FIRST NATIONAL BANK TEXAS, ROBERT W. HOXWORTH

Proposal and Comment Information

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

Comment ID: FR-2026-0030-01-C21

Submitter Information

Organization Name: First National Bank Texas

Organization Type: Company

Name: Robert W. Hoxworth

Submitted Date: 11/03/2026

See attached.

FIRST NATIONAL BANK TEXAS

Robert W. Hoxworth
President & CEO

November 2, 2026

Benjamin W. McDonough, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Docket No. OP-1880

Re: Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

Dear Mr. McDonough:

First National Bank Texas ("FNBT") is a regional community bank founded in 1901 and headquartered in Killeen, Texas. The bank serves communities throughout Texas, New Mexico, Arizona, and Arkansas and as of June 30, 2026, operates 356 branches.

FNBT focuses on both retail and commercial customers. We offer all types of consumer loans, commercial loans and lines of credit and mortgage loans along with a wide array of digital banking services. The vendor categories in the proposed guide—core processing, IT infrastructure, cybersecurity, payments and digital banking, loan systems, card processing, BSA/AML, and fraud—describe our own third-party relationships almost exactly.

FNBT thanks the Board of Governors of the Federal Reserve System (the "Board") for the opportunity to comment on the proposed *Third-Party Risk Management Guide for Traditional Community Banking Organizations* (the "Guide"). The Guide is the kind of practical resource community banks have asked for. It translates high-level principles into concrete, vendor-specific considerations, and it does so while repeatedly acknowledging that community banks have limited leverage and limited specialized staff.

The concerns and recommendations below respond to the Board's specific questions and are respectfully provided for your consideration.

Concerns and Recommendations

1. Interagency Adoption

Our most important recommendation is that the Guide be issued on an interagency basis. Non-member community banks, use the same core processors, sign the same contracts, and face the same staffing constraints as member banks. A resource this practical should be available to all community banks.

The Board issued the Guide as a companion to the interagency Proposed Third-Party Risk Management Guidance (Docket No. OP-1881). We urge the Board to work with the OCC and FDIC to issue or formally recognize a common, optional community-bank resource. Consistent practical resources help prevent differences in charter or primary regulator from producing inconsistent supervisory expectations. Interagency issuance would also be the natural vehicle for consistent examination practices.

2. The $30 Billion Threshold and the Definition of a TCBO

We support the $30 billion asset threshold. It captures the vast majority of community banks, including regional community banks that serve multiple states but share the third-party profile the Guide describes. That profile (shared core processors, limited negotiation leverage, and lean specialized staff) does not change meaningfully across community banks below the threshold.

We recommend the following clarifications:

- **Review the threshold periodically.** The Board should periodically evaluate the $30 billion threshold against changes in the banking industry and explain any resulting adjustments, rather than allowing the threshold to become outdated.

- **Focus on business model, not footprint.** The phrase "focus on serving their local communities" should not exclude banks that operate in several states or many markets. FNBT, like other regional community banks with branches in many communities and states, continues to serve local communities.

3. Usefulness of the Guide

The Guide will be useful. Its strongest features are its vendor-by-vendor structure, its emphasis on independent assessments such as SOC reports, and its practical discussion of core conversions, integration platforms, and cloud migrations. Its recognition that a TCBO may reasonably accept higher risk when adopting technology-forward core systems is especially welcome.

We suggest two additions that would make the Guide more useful in day-to-day practice:

- **Complementary user entity controls.** SOC reports often identify complementary user entity controls that the bank, rather than the service organization, must perform. A short, practical discussion of how a TCBO can identify relevant controls, assign ownership, assess gaps, and avoid duplicative testing would improve the value of those reports.

- **Concentration, data portability, exit planning, and fourth parties.** Community banks often rely on a single core provider for multiple critical banking functions, increasing their exposure to operational disruptions and challenges associated with changing providers. We recommend that the Guide provide practical, illustrative considerations for evaluating these risks, including a bank's ability to retrieve its data in a usable format, maintain essential services, plan for an orderly exit, understand the vendor's reliance on key subcontractors (fourth parties), and transition to another provider when necessary. Such guidance should recognize the limited negotiating leverage of community banks and the significant costs and operational complexities associated with vendor conversions, without establishing prescriptive requirements.

4. Level of Detail and Avoiding De Facto Standards

We appreciate the Board's efforts to provide practical guidance while preserving the flexibility for community banks to develop and implement third-party risk management programs appropriate to their size, complexity, business activities, and risk profiles. Our primary concern is not the level of detail within the Guide, but how its illustrative considerations may ultimately be interpreted and applied during regulatory examinations.

Community banks should retain the discretion to establish their own risk assessment methodologies, determine the criticality and risk classifications of third-party relationships, and establish appropriate due diligence and ongoing monitoring practices. These decisions should be reasonable, documented, and consistently applied. Where a bank departs from an illustrative consideration, it should document the risk, the alternative evidence or controls it relied on, and management's acceptability of any residual risk.

We recommend that the Board:

- Reinforce the nonprescriptive nature of the Guide. Clearly communicate that illustrative considerations are not minimum supervisory requirements and should not become standardized examination checklists.
- Promote consistency in examination practices. Provide examiner guidance and training emphasizing that supervisory assessments should focus on the reasonableness and effectiveness of a bank's risk management framework rather than an examiner's preferred risk classifications, documentation requirements, or monitoring frequencies. Examiners should evaluate the reasonableness and consistent application of a bank's documented risk assessment methodology and should judge a risk determination on the underlying risks and supporting rationale, not on whether it matches the examiner's preferred classification. Banks may reasonably classify similar relationships differently based on their circumstances, exposure, and mitigating controls.
- Ensure examination findings are supported by identified risks or deficiencies. The absence of a particular document, control, or monitoring activity described as illustrative in the Guide should not, by itself, constitute an examination finding. Supervisory concerns should be supported by identifying weaknesses in the bank's risk management practices or other applicable supervisory or legal requirements.
- Monitor consistency of implementation. Periodically evaluate examination practices to ensure the Guide is being applied as an optional supervisory resource rather than creating unintended prescriptive standards.

5. Overarching Considerations (Section IV.B)

We support the four overarching considerations identified in the Guide: operational resilience, system and information security, compliance with rules and regulations, and financial resilience. We appreciate the Board's recognition that community banks must be able to tailor their oversight practices based on the risks presented by individual third-party relationships and the information reasonably available to them.

We recommend the following clarifications:

- **Financial Resilience of Privately Held Vendors.** The Guide appropriately acknowledges the challenges community banks face in obtaining financial information from privately held vendors. We recommend that the Board explicitly recognize that banks may use alternative sources of information and reasonable judgment when assessing a vendor's financial condition. Banks should document what information they relied on and why it provided sufficient assurance, or why the

remaining risk was acceptable given the significance of the relationship. The lack of audited financial statements should not, by itself, be treated as inadequate due diligence.

- **Alternative Evidence When Vendor Information is Limited.** Community banks frequently encounter restrictions when requesting SOC reports, penetration testing results, business continuity documentation, and other independent assessments from larger service providers. We recommend clarifying that no particular report, certification, or assessment should be universally expected for every third-party relationship. Banks should be permitted to evaluate reasonably available information, consider alternative forms of assurance, and determine whether any remaining risks can be appropriately managed or accepted, with the basis adequately documented.

- **Payment network assessments.** The Guide's reference to NACHA audits and FedLine self-assessments is helpful. The Board could clarify that existing payment-network assessments may supply relevant evidence, while not automatically replacing a bank's assessment of the particular services, risks, or contractual responsibilities involved.

- **Consumer compliance boundary.** The Guide states that consumer compliance is outside its scope. We ask the Board to explain how TCBOs should use this operational risk resource alongside existing consumer-protection and fair-lending requirements for customer-facing vendor activities, without implying that any applicable consumer-compliance obligations have changed.

6. Vendor Categories (Section IV.C)

The eight categories reflect the relationships most common to community banks. We also suggest a concise, cross-cutting discussion of artificial intelligence and machine-learning features embedded in third-party products, including fraud detection, BSA/AML monitoring, and credit decisioning tools. TCBOs would benefit from illustrative questions concerning data security, output reliability, significant model or feature changes, appropriate human oversight, and the vendor's ability to provide meaningful assurance. These should be framed as risk-based considerations, not a separate one-size-fits-all AI checklist.

7. Contract Negotiations

Contract negotiations remain one of the most significant challenges community banks face in managing third-party relationships, particularly with core processors and other essential service providers. Community banks often have limited leverage to negotiate contractual provisions, while the cost and operational complexity of transitioning to another provider may substantially restrict their available alternatives.

We appreciate the Board's recognition of these challenges and its acknowledgement that banks may reasonably proceed with a third-party relationship even when preferred contractual terms cannot be obtained.

We recommend that the Board:

- **Reinforce Risk-Based Contract Negotiations**. Clarify that community banks should retain discretion to identify and prioritize contractual provisions based on the risk presented by individual relationships. No particular contractual provision should be universally expected.
- **Recognize Limited Negotiating Leverage**. Confirm that supervisory assessments should consider a bank's reasonable efforts to negotiate appropriate protections, available alternatives, mitigating controls, and documented acceptance of residual risk. Examiners should evaluate whether material contractual risks are appropriately managed rather than whether every preferred contractual provision was obtained.

- **Strengthen Oversight of Core Service Providers.** We appreciate the September 2026 interagency statement addressing supervisory oversight of core service providers. We encourage the Board and federal banking agencies to continue addressing provider practices that materially limit community banks' ability to manage risk, including unreasonable restrictions on data access, excessive deconversion fees, and contractual limitations that impede a bank's ability to transition to another provider. We also encourage the agencies to share relevant, non-confidential findings from the November 2025 Request for Information concerning community banks' relationships with essential service providers.
- **Support Collaborative Due Diligence and Negotiations.** Work with appropriate federal agencies to provide clarity regarding permissible collaborative activities among community banks, including shared due diligence efforts and collective contract negotiations through consortia or trade associations, consistent with applicable antitrust laws.

8. Deposit Placement Networks

We support including deposit placement networks as an additional vendor category. Many community banks utilize these networks to manage liquidity, facilitate deposit placement, and offer customers access to expanded FDIC deposit insurance coverage.

We recommend that the Guide provide practical, illustrative considerations addressing the unique characteristics of these relationships including:

- **Operational resilience.** The potential impact of network disruptions on deposit transactions, liquidity management, and continuity of services, based on the nature and significance of the bank's participation.

- **Regulatory Compliance.** Applicable deposit insurance recordkeeping requirements, reciprocal and brokered deposit regulations, and other relevant obligations, recognizing that requirements vary depending on the structure of the arrangement.

- **Financial resilience.** The financial condition and operational stability of the network operator and other material parties, where relevant to the bank's exposure.

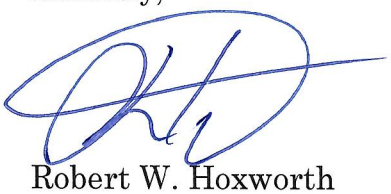
- **Customer communication.** Appropriate disclosure of deposit insurance coverage and communication of the program features, limitations, and customer responsibilities.

We recommend that these considerations remain illustrative rather than prescriptive. Participation in a deposit placement network should not, by itself, establish a presumption of heightened risk or require standardized documentation or monitoring practices. The scope of due diligence and ongoing monitoring should reflect the risks presented by the specific arrangement.

First National Bank Texas appreciates the Board's efforts to develop a practical, risk-based resource that recognizes the unique challenges community banks face in managing third-party relationships. We believe the proposed Guide represents a meaningful opportunity to strengthen third-party risk management while allowing banks the flexibility to tailor their programs to their individual risk profiles, operational complexity, and business needs. We encourage the Board to collaborate with other federal banking agencies to make this valuable resource available to all community banks.

We appreciate the Board's consideration of these recommendations and its continued commitment to supporting safe, sound, and appropriately tailored third-party risk management practices.

Sincerely,



Robert W. Hoxworth

901 E Central Texas Expressway P.O. Box 937 Killeen, Texas 76541