OPSUITE AI, INC. (RISKERNEL), AMIR SHACHAR

Proposal and Comment Information

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

Comment ID: FR-2026-0030-01-C23

Submitter Information

Organization Name: Opsuite AI, Inc. (Riskernel)

Organization Type: Company

Name: Amir Shachar

Submitted Date: 11/13/2026

Opsuite AI, Inc. (Riskernel) submits the attached comment letter on Docket No. OP-1880, the Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations. Riskernel builds fraud-detection software for banks and fintech companies. The letter answers topics 2 through 7. In short, it asks the Board to confirm that buying a fraud tool from a fintech vendor is not a complex bank-fintech partnership; to say what evidence a community bank can ask of a younger vendor that does not yet hold the usual audit reports, such as a test on the bank's own data; to keep fraud tools as their own category, including tools that come inside a payment or card processor; and to give community banks a short, ordered list of contract terms to ask for first. The full letter, signed by Amir Shachar, Founder, is attached as a PDF.

Opsuite AI, Inc. ("Riskernel")
1111B S Governors Ave STE 40435, Dover, DE 19904

November 13, 2026

Benjamin W. McDonough, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Docket No. OP-1880 (regulations.gov FRS-2026-4027); Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

Dear Secretary McDonough:

Opsuite AI, Inc. ("Riskernel") submits this comment in response to the Board's request for comment on the proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, published on September 15, 2026 (91 FR 58438). Riskernel builds fraud-detection tools for fintechs. Our founder, Amir Shachar, was Head of Fraud Data Science at NICE Actimize and Chief Data and AI Scientist at Skyhawk Security, is a named inventor on 14 patents and patent applications in fraud detection, cybersecurity and machine learning, and wrote "Introduction to Algogens" (arXiv 2403.01426). We write as a fraud-technology vendor, the kind of company a community bank may one day have to evaluate under this guide. We answer the topics where that view is useful and leave the others to banks and their examiners.

The notice lists eight specific topics without numbers. We number them 1 to 8 in the order printed and answer Topics 2 to 7.[1]

1. Scope: a fraud tool is not a "complex bank-fintech partnership" (Topic 2)

Footnotes 1 and 5 of the proposed guide say it is not meant for community banks with "complex bank-fintech partnerships," described as arrangements in which the fintech company, rather than the bank, markets, distributes or otherwise provides access to the products or services. The wording is clear for a bank that offers a fintech's deposit or lending product. It is less clear for a bank that buys a fintech's software for its own use, such as a fraud-scoring service, an identity check or a monitoring tool. In that arrangement the bank keeps the customer relationship and the fintech never faces the customer.

A bank in that position could read the exclusion as covering it and set the guide aside. In answer to the question in Topic 2 about additional examples, we ask the Board to add one: a community bank that licenses a service from a fintech vendor for its own operations, while the bank alone offers products to its customers, is within the guide. The exclusion would then plainly apply to arrangements in which the fintech provides the bank's products to customers.

2. Usefulness and level of detail for fraud vendors (Topics 3 and 4)

Section IV.C.8 is a good start. It names real-time fraud monitoring, device fingerprinting, behavioral analytics and authentication, it asks banks to track false-positive trends, and it says a bank may consider "the extent to which the provider can calibrate its model based on the TCBO's direction in keeping with the TCBO's risk appetite." Three additions would make it easier to use without turning it into a checklist.

- A trial before commitment. A bank can ask a fraud vendor to score the bank's own recent transactions while the vendor takes no action on them, and compare the results with what the bank's staff already know about those cases. This shadow test shows how the tool behaves on the bank's customers, which a demonstration on the vendor's own data cannot. It also gives the bank the

baseline it needs, because a false-positive trend cannot be read later without knowing where it started.

- Reasons for each decision. A bank has to explain a declined payment to a customer, and an examiner may ask why it was declined. The guide could say a bank may consider whether the vendor gives a reason for each decision, in terms staff can use, and whether those records can be exported.
- Changes to the tool. Section IV.C.8 asks whether the bank can direct the vendor's model. The guide should also ask whether the vendor tells the bank before it changes the model or its rules in ways that affect decisions, and whether the bank can see the effect of a threshold change before it takes effect.

On the level of detail (Topic 4): the guide's habit of saying a bank "may consider" an item is right, and we would keep it. For a bank with a small staff, a list that reads like a checklist will in practice become a standard for the examination, whatever the preface says. We think the guide is at about the right level now, and these additions are better offered as examples of what a bank may consider than as expectations.

3. Overarching considerations in Section IV.B (Topic 5)

Evidence of controls from younger vendors. Section IV.B.1 lists SOC reports, penetration testing reports and standards such as PCI DSS and ISO as the independent assessments a bank can rely on. Vendors that are young or specialized may not yet hold them. We ask the Board to say that a bank may reasonably consider other evidence when a report is not yet available: a written description of the vendor's security controls, a recent penetration test summary, a completed security questionnaire, references from other institutions, and a plan and date for obtaining the report. The guide already says a bank may reasonably proceed without optimal terms in some cases (footnote 8). Saying the same for evidence would keep a missing report from being the only reason a small bank passes over a useful vendor.

Testing a tool against the bank's own results. The joint proposal from the OCC, the Board, the FDIC and the NCUA issued the same day lists, among examples of ongoing monitoring, "in certain circumstances, periodic testing of the third party's services to the banking organization to assess the third party's performance and effectiveness" (91 FR 58536, 58542). For a fraud tool this can mean comparing the tool's decisions from time to time with confirmed fraud outcomes, customer complaints and legitimate payments the bank declined. Section IV.B could say so. SR 26-2 (April 17, 2026) points the same way for vendor models, calling for "ongoing monitoring and outcome analysis" to assess whether they remain accurate and fit for purpose. It is most relevant to banks over $30 billion, but it is a useful benchmark for what a smaller bank can scale down.

When the tool fails. Section IV.C.8 observes that a system failure can block legitimate transactions or let fraudulent ones through. We suggest the guide add that a bank decides in advance, and tests, how each tool behaves when it cannot reach the vendor.

Ending the relationship. Section IV.B.2 says a bank may benefit from verifying that data has been "successfully migrated or destroyed." For a fraud vendor we suggest the guide add a written confirmation from the vendor that all copies were deleted, with the date, and that the vendor used the bank's data only for the bank's own work during the term. The card-processing discussion in Section IV.C already suggests keeping the old processor running while the new one comes online. The same applies to a fraud tool, which runs in real time and cannot have a gap.

4. Vendor categories in Section IV.C (Topic 6)

We would keep fraud prevention and detection as its own category, as the proposed guide does, and add two points to it.

First, the guide recognizes that a bank may receive fraud tools embedded in its payment or card processor. A bank in that position still needs to see how the tool performs. The guide could say a bank may ask the processor for the same outcome information it would ask of a separate fraud vendor.

Second, the section describes tools such as device fingerprinting and authentication, which are built mainly to catch someone else using a customer's account or card. Some fraud instead comes from payments the customer makes personally after being deceived by a caller or a message posing as the bank, an agency or a relative. Device and login checks help least there, because the real customer is logged in on a known device. The guide could ask a bank to consider whether a fraud tool addresses customer-authorized payments, including instant and wire payments, as well as account takeover.

5. Better support for contract negotiations (Topic 7)

The guide says in several places that a community bank may lack leverage and may not obtain optimal terms. We agree, and we think the most useful help is a short order of priority, because a bank that cannot win every term should know which ones to ask for first. From the vendor side, these cost a vendor little to give and protect a bank the most:

- use of the bank's data only for the bank's own work, unless the bank agrees otherwise in writing;
- the right to access and extract the bank's data and decision records during the term and after it ends, as Section IV.C.7 already suggests for BSA/AML providers;
- a pilot or short initial term with a right to end it without penalty if the results do not match what was shown;
- notice before changes to the model or rules that affect decisions;
- a reason for each decision, kept and exportable;
- written confirmation of deletion at exit, with transition help while the bank moves to its next tool; and
- a stated time for notifying the bank of a security incident.

The pilot term and the exit terms matter most for a bank with little leverage, because they limit what is lost if the choice proves wrong.

We would be glad to answer questions from Board staff.

Respectfully submitted,



Amir Shachar
Founder
Opsuite AI, Inc.

[1] Board of Governors of the Federal Reserve System, Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, Docket No. OP-1880, 91 FR 58438 (Sept. 15, 2026), Parts I and II and Sections IV.B and IV.C, https://www.govinfo.gov/content/pkg/FR-2026-09-15/html/2026-18852.htm. The joint proposal cited in Section 3 is Proposed Third-Party Risk Management Guidance (OCC, Board (Docket No. OP-1881), FDIC and NCUA), 91 FR 58536 (Sept. 15, 2026), https://www.govinfo.gov/content/pkg/FR-2026-09-15/html/2026-18859.htm. SR 26-2 (Apr. 17, 2026) and its attachment are at https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm.