BONIS SYSTEMS LLC, JONIS FIELDS

Proposal and Comment Information

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

Comment ID: FR-2026-0031-01-C62

Submitter Information

Organization Name: Bonis Systems LLC

Organization Type: Company

Name: Jonis Fields

Submitted Date: 11/16/2026

Docket No. OP-1881, Third-Party Risk Management Guidance. Please see the attached comment of Bonis Systems LLC. It suggests that a vendor whose AI agent can act in customer accounts or start a payment be named as a high-risk characteristic (footnote 15), and addresses audit rights, subcontractors, ongoing monitoring, termination and footnote 9 for those vendors.

Third-Party Risk Management Guidance

OCC Docket ID OCC-2026-0793 · Federal Reserve Docket No. OP-1881 · FDIC ZRIN 3064-ZA58 · NCUA-2026-1684

November 16, 2026

Bonis Systems LLC is a small U.S. software company. It builds tools that keep a record of what AI software agents do. This comment addresses one kind of third party the proposed guidance does not yet name: a vendor whose AI agent can act inside a customer's account or start a payment.

The proposal never mentions artificial intelligence. That is reasonable for principles-based guidance. But banks are already deciding how to treat these vendors. Four short points follow, each tied to a place in the proposal, with a closing note on footnote 9.

1. Name agent vendors as a high-risk characteristic (footnote 15).

Footnote 15 asks whether a list of high-risk characteristics would help, and which ones to include. I suggest one: a third party whose software can act in customer accounts, or start, approve or change a payment, without a person at the bank reviewing each action.

The proposal's own test fits this case. It says a bank's higher-risk relationships "could include" those that could cause "an actual non-trivial violation of law or regulation," "material harm to the financial condition of the banking organization," or "a significant disruption to the banking organization's operations or customers," where there is "a material likelihood" of that harm (91 FR 58540). An agent that sends money on a customer's behalf can do that quickly, before anyone at the bank sees it. Footnote 12 says a third party with access to systems that "do not hold critical data and are appropriately segmented is not necessarily higher risk." I agree for that kind of access. An agent that can move money in a customer's account reaches the systems that hold that account, and a list would help examiners and banks tell the two apart.

2. For these vendors, keep the 2023 audit-right, notice and consent examples in view (58539, 58541–43).

The proposal says there are "no generally applicable expected contract terms," even for higher-risk relationships (58541). It also says the use of subcontractors alone does not typically create a presumption of direct oversight of them (58539). It still lists use of subcontractors as a

contract item and notes that a bank may oversee them through "contractual terms governing the use and oversight of subcontractors" (58542–43).

An agent vendor often depends on another company for the AI model that drives the agent. The Financial Stability Board notes that AI adoption in finance "increasingly depends on highly concentrated third-party providers across multiple layers of the AI supply chain" (p. 16). When that model changes, the agent's behavior can change, without any change to the contract between the bank and the vendor. That is a subcontractor chain: the 2023 Guidance counted the "suppliers, service providers, or other organizations" a third party enlists as subcontractors (88 FR 37931 n.14). It also gave three examples the proposal does not carry forward: the right to audit the third party and its relevant subcontractors (88 FR 37932), notice of new subcontractors, and consent before obligations are passed to another company (88 FR 37934). I ask that the final guidance keep these as examples a bank may weigh when the third party's agent can act on customer accounts.

3. Ongoing monitoring: a record the bank can check itself (58542).

The proposal's monitoring examples include reports from the third party and audits it conducts or hires another firm to conduct (58542). For an agent vendor, those rest on the vendor's own records, and periodic testing samples the service rather than showing each action. I suggest one more example: a record of each action the agent took, which the bank can check without relying on the vendor's own logs or word. The record would say which agent acted, for which customer, what it was allowed to do, and what it did.

The Financial Stability Board's final sound practices (October 15, 2026) describe record-keeping that lets a firm follow what an agent did and "whether it acted within its permissions" (Sound Practice 3, p. 26).

4. Let a bank stop an agent's access right away (58542–43).

The proposal's termination section discusses transition time, costs, and data access. The 2023 Guidance also named "information system connections and access control" as a risk to manage after a relationship ends (88 FR 37935). The proposal drops that item.

For an agent vendor, ending the relationship over months is not enough when something goes wrong today. I ask that the final guidance mention a bank's ability to cut off an agent's access at once and confirm that it stopped. The FSB lists "risk-based 'kill-switch' mechanisms to pause, limit, override or remove an agent's access" under human oversight (Sound Practice 10, pp. 52–53).

On footnote 9: a written-agreement test would leave out AI agents that customers bring themselves.

A bank customer can connect an AI tool to their own account. Where the company behind that tool has no written agreement with the bank, footnote 9 already treats its activity as unlikely to be a third-party relationship (58539), so a written-agreement test would leave it outside this guidance. I do not ask the agencies to stretch third-party guidance to cover these tools. I ask only that the final guidance say plainly that they are outside its scope, so banks know to manage that risk elsewhere.

Bonis Systems supports the proposal's focus on real risk over checklists. Naming this one kind of vendor would help banks put their attention where the risk now is.

Respectfully submitted,

Jonis Fields
Founder, Bonis Systems LLC
contact@bonissystems.com