BURAK OKTENLI

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guidance, OP-1881

Comment ID: FR-2026-0031-01-C70

Submitter Information

Name: Burak Oktenli

Submitted Date: 11/20/2026

Please find attached my individual comment on the Proposed Third-Party Risk Management Guidance, Docket OP-1881. The comment recommends a proportionate example on delegated automated authority, addresses the questions in footnotes 9 and 15, and distinguishes restoration of connectivity from restoration of authority after an interruption. The complete comment is in the attached PDF.

November 20, 2026

Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration

Comment on Third Party Risk Management Guidance

OCC Docket ID OCC-2026-0793; RIN 1557-ZA18
Board Docket No. OP-1881
FDIC ZRIN 3064-ZA58
NCUA Docket No. NCUA-2026-1684; RIN 3133-ZA54

Dear Members of the Agencies:

I submit this comment in my individual capacity as an independent researcher studying authorization and recovery in automated systems. I support the proposal's tailored approach. My recommendation is to add a concise example explaining how its four risk management components apply when a third party's automated system can exercise delegated authority. The proposal already recognizes differences in third-party discretion and presents non-enforceable guidance. [1] The example should clarify those principles without creating a technology-specific checklist.

The practical distinction is between an instruction that a system can execute and an action that the bank or its customer has authorized. For example, a service could use valid credentials to act on an invoice whose beneficiary was altered by untrusted content. Successful authentication would not establish that the resulting payment stayed within the payer's mandate. This is an illustrative failure mode, not a claim about its measured frequency. Similar concerns can arise with conventional automation as well as AI agents.

1 Risk identification and assessment

Banks could identify which third-party services can initiate or execute consequential actions: moving funds, changing access rights, or making commitments for the bank or its customers. The assessment could describe whose authority is exercised, its permitted scope, and what prevents the service from exceeding it. Ordinary tools that only provide information should not acquire a new risk classification merely because they use AI.

In response to footnote 15, I recommend an illustrative risk indicator: a third-party service can cause material financial or operational consequences through delegated authority, particularly where action volume is large, effects are difficult to reverse, or independent limits and revocation controls are weak. This should prompt assessment rather than automatically determine that every such relationship is high risk.

In response to footnote 9, scope should not turn on whether an agreement was individually negotiated. Standard online terms and electronically accepted agreements may themselves be written agreements. The guidance could explain this and encourage banks to assess an actual service arrangement according to its functions and permissions. This would avoid a gap caused by treating informal procurement as evidence of immaterial risk, while preserving a meaningful boundary around third-party business relationships.

2 Risk oversight

Due diligence could examine the actions a service can take, the authority it relies on, and the controls that constrain execution. For material actions, a bank could seek a retrievable mandate record describing the authorizing party, permitted actions, relevant limits, validity period, and responsibility for exceptions. This need not require a new platform or a prescribed record format. Existing permissions, transaction controls, and audit records may provide the necessary evidence.

Contracts could address access to that evidence, changes in delegated permissions, incident notification, and revocation, including relevant subcontractor activity. Where customized terms are unavailable, the bank could assess compensating controls and the remaining exposure. Oversight should examine whether

consequential actions remain within current permissions; retrospective logs alone may be insufficient where unauthorized effects cannot readily be reversed. Controls may be automated: the recommendation does not require human approval of every transaction.

Operational resilience planning should distinguish restoration of connectivity from restoration of authority. An interruption, software update, or incident may invalidate assumptions behind a previously approved permission. Where relevant authority or its supporting evidence may have changed, the bank could require revalidation before affected consequential actions resume. Recovery should also reconcile queued and in-flight instructions against current mandates, checking expiry, revocation, duplicate execution, and conflicting outcomes. A restored connection should not, by itself, authorize replay of an old instruction.

Termination planning could identify how permissions, credentials, and downstream delegations will be revoked or transferred, and how completion will be evidenced. This should accompany orderly service transition rather than inadvertently interrupt necessary customer services.

3 Residual risk acceptance

Risk acceptance could state which actions may proceed without separate bank approval, within what exposure limits, and who can authorize exceptions. Responses to anomalies should be proportionate: restrict the affected permission when a defined risk condition is met, rather than suspend every service after any alert. Expansion of restricted authority should require renewed evidence and any approval required under the bank's established policy. Changes beyond a customer's agreed mandate should require fresh customer authorization.

Continuity arrangements could preserve unaffected services and provide a controlled manual or alternative route for essential transactions. They should account for customer harm from delay and applicable obligations as well as unauthorized execution. The objective is a defensible decision about the authority available during degraded operation, not a universal requirement to stop all activity.

4 Governance

Management could identify accountable owners for granting, monitoring, restricting, and restoring material delegated permissions. An existing third-party inventory could record these responsibilities without becoming a separate register for every software tool. Independent review could test whether restrictions actually prevent affected actions and whether recovery respects updated mandates, using selected scenarios such as a changed beneficiary, revoked permission, or unresolved prior transaction. Where practicable, the component enforcing permissions should not rely solely on the same automated service's assertion that its action is authorized.

A short example organized in this way would make the proposed principles more usable while preserving proportionality. It would focus oversight on consequential authority and evidence of its proper exercise, without favoring a vendor, architecture, or specific technology. Thank you for considering these comments during the extended comment period. [2]

Respectfully submitted,

Burak Oktenli, MBA
Independent Researcher

References

[1] OCC, Board, FDIC, and NCUA, Proposed Third-Party Risk Management Guidance, 91 Fed. Reg. 58536-58544 (September 15, 2026), proposed guidance sections A and B; footnotes 9 and 15. https://www.govinfo.gov/content/pkg/FR-2026-09-15/html/2026-18859.htm

[2] OCC, Board, FDIC, and NCUA, Proposed Third-Party Risk Management Guidance; Extension of Comment Period (comments due December 16, 2026). https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20261113a1.pdf