

Last Modified on 10/29/2026 9:21 am MDT

Governance and operating decisions for modern treasury channels

When a customer's software can initiate payments continuously, a treasury service depends on more than a signed agreement and a weekday support desk. Instant payments, application programming interfaces, and embedded delivery change who can instruct the bank, when an instruction becomes effective, and how quickly the bank must respond to a compromised credential. Those operating questions should drive the next phase of treasury investment.

Match instant settlement with continuous operating controls

FedNow provides a useful example of why speed changes risk. Settlement finality is determined under its governing rules, not by the customer's screen or the bank's next core posting cycle. Return requests are different from a unilateral right to reverse a settled payment. Service descriptions should state the actual cancellation window and avoid suggesting that a bank can reliably recover a mistaken or fraudulent payment after settlement. [1]

Before enabling a customer, test an after-hours credential compromise, a funding shortage, and a processor outage. Identify who can suspend a credential or channel, reach the receiving institution, and communicate with the customer. Confirm available liquidity, escalation coverage, and the service limits promised to customers. Review current operating procedures as well as the contract; FedNow procedures were updated effective October 13, 2026. [2]

Treat API credentials as delegated payment authority

An application programming interface, or API, allows software to communicate directly with the bank's systems. A payment-enabled credential can function like a powerful

treasury user, although access should be limited to its authorized purpose. The onboarding record should identify the customer, the software provider, the person or entity controlling the credential, and the authority for instructions submitted through it.

Record the permitted functions, accounts, beneficiary creation rights, transaction and daily limits, approval requirements, rotation schedule, and revocation contacts. If a vendor controls the credential, verify the customer's delegation to that vendor. The relevant issue is whether the vendor can bind the customer through instructions to the bank; possession of an API key does not itself authorize the vendor to bind the bank to an unseen vendor contract. Test revocation across the connected systems and retain a credential inventory. [3]

For example, a credential intended only to retrieve balances should not inherit the ability to create beneficiaries because the API supports that function. If the customer later adds payment initiation, require a new scope approval, appropriate payment security terms, and a test of transaction limits before enabling it.

Control the partner functions in embedded treasury

Embedded treasury places accounts or payments inside another company's software. Identify which entity markets the service, verifies eligibility, obtains customer acceptance, holds the account, provides support, and receives complaints. A partner may perform several of those functions, but the bank needs a record of the allocation and access to information needed to perform its own duties. [4, 5]

Require approval before a partner changes a material customer flow, disclosure, payment capability, or delegated function. Specify incident notices, customer record access, reconciliation, complaint escalation, audit rights, and transition support. If a partner fails, the bank should be able to identify affected customers and operate or wind down their services without depending on unavailable partner staff.

Connect fraud controls to current payment obligations

Maintain a security baseline for each high-risk service and identify optional controls above that baseline. Beneficiary restrictions, dual approval, preventive limits, and independent verification of sensitive changes address different failure modes. Preserve customer elections, but do not present a signed rejection as a substitute for an acceptable residual risk decision.

ACH fraud governance also requires attention to current Nacha rules. Phase 2 extends the risk-based fraud monitoring requirements to all nonconsumer originators, relevant service providers and senders, and receiving financial institutions within their

respective roles. Its stated June 19, 2026 effective date fell on a federal holiday, making June 22 the practical implementation date. Applicable processes require at least annual review; the rules do not prescribe one universal control or require every entry to be screened individually before processing. [6, 7]

Price the operating commitment as well as the transaction

An API or instant payment price should account for onboarding, credential administration, monitoring, support coverage, reconciliation, and incident response. Specify usage measurement, implementation charges, tiers, earnings credit treatment where relevant, and the notice needed to change pricing. Confirm the billing system can reproduce the charge from the customer's usage records.

Before adding a rail or distribution partner, identify which control costs recur regardless of transaction volume. A product that appears profitable using only per-item processing costs may become uneconomic once the bank provides the service it promised. Management should approve pricing with the same operating assumptions used in the risk review.

Require evidence before expanding the program

Keep a program file containing the approved activity description, partner diligence and contract, customer agreement versions, credential inventory, data and funds flows, complaint routing, and tested exit process. For third-party functions, obtain reports that let the bank verify performance rather than merely receive a certification that controls exist. [4]

Authorize expansion only after the bank can suspend payment initiation, revoke vendor access, reconstruct a customer balance, and retrieve the relevant customer and transaction records. A failed test should identify the capability or exposure that remains restricted and the owner responsible for fixing it.

The management deliverable

- Maintain a channel approval for instant payments and APIs that identifies authority, limits, finality, incident response, and after-hours support.
- Keep a current inventory of payment-enabled credentials and verify that a revocation reaches every connected system.
- Review embedded partner controls and role-specific ACH fraud processes before increasing customers, functionality, or exposure.

Sources and application

[1] **FedNow governing materials**. Federal Reserve Operating Circular 8, effective April 1, 2026, particularly section 7 on settlement.

[2] **FedNow operating procedures**. FedNow Service Operating Procedures, version 3.7, effective October 13, 2026.

[3] **FFIEC authentication guidance**. Authentication and Access to Financial Institution Services and Systems, August 2021. Risk-based guidance covering customers, staff, third parties, and system access.

[4] **Interagency third-party guidance**. Interagency Guidance on Third-Party Relationships: Risk Management, June 2023; Federal Reserve SR 23-4. Risk management guidance, not a new regulatory requirement.

[5] **Interagency deposit delivery statement**. Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services, July 25, 2024; Federal Reserve SR 24-5.

[6] **Nacha fraud monitoring rules**. Risk Management Topics, Fraud Monitoring Phase 2. Requirements are role specific and risk based.

[7] **Nacha effective date bulletin**. ACH Operations Bulletin 1 2024. June 19, 2026, is a federal holiday; the practical Phase 2 implementation date is June 22, 2026.
