

PEHTEE-NU LLC, ARIEL IGHUMA SAMA

Proposal and Comment Information

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

Comment ID: FR-2026-0031-01-C19

Submitter Information

Organization Name: Pehtee-Nu LLC

Organization Type: Company

Name: Ariel Ighuma Sama

Submitted Date: 10/12/2026

Docket No. OP-1881, Proposed Third-Party Risk Management Guidance. Comment of Ariel Ighuma Sama, Founder, Pehtee-Nu LLC. The full comment is attached as a PDF.

October 12, 2026

To: Office of the Comptroller of the Currency (Docket ID OCC-2026-0793); Board of Governors of the Federal Reserve System (Docket No. OP-1881); Federal Deposit Insurance Corporation (RIN 3064-ZA58); National Credit Union Administration (Docket No. NCUA-2026-1684)

Re: Proposed Third-Party Risk Management Guidance, 91 FR 58536 (September 15, 2026)

Thank you for the opportunity to comment. I am building verifiable audit trails for agentic payments, with a background in engineering and an MBA in financial mathematics. This comment concerns one kind of third party the proposal does not yet address: a vendor whose AI system can prepare, initiate or approve payments on a banking organization's behalf.

I support the proposal's principles-based, risk-tailored approach, and its recognition that newer and innovative third parties can benefit banking organizations and their customers. This comment does not ask for new rules. It suggests one sentence of guidance, in the proposal's own terms (Section 6 below).

1. AI agents fall between two pieces of guidance

The model risk management guidance issued in April 2026 by the OCC, the Board and the FDIC excludes agentic AI: "Generative AI and agentic AI models are novel and rapidly evolving. As such, they are not within the scope of this guidance." It also says those agencies plan to issue a request for information that considers banks' use of AI, "including generative AI and agentic AI."¹ That request had not been published as of October 12, 2026.

This proposal does not mention artificial intelligence or AI agents. A banking organization that obtains an AI agent from a vendor therefore finds guidance on neither the model nor the relationship.

The question is no longer hypothetical. In May 2026, Fiserv launched agentOS, "an agentic AI operating system designed to help financial institutions deploy, manage, and scale AI agents across their banking workflows," including "service, fraud, payments, compliance and growth workflows." Its marketplace offers agents built by Fiserv and by third parties, and six financial institutions are co-developing it.² Agent-initiated payments are still early, and this comment looks ahead. Federal Reserve Governor Christopher J. Waller made the same point about business payments in a recent speech: "the higher transaction values typical in B2B commerce amplify the financial exposure from agent errors or unauthorized actions, so robust controls and monitoring systems will be essential."³

2. Establishing what happened requires a record of the agent's actions (Section 2.iii, Ongoing Monitoring)

Banking organizations already have to establish what happened in a disputed transfer.

When a consumer reports an unauthorized or incorrect electronic fund transfer, Regulation E requires the institution to determine within 10 business days whether an error occurred, and, if it finds none, to tell the consumer of the right to request the documents it relied on.⁴

If an AI agent obtained from a third party prepared or made the transfer, the institution will need to know three things: what the agent was instructed, what information it acted on, and what it executed. The first two may exist only in the vendor's records, and those records can be short-lived and split across systems. Oracle's documentation for the NetSuite AI Connector Service, for example, states that its execution log data is available for 21 days in production, and advises customers to review that log "together with logs from external AI agents or MCP servers, when available," since external AI agents "operate outside NetSuite."⁵

The same need arises whether someone deceived the agent, for example with a fraudulent payment instruction, or the agent erred on its own. Governor Waller put the question plainly: "Who is on the hook if an agent makes the wrong purchase?" He suggested that technical standards "could be designed to give everyone a better understanding of what the buyer intended and how their agent carried it out."³

The proposal's examples of ongoing monitoring address a third party's performance and controls overall: reports and data, audits, visits, testing, examination reports and complaints. They are sound. None of them refers to records of the individual actions an AI system takes. The proposal already allows monitoring "on a periodic or continuous basis."⁶ For a third party whose AI system acts on individual transactions, records of those actions are the means of monitoring it.

3. The model is a subcontractor that can change between transactions

The proposal states that "the banking organization remains responsible for complying with applicable laws and regulations, and operating in a safe and sound manner, regardless of a third party's use of subcontractors."⁷ For a vendor's AI agent, the most consequential subcontractor is often the model behind it, and the vendor can update or replace that model between one payment and the next. Effective oversight therefore needs to know which model acted on which transaction. The records described above should identify it.

4. Contracts the bank cannot negotiate (Sections 2.ii and 3)

The proposal recognizes that "third parties often offer standard contracts," and that a banking organization with limited negotiating power may proceed if residual risks are

within its risk appetite.⁸ Standard terms already assign the consequences of agent actions to the customer. Stripe's Services Agreement, for example, provides that the user "is solely responsible for each action initiated by or through the AI Agent," and that such actions "are legally binding on User," and defines an AI agent to cover technology acting for the user "whether or not User has direct control over or visibility into each intermediate system in the chain."⁹ Where such terms cannot be negotiated, access to and retention of action-level records is one practical way to understand, and so manage, the residual risk.

5. Credit unions

Among its examples of ongoing monitoring, the proposal lists reviews of reports of examination arising from the agencies' supervision of certain large third parties, citing the banking agencies' authority to examine service providers.¹⁰ Credit unions have no equivalent source: as the NCUA's Examiner's Guide states, the agency "does not have the authority to examine third-party vendors."¹¹ A credit union that uses a vendor's AI agent therefore relies entirely on its own access to records of the agent's actions.

6. Suggested language

In Section 2.iii (Ongoing Monitoring), one sentence along these lines:

"Where a third party's AI system can prepare, initiate or approve transactions on the banking organization's behalf, ongoing monitoring may include records of the system's individual actions (for example, what it was instructed, the information it acted on, what it executed, and which underlying model acted), retained and protected from alteration for a period commensurate with the risk."

Optionally, in the Subcontractors example, a note that AI systems may rely on underlying models and services that can change without notice to the banking organization.

This suggestion is deliberately limited. It does not prescribe a technology, a retention period or a format, and it does not require that records be held by an independent party; a banking organization's own records, or its vendor's, with appropriate controls, would satisfy it. It is consistent with Governor Waller's emphasis on industry-developed standards.

Finally, I encourage the agencies to address AI agents in the promised request for information on model risk management, and to keep that work and this guidance consistent, so that an AI agent obtained from a vendor is covered as both a model and a relationship.

Respectfully submitted,

Ariel Ighuma Sama

Founder, Pehtee-Nu LLC

ariel.sama@pehtee-nu.com
pehtee-nu.com

1. OCC Bulletin 2026-13, "Model Risk Management: Revised Guidance" (April 17, 2026), <https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-13.html>; issued by the Board as SR 26-2, <https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm>. ↩
2. Fiserv, "Fiserv Launches agentOS: The Operating System for Agentic AI in Banking," press release, May 14, 2026, <https://www.globenewswire.com/news-release/2026/05/14/3294727/0/en/Fiserv-Launches-agentOS-The-Operating-System-for-Agentic-AI-in-Banking.html>. ↩
3. Christopher J. Waller, "Payments in the Age of AI Agents," speech at Sibos 2026, Miami, Florida, September 29, 2026, <https://www.federalreserve.gov/newsevents/speech/waller20260928a.htm>. As the speech notes, the views are his own. ↩↩
4. 12 CFR 1005.11(a)(1)(i) and (ii), (c)(1) and (d)(1). ↩
5. Oracle NetSuite, "NetSuite AI Connector Service FAQ," https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/article_4160616848.html (monitoring, retention of 21 days in production and 7 in sandbox, and external components); see also "Connect to the NetSuite AI Connector Service," https://docs.oracle.com/en/cloud/saas/netsuite/ns-online-help/section_0714082142.html (the execution log's fields). ↩
6. 91 FR 58542 (Section 2.iii). ↩
7. 91 FR 58543 (Subcontractors). ↩
8. 91 FR 58542 (Section 2.ii); see also 91 FR 58544 (Section 3, Residual Risk Acceptance). ↩
9. Stripe Services Agreement, General Terms, Sections 1.7 and 12 (last modified September 28, 2026), <https://stripe.com/legal/ssa>. ↩
10. 91 FR 58542 and note 17, citing 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1). ↩
11. NCUA Examiner's Guide, "Credit Union Service Organizations," <https://publishedguides.ncua.gov/examiner/content/examinersguide/CUSOs/IntroCUSO.htm>. ↩