

CSILLA BRIMER

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, OP-1880

Comment ID: FR-2026-0030-01-C18

Submitter Information

Name: Csilla Brimer

Submitted Date: 10/26/2026

While the proposed guidance appropriately addresses traditional third-party risk management, it should place greater emphasis on systemic concentration risk and AI-enabled cyber threats arising from shared technology providers that serve large portions of the U.S. financial sector.

Third-party risk has traditionally focused on vendor management, operational resilience, and regulatory compliance. Increasingly, however, certain third-party providers have become critical components of the nation's financial infrastructure. Companies such as FIS, Fiserv, and Jack Henry provide critical technology services to thousands of financial institutions. As a result, these organizations have effectively become systemically important technology intermediaries.

A successful compromise of one of these ecosystems, particularly through software supply-chain manipulation, privileged-access abuse, identity-provider compromise, or AI-accelerated exploitation of vendor dependencies, could simultaneously affect a substantial portion of the U.S. banking sector.

The agencies should consider a threat scenario involving advanced autonomous AI agents capable of continuously identifying exposed vulnerabilities, mapping software dependencies, correlating trust relationships, analyzing identity systems, and coordinating attacks across multiple organizations at machine speed. Such systems could accelerate reconnaissance, lateral movement, supply-chain compromise, and operational disruption far beyond what traditional threat actors can achieve manually.

The most significant concern is not necessarily the direct compromise of critical infrastructures such as Fedwire or SWIFT. Rather, it is the possibility that a compromise of a concentrated vendor ecosystem could undermine confidence in the institutions that rely upon those infrastructures.

For example, an attack against a major technology provider, identity provider, KYC vendor, AML platform, fraud-detection service, or payment-processing ecosystem could create uncertainty regarding:

- Account balances
- Transaction integrity
- Payment authentication
- KYC and AML controls
- Fraud-detection outputs
- Transaction reconciliation
- Settlement obligations

If multiple institutions simultaneously lose confidence in their ability to validate and process transactions, they may voluntarily restrict payment activity while attempting to verify the integrity of their systems.

Under stressed market conditions, this could produce a cascading sequence:

Vendor compromise → Transaction uncertainty → Liquidity hoarding → Delayed settlement → Increased collateral demands → Margin pressure → Counterparty contagion → Loss of confidence

The resulting disruption could occur even if Fedwire, SWIFT, and other market infrastructures remain technically operational.

Accordingly, I encourage the agencies to explicitly address concentration risk, shared technology dependencies, and AI-enabled systemic cyber threats within the final guidance.

In addition to traditional third-party risk management controls, the agencies should encourage the industry to adopt a broader systemic-resilience framework that includes:

- Cryptographically verifiable software provenance and software supply-chain integrity controls.
- Independent trust domains that limit the propagation of a vendor compromise.
- Strong limitations and auditability for AI-assisted administrative functions.
- Independent transaction-integrity verification mechanisms.
- Cross-institution resilience exercises involving simultaneous failure of multiple critical third-party providers.
- Stress testing of correlated cyber failures during periods of elevated liquidity demand such as quarter-end and month-end settlement cycles.
- Enhanced supervision of service-provider concentration risk across the financial sector.

Additional Immediate Mitigation Measures

Given the rapidly evolving capability of AI-assisted cyber operations, the agencies should encourage implementation of practical safeguards designed specifically to limit machine-speed attacks against concentrated service-provider ecosystems, including:

- Mandatory privileged-access isolation for critical third-party providers.
- Independent out-of-band recovery environments.
- Cryptographically enforced machine identities.
- Continuous attack-path analysis across interconnected vendor ecosystems.
- AI-versus-AI defensive monitoring.
- Sector-wide cyber circuit breakers.
- Independent transaction-reconciliation channels.
- Mandatory software bills of materials (SBOMs) and continuous dependency monitoring.
- Vendor concentration-risk thresholds requiring enhanced regulatory review.
- AI-enabled red-team exercises simulating machine-speed attacks.
- Rapid sector-wide threat-intelligence sharing mechanisms.

The agencies should also evaluate how distributed-ledger technologies could strengthen systemic resilience.