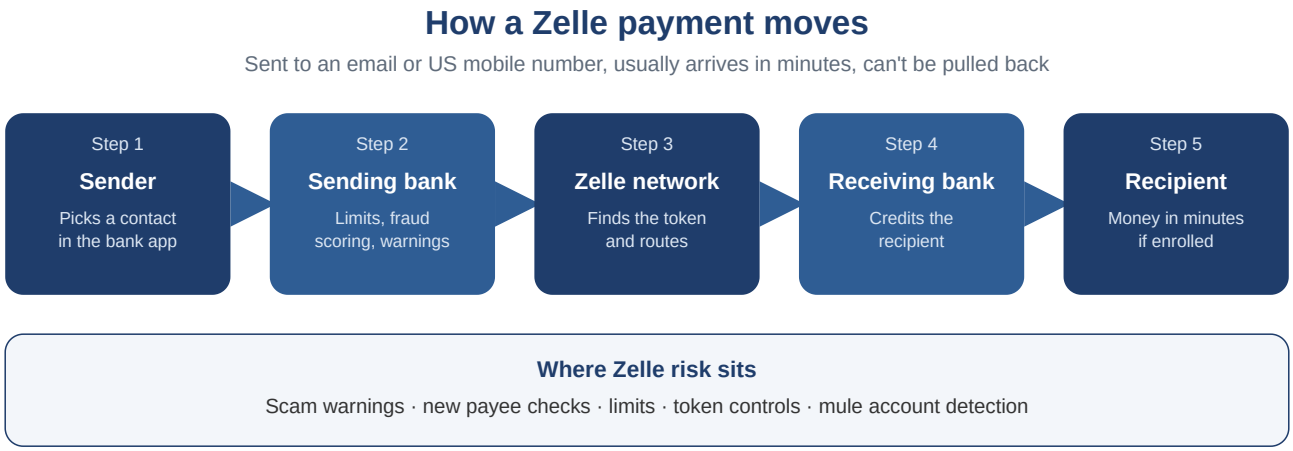
Level	What it holds	Who owns it	Reviewed
Product roadmap	Consumer, small business, request-to-pay, Zelle network release dates	Product manager	Quarterly
Release or PI plan	Features committed, certification slots, processor dependencies	Product manager, delivery lead	Every planning increment
Sprint plan	User stories for 2 weeks	Product owner and team	Every sprint
Release calendar	Deployment dates, freezes, network test windows	Release manager	Weekly

- **Track outside dependencies:** Early Warning Services (the network operator), your core or digital banking processor, and fraud vendors.

- **Plan to real capacity** with 15 to 20% buffer for fraud claims and support work.
- **Measure it:** say/do ratio, feature predictability, scope change and milestone status, reported weekly.

Zelle basics for the team

Zelle is owned and operated by Early Warning Services, a company owned by large US banks. In 2025 customers sent more than $1.2 trillion through Zelle, up 20% on 2024, in 4.2 billion transactions, through a network of more than 2,300 banks and credit unions. Nearly 30% of the dollars went to or from small businesses (Zelle press release, 2026). The standalone Zelle app closed in April 2025, so customers now use Zelle inside their bank's app.



How a Zelle payment moves

> **How to read this picture:** Read left to right: each box is one step of a Zelle payment, from the sender's banking app to the recipient. The band at the bottom lists the controls that matter most, because most losses come from customers being tricked into sending money, and the payment can't be pulled back once sent.

Who is involved

Party	Role
Sender	Customer who sends money using a recipient's email or US mobile number
Sending bank	Checks the customer, limits and fraud, then sends the payment
Zelle network (Early Warning Services)	Looks up the token, routes the payment and runs the network rules
Receiving bank	Credits the recipient's account

Party	Role
Recipient	Gets the money, usually in minutes if enrolled
Processor (optional)	Many banks join through a processor's Zelle service

Key facts for delivery

Topic	What to know
Enrolment	Each customer links an email or US mobile number (token) to an account
Not enrolled recipient	The recipient gets a notice and must enrol to receive; until then the payment waits
Finality	Once sent to an enrolled recipient, the payment can't be cancelled
Limits	Set by each bank, often by customer type and account age
Settlement between banks	Handled under the Zelle network rules after the customer is credited

Rules and regulations

Rule	What it means for delivery
Zelle network rules	Participation, timing, disputes, fraud reporting and branding
Regulation E	Error resolution and unauthorized transfers for consumer accounts; scams where the customer sends the money themselves are a growing area of debate and network policy
UDAAP	Clear, fair messages about what Zelle is, its risks and its finality
BSA/AML and OFAC	Customer checks, monitoring, mule account detection and SARs
Privacy (GLBA)	Protect customer data, including tokens and contact details

Regulators and state attorneys general continue to focus on Zelle scams: for example, the New York Attorney General sued Early Warning Services in August 2025. Plan for strong scam controls and clear records.

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

- Features: send, receive, request, split, small business, enrolment, token change.
- Limits by customer type, account age and channel.
- Fraud: new payee checks, first-payment friction, scam warnings, mule detection on receive.
- Customer messages: who you are paying, "only pay people you know and trust", final payment warnings.

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

Phase 2: Design

- Integration with the Zelle network directly or through a processor.
- Real-time posting and balances in core banking.
- Token management: add, change, remove, and checks when a token moves to a new account.
- Fraud scoring before sending; holds and step-up checks for risky payments.

Exit: architecture, security and fraud design reviews passed.

Phase 3 to 5: Development, unit and performance testing

- Build to the network's specifications; no customer data in logs.
- Unit tests for limits, token rules, fraud triggers and messages.
- Performance tests for peak evenings, weekends, rent days and holidays.

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

- Send and receive with enrolled and not-enrolled recipients, request-to-pay, declines, holds and limit breaches.
- Fraud and scam scenarios, claims and network fraud reporting.
- Posting, notifications and reconciliation.

Phase 7: User acceptance testing (UAT)

- Service and fraud teams run real cases: scam claim, wrong recipient, token takeover, disputes.
- Customer journeys in the app, including warnings and enrolment.

Phase 8 and 9: Release and deployment

- Change approval, rollback plan; avoid peak evenings and the first of the month.
- Deploy, smoke test, then a live pilot (see "Proving it in production"); hypercare including weekends.

Exit criteria and sign-off: E2E and UAT

E2E exit criteria

- [ ] Zelle network certification passed
- [ ] 100% of planned test cases run; at least 95% passed; no open Severity 1 or 2 defects
- [ ] Fraud and scam scenarios behave as designed
- [ ] Enrolment and token change rules proven
- [ ] Posting and reconciliation balanced

UAT exit criteria

- [ ] Business scenarios signed by the business owner
- [ ] Fraud claim and service procedures tested by the people who use them
- [ ] Customer warnings and messages checked

Sign-off matrix

Who signs	What they confirm
Product owner	Features meet acceptance criteria
QA lead	Exit criteria met, evidence stored
Operations and service heads	Teams trained, evening and weekend cover in place
Fraud	Scoring, warnings and mule detection live
Compliance	Reg E, UDAAP and AML requirements met
Change manager	Release approved

Proving it in production

1. Employees enrol with their own tokens and send small payments to each other and to customers of other banks.
2. Receive from another bank; confirm posting and notifications in minutes.
3. Send to a not-yet-enrolled recipient and follow the enrolment journey.

4. Trigger a fraud warning and a limit decline on purpose.
5. Raise and resolve a test claim.
6. Reconcile all pilot payments.

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

Controls that run across every payment

Control	What good looks like
Fraud scoring	Every outgoing payment scored; risky payments held or need extra checks
Scam warnings	Clear warnings at the moment of sending, especially for first payments
Limits	Daily and monthly, lower for new accounts and new payees
Token controls	Checks when a token is added or moved; alerts to the customer
Mule detection	Watch incoming payments for accounts used to collect and move scam money
Claims handling	Reg E timelines met; network reporting done
Reconciliation	Daily, with breaks investigated

Security, certificates and certification

- **Access:** least privilege, quarterly reviews, PAM, NIST SP 800-63B and strong customer authentication in the app.
- **Connections:** track certificates and keys for the network or processor connection; alert 60, 30 and 7 days before expiry.
- **Certification:** network certification before go-live and after major changes.
- **Vendors, licences and open source:** processor and fraud vendor versions, SOC reports, dependency scanning on every build.

Production support: L1, L2 and L3

Level	Who	What they do	Target
L1	Contact centre and fraud desk, including evenings and weekends	Customer calls, scam claims, holds, first triage	Acknowledge within 15 minutes

Level	Who	What they do	Target
L2	Digital and payments application support	Diagnose failures, posting and token issues	Respond within 30 minutes
L3	Engineering, processor and network	Code fixes, hotfixes, root cause	Engaged within 1 hour for Sev 1

Severity levels: Sev 1 when customers can't send or receive or a fraud attack is under way (bridge within 15 minutes); Sev 2 for slow payments or one feature down (30 minutes); Sev 3 for a single payment (next business day).

Alerts: to Slack or Teams and paging for failures and declines above normal, network connection loss, fraud alerts spiking, posting failures and certificate expiry. Email stakeholders for Sev 1 and Sev 2 every 30 minutes.

Escalation and hotfixes: L1 to L2 at 15 minutes; L2 to L3, processor and network at 30 minutes; senior leaders for any Sev 1. Hotfixes follow the emergency change process with a review within 5 business days.

Operational runbooks for common incidents

1. Customer reports a scam payment

1. Log the claim, report it to the network and contact the receiving bank at once.
2. Follow Reg E and your policy for reimbursement decisions; file a SAR if needed.
3. Check the receiving account for mule patterns and block if confirmed.

2. Payment sent to the wrong person

1. Ask the receiving bank, through the network, to contact the recipient; explain that a return can't be forced.
2. Improve the "confirm the recipient's name" step if this repeats.

3. Token takeover (a fraudster moves a customer's phone number)

1. Freeze the token and contact the customer through a known channel.
2. Review recent payments and recover what you can.

Disaster recovery

Item	Example target
Recovery time objective (RTO)	Under 1 hour

Item	Example target
Recovery point objective (RPO)	Zero for sent and received payments

- [ ] Backup connection to the network or processor tested
- [ ] DR test at least once a year, with evidence
- [ ] After failover, reconcile every payment to avoid duplicates

Internal and external audit

Internal audit checklist

- [ ] Zelle policies, limits and fraud rules current and approved
- [ ] Network agreements and certification on file
- [ ] Scam warnings and step-up checks working (sample payments)
- [ ] Claims handled within Reg E timeframes; network reports filed
- [ ] Mule account monitoring and SARs process working
- [ ] Access reviews quarterly; no direct database changes without approved tickets
- [ ] Daily reconciliation balanced
- [ ] DR test in the last 12 months

External audit and exam checklist

- [ ] Evidence index linking each control to its evidence
- [ ] Payment and claims population lists ready to sample
- [ ] Change records with approvals, certification and pilot evidence
- [ ] Complaint and claim trends with actions taken
- [ ] BSA/AML policies, training and independent testing
- [ ] Processor and vendor SOC reports
- [ ] Open findings tracker with owners and dates

Measures to watch

Measure	Why it matters
Payment success rate	Customers expect it to just work
Scam and fraud claims per 10,000 payments	The main customer harm
Claim decision time	A Reg E and trust issue

Measure	Why it matters
Mule accounts found	Shows receive-side controls work
Enrolment completion rate	Product health

Go-live checklist

- [ ] Network certification complete
- [ ] E2E and UAT exit criteria met and signed
- [ ] Pilot payments reconciled
- [ ] Fraud scoring, warnings and limits live
- [ ] Evening and weekend support in place
- [ ] Alerts and escalation tested
- [ ] DR path tested

Sources

- Zelle: 2025 results press release (2026)
- Regulation E; UDAAP; BSA/AML and OFAC; Zelle network rules (from Early Warning Services)
- New York Attorney General lawsuit against Early Warning Services (August 2025)