PAYMENTS · DATA · AI · COMPLIANCE

Wire Payments (Fedwire and CHIPS) Delivery and Support Runbook

From requirements to live L1, L2 and L3 support: Fedwire and CHIPS basics, ISO 20022, exit criteria, sign-off, live pilot, fraud and sanctions 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 Federal Reserve, The Clearing House and your own bank policies.

Contents

1. Purpose and how to use this runbook
2. Planning vs delivery alignment
3. Wire 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 wire
9. Security, certificates and certification
10. Production support: L1, L2 and L3
11. Operational runbooks for common wire 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 US wire change, for example a new wire product, a new channel or a platform upgrade, from idea to live production and day-to-day support. It is written for product managers, delivery leads, engineers, testers, operations and compliance teams.

Wires are different from ACH in one important way: **a wire is final once it settles**. There is no return window to fix a mistake. So the controls before release (verification, approval, screening and limits) matter more than anything after it.

Golden rules for Agile wire delivery

- Work in sprints, but never skip the hard gates: security sign-off, E2E and UAT exit criteria, change approval and a live pilot before customers use it.
- Test every message type you will send and receive, including returns and rejects, not just the happy path.
- Treat callback verification, dual approval and sanctions screening as features with acceptance criteria, not as "compliance tasks".
- Plan around fixed dates: Federal Reserve holidays, cutoffs, year-end freezes and any Federal Reserve or CHIPS release dates.
- If in doubt, hold the wire. A delayed wire is a complaint; a wrong wire can be a permanent loss.

Planning vs delivery alignment

Wire projects usually carry fixed outside dates: Federal Reserve software releases, CHIPS releases, bank certification slots and change freezes at month end and year end. Put these on the calendar first and plan backwards from them.

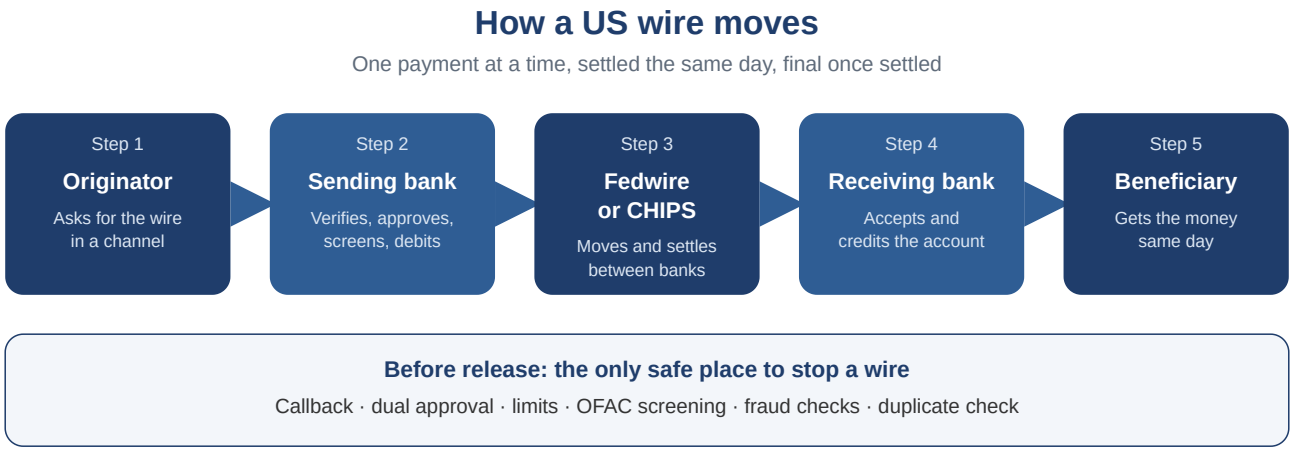
Level	What it holds	Who owns it	Reviewed
Product roadmap	Business outcomes, Federal Reserve and CHIPS release dates, big features	Product manager	Quarterly
Release or PI plan	Features committed for the quarter, dependencies, risks	Product manager, delivery lead	Every planning increment (8 to 12 weeks)
Sprint plan	User stories the team commits to for 2 weeks	Product owner and team	Every sprint
Release calendar	Deployment dates, freezes, Fedwire and CHIPS test windows	Release manager	Weekly

- **One backlog, fully traced:** each requirement links to its stories, tests, defects and release.
- **Plan to real capacity:** use actual velocity and keep 15 to 20% buffer for production support.
- **Track outside dependencies:** Federal Reserve, CHIPS, correspondent banks and vendors, each with an owner and date.
- **Measure it:** say/do ratio (80% or more), feature predictability, scope change and milestone status, reported weekly.

Wire basics for the team

A wire moves money from one bank account to another, one payment at a time, and settles the same day. In the US, banks send domestic dollar wires through two systems:

- **Fedwire Funds Service**, run by the Federal Reserve Banks. In 2025 it handled 217.3 million transfers worth about $1.15 quadrillion, an average of $5.28 million per transfer (Federal Reserve annual statistics).
- **CHIPS**, run by The Clearing House, a private system used mostly for large domestic and cross-border dollar payments. In 2025 its average daily value was $2.014 trillion, up 9% on 2024, with 43 direct participant banks (The Clearing House).



How a US wire moves

> **How to read this picture:** Read left to right: each box is one step a wire passes through, from the customer who asks for it to the person who receives it. The band at the bottom lists the checks that must happen before the sending bank releases the wire, because after Step 3 the payment is final.

Who is involved

Party	Role
Originator	The customer who asks for the wire (a person or company)
Originator's bank (sending bank)	Checks the request, debits the customer and sends the payment order
Fedwire or CHIPS	Moves the payment between banks and settles it
Intermediary bank	Optional bank in the middle, common for cross-border wires
Beneficiary's bank (receiving bank)	Receives the payment and credits the beneficiary
Beneficiary	The person or company who receives the money

Key facts

Topic	Fedwire	CHIPS
Operator	Federal Reserve Banks	The Clearing House
Settlement	Real-time gross settlement in central bank money: final when processed	Continuous netting with prefunded balances: final when released
Message format	ISO 20022 since July 14, 2025	ISO 20022 since April 8, 2024
Typical use	Domestic wires, bank-to-bank funding, securities and real estate	Large commercial and cross-border dollar payments
Hours	9:00 p.m. ET (previous day) to 7:00 p.m. ET, Monday to Friday, except Federal Reserve holidays	Check the current CHIPS operating schedule

Fedwire cutoffs (Eastern Time)

Message	Cutoff
Customer transfers (pacs.008) and their returns	6:45 p.m.

Message	Cutoff
Bank transfers (pacs.009) and other messages	7:00 p.m.
Service closes	7:00 p.m.

Your own customer cutoff must be earlier, to leave time for screening, approvals and repairs. Many banks use 4:00 to 5:00 p.m. ET.

Coming change: the Federal Reserve Board has announced that Fedwire and the National Settlement Service will move to 22 hours a day, 6 days a week (Sunday to Friday, including weekday holidays), expected in 2028 or 2029. Plan staffing, support and batch jobs for this now.

ISO 20022 messages your team must know

Message	Use
pacs.008	Customer credit transfer (a wire for a customer)
pacs.009	Bank-to-bank transfer, including cover payments
pacs.004	Return of funds
pacs.002	Payment status (accepted or rejected)
pain.013	Drawdown request (asking another party to pay you)
pacs.028	Payment status request
camt.052 / camt.054	Account reports and debit or credit notifications

Rules and regulations

Rule	What it means for delivery
UCC Article 4A	The main law for commercial wires: when a payment order is accepted, who bears loss, and the need for a commercially reasonable security procedure
Regulation J, Subpart B and Operating Circular 6	Federal Reserve rules for wires sent through Fedwire
CHIPS Rules and Administrative Procedures	Rules for CHIPS participants

Rule	What it means for delivery
Regulation E, Subpart B (Remittance Transfer Rule)	Consumer cross-border wires: disclosures, 30-minute cancellation right, error resolution
Bank Secrecy Act recordkeeping and Travel Rule	For transfers of $3,000 or more, keep and pass on originator and beneficiary information
OFAC sanctions	Screen every wire before release; block or reject hits as required
BSA/AML monitoring	Monitor for suspicious activity and file SARs
FFIEC guidance	Authentication, information security and business continuity expectations

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

- Wire types in scope: domestic customer, domestic bank-to-bank, drawdown, international USD, repetitive (template) and future-dated wires.
- Channels: online banking, mobile, file upload, API, branch and phone.
- Limits by customer, user and channel; dual approval thresholds.
- Callback rules: when a phone callback is required (for example new beneficiaries or changed instructions).
- Data needed for ISO 20022: structured names and addresses, purpose and remittance information.
- Fees, cutoffs, holiday handling and customer notifications.

Exit: requirements signed off by product, operations, compliance and fraud; each has acceptance criteria.

Phase 2: Design

- End-to-end flow: capture, validation, approval, fraud and sanctions checks, funds check, release, Fedwire or CHIPS send, acknowledgement, posting and notification.
- Routing rules: Fedwire or CHIPS, intermediary banks and correspondent accounts.
- Exception queues: repair, OFAC review, fraud review, insufficient funds, rejected messages.
- Idempotency: a unique reference per wire so a retry never sends twice.
- Data protection: account numbers masked in logs and screens.

Exit: architecture and security reviews passed; design traced to requirements.

Phase 3: Development

- Build to the ISO 20022 specifications for Fedwire (MyStandards) and CHIPS.
- Validate messages against the schema before sending.
- Store the IMAD and OMAD (Fedwire message references) for every wire.
- Code review, static analysis and dependency scanning on every change.

Exit: code reviewed, scans clean or risk-accepted, unit tests passing.

Phase 4: Unit testing

- Field validation, limits, approval rules, cutoff logic, holiday calendar and fee calculation.
- Message building for each message type; schema validation.
- Target at least 80% code coverage on wire logic, with 100% on limit and approval rules.

Exit: unit tests passing in the pipeline; no open critical defects.

Phase 5: Performance testing

- Peak volume: month end, quarter end and the last hour before cutoff.
- Release throughput: how many wires per minute can be screened, approved and sent.
- Queue recovery: how fast a backlog clears after an outage.

Exit: peak volume handled with headroom (for example 2 times expected peak), no message loss.

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

- Full flow from channel to Fedwire or CHIPS test environment and back, including acknowledgements and rejects.
- Returns (pacs.004), status requests, drawdowns and cover payments.
- OFAC hits, fraud holds, insufficient funds, duplicate detection and cutoff misses.
- Posting, general ledger, statements and customer notifications.

Phase 7: User acceptance testing (UAT)

- Operations and business users run real scenarios: create, approve, repair, release, return, investigate.
- Customer journeys in each channel, including callback and approval.

Phase 8: Release management

- Change approval (CAB), release notes, rollback plan and communication plan.

- Releases outside the Fedwire business day where possible; never during the last hours before cutoff.

Phase 9: Deployment

- Deploy, run smoke tests, then a live pilot (see "Proving it in production").
- Watch queues, acknowledgements and reconciliation closely for the first days (hypercare).

Exit criteria and sign-off: E2E and UAT

E2E entry criteria

- [ ] Build deployed to the E2E environment and smoke tested
- [ ] Connection to the Federal Reserve or CHIPS test environment working
- [ ] Test data ready: customers, accounts, beneficiaries, limits and sanctions test names

E2E exit criteria

- [ ] 100% of planned test cases run; at least 95% passed
- [ ] No open Severity 1 or 2 defects; Severity 3 defects have an agreed fix plan
- [ ] Every message type sent and received successfully, including returns and rejects
- [ ] Reconciliation between the wire system, core banking and general ledger balanced
- [ ] OFAC and fraud scenarios behave as designed

UAT exit criteria

- [ ] All business scenarios passed and signed by the business owner
- [ ] Operations procedures tested by the people who will use them
- [ ] Customer 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 head	Team trained, procedures ready
Compliance / BSA officer	OFAC, Travel Rule and Reg E requirements met
Information security	Security testing passed
Change manager	Release approved

Any exception needs a written waiver with risk owner, reason and expiry date.

Proving it in production

Wires can't be undone, so prove the live path with small, controlled payments before customers use it.

1. Send a small wire (for example $1) from an internal account to an account you control at another bank.
2. Confirm the Fedwire acknowledgement and record the IMAD and OMAD.
3. Confirm the receiving bank credited the right account with the right name and reference.
4. Receive a small incoming wire and confirm it posts correctly.
5. Send a return and confirm it is processed.
6. If CHIPS is in scope, repeat over CHIPS.
7. Reconcile all test wires to the general ledger before opening to customers.

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

Controls that run across every wire

Control	What good looks like
Strong authentication	Multi-factor sign-in for every user who creates or approves wires
Dual approval	A second person approves wires above a set amount; no self-approval
Callback verification	Phone callback on a known number for new or changed beneficiary instructions
Limits	Per wire, per day, per user and per customer, enforced by the system
OFAC screening	Every wire, every party, before release; hits reviewed and decided by trained staff
Fraud monitoring	Rules and models for new beneficiaries, unusual amounts, unusual times and business email compromise patterns
Duplicate detection	Same amount, beneficiary and date flagged before release
Reconciliation	Wire system, Federal Reserve account statement and general ledger balanced every day
Audit trail	Every create, change, approval and release logged with user and time

Business email compromise (BEC) is the biggest wire fraud risk: a criminal poses as a supplier or executive and asks for a change of bank details. The defence is a process: verify any change of instructions by calling a known number, never a number in the email.

Security, certificates and certification

- **Access:** least privilege, quarterly access reviews, and privileged access through a PAM tool. Follow NIST SP 800-63B for passwords and multi-factor authentication.
- **FedLine:** Fedwire connections use FedLine Direct or FedLine Advantage. Manage FedLine certificates, tokens and subscriber roles carefully, and track every expiry date.
- **Certificates and keys:** keep an inventory of TLS certificates and keys for CHIPS, SWIFT and APIs; alert 60, 30 and 7 days before expiry; renew in a planned change.
- **Software certification:** the Federal Reserve and The Clearing House require testing and certification before production and after major releases. Keep evidence.
- **Vendors and licences:** track vendor versions, support end dates and licence terms; review SOC reports yearly.
- **Open source:** scan dependencies for vulnerabilities and licences on every build.

Production support: L1, L2 and L3

Level	Who	What they do	Target
L1	Wire operations and service desk	Monitor queues, repair wires, answer customer calls, first triage	Acknowledge within 15 minutes
L2	Application support	Diagnose system issues, restart jobs, fix data, manage incidents	Respond within 30 minutes during the Fedwire day
L3	Engineering and vendor	Code fixes, hotfixes, root cause	Engaged within 1 hour for Sev 1

Severity levels

Severity	Example	Response
Sev 1	Cannot send wires, Fedwire or CHIPS connection down near cutoff	Bridge call within 15 minutes; leaders and the Federal Reserve contact informed
Sev 2	Wires delayed, one channel down, screening queue backed up	Response within 30 minutes
Sev 3	Single wire issue, report wrong	Next business day

Alerts and notifications

- Real-time alerts to Slack or Teams and on-call paging for: connection loss, no acknowledgements in X minutes, queue above threshold, wires pending close to cutoff, certificate expiry and reconciliation breaks.
- Email to stakeholders for Sev 1 and Sev 2 at start, every 30 minutes, and at resolution.
- Customer notice through channels if wires will miss the same day.

Escalation: L1 to L2 at 15 minutes without progress; L2 to L3 and the incident manager at 30 minutes; to senior leaders for any Sev 1 or if any wire may miss the cutoff.

Hotfixes: an emergency change with a named approver, peer-reviewed code, tests in a lower environment, and a post-implementation review within 5 business days.

Operational runbooks for common wire incidents

1. Fedwire connection down

1. Confirm the problem (FedLine status, network, certificates).
2. Open a Sev 1 bridge and contact the Federal Reserve customer support line.
3. Switch to the backup connection (for example FedLine Advantage if FedLine Direct is down).
4. If needed, use the Federal Reserve's contingency options for urgent wires, following your bank's procedure.
5. After recovery, reconcile every wire sent during the incident; check for duplicates before resending anything.

2. Wire sent to the wrong account or wrong amount

1. Stop: do not send a second wire to "fix" it.
2. Ask the receiving bank to return the funds (request for return), with the IMAD and OMAD.
3. Inform the customer, compliance and, if fraud is suspected, the fraud team.
4. Record the loss or recovery and run a root cause review.

3. Suspected fraud (BEC) after release

1. Contact the receiving bank immediately and ask them to freeze and return the funds.
2. Report to the FBI IC3; act fast, recovery chances fall quickly.
3. File a SAR if required; preserve all evidence.

4. Wires stuck before cutoff

1. Find where they are stuck: approval, OFAC, fraud, funds or repair queue.
2. Add staff to the queue; contact customers whose approval is missing.

3. Tell customers early if a wire will go next day.

5. Duplicate wire sent

1. Confirm both wires settled (IMAD and OMAD).
2. Request return of the duplicate from the receiving bank.
3. Fix the cause (retry logic, idempotency key) before the next release.

Disaster recovery

Wires must still go out if the main site fails. Agree recovery targets with the business; for many banks the wire platform is a critical system.

Item	Example target
Recovery time objective (RTO)	2 to 4 hours, and always before the Fedwire cutoff
Recovery point objective (RPO)	Near zero: no accepted wire may be lost

- [ ] Backup site connected to Fedwire and CHIPS and certified
- [ ] FedLine backup connection and tokens tested
- [ ] Contingency procedures for urgent wires documented and tested
- [ ] DR test at least once a year, with evidence and lessons learned
- [ ] After failover, reconcile every wire to avoid duplicates or losses

Internal and external audit

Internal audit checklist

- [ ] Wire policies and procedures current and approved
- [ ] Customer wire agreements and security procedures signed
- [ ] Dual approval and callback controls working (sample wires)
- [ ] Limits set, reviewed and enforced by the system
- [ ] OFAC screening complete; hits decided and documented
- [ ] Travel Rule data included for wires of $3,000 or more
- [ ] Reg E remittance disclosures and error cases handled on time
- [ ] Access reviews done 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
- [ ] Wire population lists ready to sample
- [ ] Change records with approvals, test sign-offs and pilot evidence
- [ ] Access lists and review sign-offs
- [ ] Incident records and root cause reviews
- [ ] BSA/AML and OFAC policies, training and independent testing
- [ ] Vendor SOC reports and reviews
- [ ] Open findings tracker with owners and dates

Measures to watch

Measure	Why it matters
Straight-through processing rate	Wires that need no manual repair
Wires released before cutoff	Missed cutoffs hurt customers
OFAC and fraud queue age	Long queues delay wires and risk cutoff misses
Fraud losses and recoveries	The main risk for wires
Rejects and returns	Data quality and routing problems
Reconciliation breaks	Must be zero at end of day
Availability of the wire platform	During the Fedwire business day

Go-live checklist

- [ ] E2E and UAT exit criteria met and signed
- [ ] Federal Reserve and CHIPS certification complete
- [ ] Live pilot wires settled and reconciled
- [ ] Limits, dual approval and callback switched on
- [ ] OFAC and fraud screening live and staffed
- [ ] Alerts, on-call and escalation tested
- [ ] DR path certified
- [ ] Operations and service desk trained

Sources

- Federal Reserve Financial Services: Fedwire Funds Service annual statistics, operating hours and ISO 20022 implementation center
- Federal Reserve Board: Fedwire Funds Service overview; notice on expansion to 22x6 operating hours (October 2025)
- The Clearing House: CHIPS network overview and 2025 results
- UCC Article 4A; Regulation J; Regulation E Subpart B; BSA recordkeeping rules (31 CFR 1010.410); OFAC