September 24, 2026
Submitted electronically via regulations.gov

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 1E-216
Washington, DC 20219

Re: Docket ID OCC-2026-0793 (RIN 1557-ZA18), Proposed Third-Party Risk Management Guidance

Dear Chief Counsel:

Coverbase Inc. submits this letter in response to the proposed third-party risk management guidance published in the Federal Register on September 15, 2026. It also includes brief remarks on the Joint Statement on Community Banks' Engagement with Core Service Providers released the same day, since the institutions we serve will read the two documents together. We are filing with the OCC and have copied the other three agencies.

I. About Coverbase and our position

Coverbase builds software that banks, credit unions, and insurers use to run their third-party risk programs: the vendor inventory, risk assessments, due diligence, contract review, and ongoing monitoring. Our customers range from community institutions with a few hundred vendors to national banks with tens of thousands, which gives us a direct view of how the 2023 guidance has been applied at both ends of the market.

Coverbase supports the proposal. The agencies' account of how the 2023 guidance played out is accurate, and in our experience understated. The 2023 guidance was not written as a checklist, but most institutions turned it into one, because a checklist is easier to defend in an exam than a judgment call. At many of the programs we work with, a marketing agency and a core processor receive the same 200-question form, the same annual review, and roughly the same staff time. Nobody involved thinks that makes sense. They do it because no one has told them they can stop.

We would caution against reading the proposal as a call for less third-party risk management. It asks institutions to stop doing the parts that never managed any risk, which is a different thing. An institution can only cut back on its low-risk relationships if it knows which ones those are, and that knowledge has to come from a real assessment rather than a default rating. The proposal asks more

of a program's judgment and less of its filing cabinet. Most of this letter is about making sure the final text is read that way.

II. Comments on the proposed guidance

A. Characteristics of higher-risk relationships (footnote 15)

The agencies ask whether the guidance should list characteristics that generally indicate a higher-risk relationship. A list is the kind of thing that got the 2023 guidance into trouble, and it is easy to imagine one being pasted into an examination workpaper within a month of publication. We still recommend including one. Without it every institution will write its own, and the ones we have seen are longer, keyed to vendor type rather than to harm, and rarely revisited.

The framing matters more than the contents. The text around the list should say that no single characteristic makes a relationship high risk, that characteristics are weighed against whatever mitigates them (segmentation, contract terms, insurance, a tested resilience plan), and that an institution which concludes, with reasons, that a relationship with several of these characteristics is lower risk receives the same deference as any other reasonable judgment.

The characteristics that in our experience actually predict harm when a vendor fails are these:

1. The vendor holds or has broad access to non-public customer data, or to systems that are not segmented from it.
2. The vendor runs or directly supports something that, if it stopped, would stop the institution from serving customers, settling payments, or meeting a reporting or compliance obligation.
3. There is no realistic alternative, or switching would be so slow or expensive that the institution could not credibly walk away.
4. The vendor exercises discretion or deals with customers in the institution's name in a way that could produce a consumer protection or fair lending violation.
5. A single vendor carries a large share of a business line, so the exposure is concentrated.
6. The vendor depends on its own subcontractors for the risky part of the work, so the institution's oversight is one step removed.
7. The vendor is new, financially weak, or has a track record of incidents, outages, or repeat audit findings.

The list should not include anything keyed to what kind of company the vendor is. "Fintech" is not a risk characteristic and neither is "uses AI." The preamble notes that the 2023 guidance discouraged banks from working with newer providers; a list that names categories of provider would do it again.

B. Scope: relationships with a written agreement (footnote 9)

We support limiting the guidance to relationships with a written agreement. It gives institutions a defensible edge to the vendor inventory, and the inventory is what everything else in the proposal depends on. We have watched customers spend hours debating whether an unpaid data feed or a trade association membership is a "business arrangement," and nothing useful comes out of it.

One clarification: "written agreement" should include click-through terms, online terms of service, and order forms the institution accepts as-is. Many of the vendors that matter (SaaS tools, data providers) are governed by terms nobody negotiated, and leaving them out because there was no redline would pull real relationships out of scope. The guidance should also say the reverse: a signed agreement with a low-risk vendor does not by itself create an expectation of oversight beyond what the risk assessment supports.

C. Other guidance to rescind (footnote 5)

We do not recommend further rescissions. A single page published with the final guidance, listing which prior bulletins, letters, and statements remain in effect and how they relate to the new text, would do more. Institutions and examiners are working from a stack of documents issued over twenty years, and the inconsistency we see in exams comes more from that stack than from any one document in it.

D. Reliance on technology, public sources, and collaborative arrangements

The proposal says institutions may rely on public and alternative sources for due diligence, on consortia and certification bodies, on outside experts, and on "third-party technologies or processes" to supplement their own oversight, and it notes that community banks in particular stand to benefit. We are not aware of prior guidance saying this as directly, and we think it is the most useful passage in the document for smaller institutions. We ask the agencies to keep it and to add the following so that it survives contact with examination.

First, say that analysis done with the help of software counts. If an institution uses a tool to read a SOC 2 report, pull the exceptions, map them to its control expectations, and flag what is missing, the conclusion should be as acceptable as one a person reached by reading the same report, provided the institution understands how the tool works, keeps the underlying evidence, and owns the conclusion. Some examiners today treat software-assisted review as inherently weaker than a human reading the document. If the final guidance is silent, that habit will continue and the benefit the agencies describe will not arrive.

Second, the proposal says that relying on third parties for risk management "can itself involve risks." We read this to mean that an institution should understand the limits of whatever it relies on. One sentence confirming that it does not require a provider of risk management tooling to be overseen at the level of the highest-risk relationships the tooling assesses would close a loop that a cautious compliance officer will otherwise notice, and resolve by not adopting the tool.

Third, as more of the reading and analysis is done by software, the agencies should say what they expect from its governance. We would keep it short: the institution can trace a conclusion back to the evidence it rests on and forward to the action taken; a named person is accountable for each consequential decision; and management can explain to the board and to the examiner how the conclusion was reached.

Finally, the due diligence section should make the sequence explicit. Under the checklist model, the institution sends every vendor the same questionnaire and then figures out what the answers mean. Under this proposal the order reverses: understand the relationship and the exposure, look at the evidence that already exists (internal records, public filings, certifications, prior assessments, the vendor's own trust documentation), and ask the vendor only for what is missing. Where the evidence in hand supports a defensible conclusion, another questionnaire adds cost and no assurance. This reordering is how the tailoring the agencies want actually happens in practice.

E. Risk assessment

We support the magnitude and likelihood framing, the option to assess at the relationship or activity level, and footnote 12's point that a vendor with access to segmented, non-critical systems is not automatically high risk. We would add one sentence stating that the assessment is iterative: the initial rating sets the depth of due diligence, and what due diligence and monitoring turn up feeds back into the rating. Many institutions treat the initial rating as fixed for the life of the contract.

F. Ongoing monitoring

The risk a vendor poses does not change because a review date arrives. It changes when something happens: a breach, a change of ownership, a lapsed certification, a lost anchor customer, or a scope of services that has quietly grown. Watching for those events, for the relationships that warrant it, is both cheaper and more useful than a comprehensive annual reassessment. The guidance should say that an institution doing the former is not expected to also do the latter absent a meaningful change.

G. Subcontractors

The statement that subcontractor use creates no presumption of direct oversight, and that the risk can be handled through contract terms and by evaluating the vendor's own third-party program, is the right answer. We ask that it be retained as written.

H. Residual risk acceptance

We support treating this as its own component. In our experience programs kept collecting because there was never a sanctioned moment to stop. Without a step where someone with authority says "we understand what remains and we accept it," the only defensible move was to ask for one more document. The guidance should say that a documented acceptance of that kind is itself evidence

of sound risk management, and that examiners should evaluate whether the decision was reasonable rather than how thick the file is.

Relatedly, each material finding from due diligence or monitoring should end somewhere: remediation by the vendor, closer monitoring, escalation, or explicit acceptance. Which one is the institution's call. That it goes somewhere should not be.

I. Credit unions and examination consistency

We welcome the NCUA's participation. Credit unions and community banks buy from the same vendors and run into the same problems, and a shared framework is overdue.

The proposal says several times that the agencies will give due consideration to reasonable decisions and that departing from the guidance is not by itself grounds for criticism. The value of those commitments depends on what happens in the exam room. We ask that the final guidance be accompanied by examination procedures and examiner training that reflect it, and that institutions have somewhere to go when an exam finding contradicts the final text.

III. The Joint Statement on core providers

The Joint Statement is not open for comment, but it will shape how the proposal operates for community institutions. The practices the agencies say they will weigh (withholding SOC reports, back billing, undefined deconversion fees, restrictions on third-party integration) match what our community bank and credit union customers describe, and it is useful to see them written down by a regulator.

Two places where the final guidance should match it. The proposal says that where a vendor will not provide the information needed for due diligence and monitoring, alternative sources may not be enough to proceed. For a core provider, most community institutions have no real option to decline. The guidance should acknowledge that where a core's lack of transparency is something the agencies are themselves addressing through supervisory allocation, an institution's documented acceptance of the resulting residual risk is a reasonable decision. Separately, the agencies should push core providers to make the SOC reports, penetration test results, and standard assessments listed in the Joint Statement available through standard, machine-readable channels rather than one-off requests. That is what would let the technology-assisted oversight the proposal endorses work for the relationships where it matters most.

IV. Summary of recommendations

1. Include a list of higher-risk characteristics, framed as indicators weighed against mitigants and keyed to the relationship and the harm, never to the type of vendor.
2. Scope the guidance to relationships with a written agreement, including click-through and online terms.

3. Publish a consolidated list of which prior issuances survive, rather than further rescissions.
4. State that software-assisted analysis of evidence is an acceptable basis for a conclusion when the institution understands the method, keeps the evidence, and owns the result.
5. Confirm that using risk management tooling does not require overseeing the tool provider at the level of the relationships it assesses.
6. Set a short governance expectation for technology-assisted oversight: traceability from evidence to conclusion to action, and a named accountable person.
7. Make the sequence explicit: existing evidence first, then request only what is missing.
8. State that the risk assessment is iterative.
9. Recognize that event-based monitoring may replace periodic full reassessment where risk has not changed.
10. Retain the subcontractor language as proposed.
11. Treat a documented residual risk acceptance as evidence of sound risk management, and expect each material finding to reach a disposition.
12. Pair the final guidance with examination procedures and training, and a way to raise inconsistent application.
13. Recognize residual risk acceptance for core provider relationships, and encourage standardized disclosure by core providers.

V. Closing

We appreciate the agencies' candor about how the 2023 guidance was applied. The proposal gives institutions permission to put their people where the risk is. We hope the final version keeps that permission intact rather than hedging it back.

We would be glad to discuss any of these comments or to share more on how institutions of different sizes are running their programs. Questions may be directed to the undersigned.

Respectfully submitted,

Clarence Chio
Co-Founder and Chief Executive Officer
Coverbase Inc.
contact@coverbase.ai

cc: 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)