November 16, 2026

Via Electronic Submission

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 1E-216
Washington, DC 20219
Docket ID OCC-2026-0793

Jennifer M. Jones
Deputy Executive Secretary
Attention: Comments, ZRIN 3064-ZA58
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Benjamin W. McDonough
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Docket No. OP-1881

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
Docket No. NCUA-2026-1684

Re: Proposed Third-Party Risk Management Guidance (OCC: Docket ID OCC-2026-0793, RIN 1557-ZA18; Board: Docket No. OP-1881; FDIC: ZRIN 3064-ZA58; NCUA: Docket No. NCUA-2026-1684, RIN 3133-ZA54)

To Whom It May Concern:

Introduction

The Financial Data and Technology Association of North America ("FDATA") appreciates the opportunity to comment on the proposed interagency third-party risk management guidance (the "proposal" or "proposed guidance")[1] issued by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA") (collectively, the "agencies"). FDATA is North America's leading trade association dedicated to open finance and consumer-permissioned access to financial data. Its members provide digital banking, payments, credit, savings and investment, and financial management services to more than 100 million consumers and small and medium-sized businesses in the United States. While some of FDATA's members do work with depository institutions in various service provider capacities – and accordingly adhere to prudential third-party risk management ("TPRM") expectations in those circumstances – *all* of FDATA's members depend on customer-permissioned data access in their capacities as *the customer's representative,* consistent with

[1] Proposed Third-Party Risk Management Guidance, 91 Fed. Reg. 58536 (Sept. 15, 2026).

consumers' rights under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act"). As such, FDATA members have unique insight into how the agencies' TPRM guidance is applied (and misapplied) in practice.

FDATA welcomes the proposed guidance's risk-based, tailored approach and the agencies' recognition, consistent with Executive Order ("EO") 14405,[2] that partnerships between banking organizations and technology firms benefit institutions and their customers. FDATA is particularly supportive of the distinction the proposal draws between the core services a banking organization procures to support its own operations and data access a customer directs. Without that distinction, third-party risk management could become a barrier to consumer adoption of innovative products and services, and prevent small banks and credit unions from remaining competitive with the largest banks.

FDATA's principal recommendations are that the agencies:

1. Clearly state in the text of the final guidance, rather than in footnotes, that customer-permissioned data access does not by itself create a third-party relationship,[3] whether or not a written agreement governs it, and that such connections are more appropriately managed through cybersecurity risk management;
2. Confirm that information security, governed by the Gramm-Leach-Bliley Act ("GLBA"), is the applicable framework for consumer-permissioned data access, and define key terms such as "critical data" and "appropriately segmented";
3. Refrain from making a written agreement a dispositive test for the presence of a third party relationship (footnote 9 of the proposal), and build any list of high-risk characteristics (footnote 15 of the proposal) on the magnitude and likelihood of harm, recognizing that access through an application programming interface ("API") reduces risk;
4. Confirm that the guidance provides no basis for denying, degrading, or conditioning consumer-permissioned data access under Section 1033 of the Dodd-Frank Act, and coordinate with the Consumer Financial Protection Bureau ("CFPB"); and
5. Permit institutions to rely on recognized standards, certifications, and shared assessments as a meaningful input to due diligence, with conformance to a recognized standard creating a rebuttable presumption that the information security element is satisfied.

---

[2] Exec. Order No. 14405, Integrating Financial Technology Innovation into Regulatory Frameworks, 91 Fed. Reg. 30475 (May 22, 2026).

[3] For the purposes of this letter, "third party" and "third-party relationship" carry the meaning given in the proposed guidance: a business arrangement between a banking organization and another party for products, services, or other activities that support the banking organization. Importantly, a firm that a consumer has authorized to access the consumer's own data is not a "third party" in that sense; this letter refers to such a firm as an "authorized representative."



FDATA offers these comments in a spirit of support and collaboration and stands ready to meet with agency staff to discuss them.

Risk-Based and Proportionate Approach

FDATA supports the agencies' shift toward a risk-based and proportionate framework and agrees that risk should be assessed by the magnitude and likelihood of harm arising from a relationship rather than the category of third-party activity. Proportionality, however, works only where risk assessments rest on objective, articulable criteria. Otherwise, materially similar relationships attract divergent expectations unrelated to the risk presented.

A customer-authorized representative does not present the risks this framework was designed to address. Such a provider performs no banking function on an institution's behalf; it merely serves the institution's customers directly, and at their direction. FDATA therefore asks the agencies to confirm that customer-authorized providers will not be treated as higher risk by default.

FDATA also encourages the agencies to keep the final guidance technology neutral. A framework that focuses on the magnitude and likelihood of harm and the controls in place, rather than on the technology a third party uses, will remain durable as technology evolves, and will give market participants the necessary predictability. Where a particular technology warrants additional attention, separate guidance or bulletins advising supervised entities may be appropriate, so long as they do not conflict with final interagency guidance.

Scope of the Guidance: Customer-Directed Access Is Not a Third-Party Relationship

Customer-permissioned data access is not a third-party relationship, and the final guidance should clearly say so. The proposal already points in this direction. FDATA welcomes the agencies' acknowledgment in footnote 12 that a third party with access to systems "that do not hold critical data and are appropriately segmented is not necessarily higher risk," and that such risks may be managed "primarily through safe and sound cybersecurity risk management rather than through extensive third-party risk management."

The statutory framework supports the same conclusion. The agencies' authority under the Bank Service Company Act ("BSCA") extends to services a banking organization "causes to be performed for itself, by contract or otherwise."[4] That relationship, rather than a third party's connection to an institution's systems, defines the proper scope of this guidance. A data access platform retrieves the information a customer has asked to share and transmits it to the provider the customer has chosen. It does so on the customer's authorization, not under a contract to perform services for the bank. When a customer directs a provider to access the customer's own

[4] 12 U.S.C. § 1867(c).

data, the banking organization has caused nothing to be performed for itself. Importantly, relationships outside that scope are not unregulated. Congress assigned the framework for consumer financial data access to the CFPB under Section 1033 of the Dodd-Frank Act, while the GLBA sets information security standards addressing the risks such access presents to banking organizations.[5]

Absent such clarity in the text of the guidance, third-party risk management guidance can be invoked to justify diligence, audit, and contractual requirements on customer-authorized representatives unrelated to the risk presented. This risk is structural rather than a reflection of any institution's intent: where assessment rests entirely on the judgment of a party that may compete for the same customer, an undefined standard will tend toward restrictive outcomes.

FDATA therefore urges the agencies to state in the text of the final guidance that a third-party relationship arises only where a banking organization engages another party to provide products, services, or activities that support the institution. The final guidance should also confirm that an agreement, written or otherwise, governing customer-permissioned data sharing does not by itself create such a relationship. The principles the proposal now places in footnotes 9 and 12 should be elevated into the text of the guidance itself, where examiners and institutions will apply them.

This position is consistent with the view of the banking industry. In its comment letter to the OCC on community banks' engagement with core service providers, the American Bankers Association stated that where a bank and a data aggregator establish contractual criteria for access to customer-permissioned data, "this arrangement does not make the aggregator a third-party service provider to the bank."[6]

Independent Data Recipients and Subcontractors

A customer-authorized data recipient should not be presumed to be a banking organization's third party, or a bank service provider's subcontractor, solely because a shared customer directs data to that recipient through an aggregator. Banking organizations should evaluate whether the recipient performs an activity that the banking organization or its service provider has engaged it to perform on the institution's behalf. An independent application serving the customer does not become part of an outsourced bank service merely by receiving data through that connection. Nor should the guidance imply a transfer of legal responsibility among the bank, the aggregator, and the independent recipient.

---

[5] 12 U.S.C. § 5533; 15 U.S.C. § 6801 et seq.; 16 C.F.R. part 314.

[6] American Bankers Association, Comment Letter on Request for Information Regarding Community Banks' Engagement with Core Service Providers and Other Essential Third-Party Service Providers, Docket ID OCC-2025-0537, at 13 (Jan. 27, 2026).



For relationships that constitute genuine subcontracting, FDATA supports the proposal's treatment of subcontractor oversight, under which the use of subcontractors "alone does not typically create an independent third-party relationship or create a presumption of direct banking organization oversight of any subcontractors." FDATA asks the agencies to confirm that a banking organization may assess the primary provider's subcontractor oversight program according to the risk of the relationship, rather than reviewing each subcontractor directly.

Information Security and Customer-Authorized Access

When a customer authorizes a provider to access the customer's data, rather than a banking organization procuring a service from that provider, the institution's legitimate interest is the security of its systems and customer information. The GLBA sets the applicable expectations, and cybersecurity risk management, including authentication of the requesting party, access controls, segmentation, monitoring, and incident response, is the appropriate tool for these connections. Such oversight should be proportionate to the sensitivity of the data accessed and the method of access, rather than uniform across all consumer-permissioned access.

To be clear, FDATA supports holding firms that access customer financial data to rigorous and consistent information security expectations. FDATA members treat data security as fundamental to their businesses, are subject to the GLBA and its implementing standards, and meet those expectations today.

FDATA asks the agencies to confirm that any limitation or condition an institution places on customer-permissioned access must rest on a specific, identified risk and apply consistently across similarly situated providers. Consistent with the federal banking agencies' removal of reputation risk from their supervisory programs, such limitations should not rest on reputational considerations.[7] This reflects FDATA's long-standing position that restrictions on customer-directed access should be limited to specific, identified risks, such as suspected fraud or unauthorized access.

Request for Clarity on Key Terms

The agencies' tailored approach can be applied consistently only if institutions and examiners understand its key terms the same way. Several of those terms remain undefined or unclear, so each institution will interpret them differently, giving consumers uneven access depending on where they bank. FDATA requests clarification of the following:

---

[7] See Prohibition on the Use of Reputation Risk by Regulators, 91 Fed. Reg. [18286] (Apr. 10, 2026) (OCC and FDIC final rule); Board of Governors of the Federal Reserve System, Press Release, Federal Reserve Board Announces That Reputational Risk Will No Longer Be a Component of Examination Programs in Its Supervision of Banks (June 23, 2025).

- **Critical data:** The proposal suggests the risk of a connection turn on whether the systems it reaches hold "critical data," but does not say what makes data critical. FDATA asks the agencies to define the term as data whose compromise would materially impair a banking organization's operations or substantially harm its customers, and to confirm that customer data shared at the customer's direction does not qualify on that basis alone.
- **Appropriately segmented:** The proposal gives no indication of what degree of segmentation suffices. FDATA asks the agencies to confirm that segmentation is appropriate where a connection cannot reach critical data, as with a dedicated data access API that is separated from an institution's core systems, and that established security frameworks may be used to demonstrate it.
- **Extensive third-party risk management:** Footnote 12 allows lower-risk connections to be managed through cybersecurity risk management rather than "extensive third-party risk management," but the proposal does not describe what the former involves in practice. FDATA asks the agencies to provide illustrative examples, such as authentication of the requesting party, access controls, segmentation, and monitoring; without them, institutions are likely to default to the full framework, undermining the intent of the proposal.
- **Activities that support the banking organization:** This phrase sets the scope of the guidance. FDATA asks the agencies to confirm that it covers activities performed on an institution's behalf, not services provided directly to a customer, as a broader reading would capture any authorized representative a customer chooses.
- **Clear consideration:** The guidance treats the absence of clear consideration as a reason an activity is unlikely to be a third-party relationship. FDATA asks the agencies to confirm that an agreement setting the terms of consumer-permissioned access, without payment for services to the institution, is not consideration.

Access Methods and Risk Indicators

In footnote 15 of the proposal, the agencies ask whether the guidance should include a list of characteristics that generally indicate a high-risk relationship. To the extent that it produces such a list, FDATA asks the agencies to recognize that API-based access generally reduces the risk of a data connection, because it allows an institution to authenticate the requesting party, limit the data shared to what the customer has authorized, and revoke access.

Connectivity, maturity, size, and business model do not belong on any such list. A connection to an institution's systems is not itself an indicator of elevated risk, and treating recent entrants or smaller firms as higher risk would conflict with the agencies' own recognition that partnerships with technology firms benefit institutions and their customers, and with EO 14405.

In footnote 9 of the proposal, the agencies ask whether the guidance should apply only to third parties subject to a written agreement. FDATA cautions against making an agreement's existence the test for scope. API-based access is typically governed by a written agreement, while credential-based access generally is not, so such a test would apply the full framework to the access method that gives institutions the most control. It would also discourage the transition to APIs, leaving customers of smaller institutions that do not yet offer them reliant on credential-based access. While FDATA agrees that the absence of a written agreement makes a third-party relationship unlikely, the presence of one should not indicate the opposite. The final guidance should make clear that consumer-permissioned access is outside scope whether or not an agreement governs it.

Due Diligence and Onboarding Burden

A firm serving customers of many institutions answers materially similar diligence requests from each of them. The more institutions FDATA's members partner with, the more resources they must devote to providing the same information to each one during onboarding, major product updates, or regular audits. That cost falls hardest on smaller institutions and smaller providers, with limited benefit to safety and soundness.

The proposal's due diligence elements, such as financial condition, business experience and key personnel, staffing, legal and regulatory compliance, insurance, and information security and cybersecurity, apply "as applicable." To the extent an institution conducts due diligence on a connection that accesses customer data at the customer's direction, FDATA asks the agencies to confirm that information security and cybersecurity are the applicable elements.

FDATA welcomes the agencies' recognition that an institution may consider a third party's regulatory status and obligations as part of its risk assessment. FDATA asks that the final guidance confirm that existing supervision, recognized certifications, and shared assessments may be relied upon rather than duplicated. FDATA recognizes, as the agencies note, that supervisory and regulatory schemes may differ materially between entity types. Where the relevant scheme is the GLBA, however, including the Federal Trade Commission's Safeguards Rule, it addresses the very information security risks at issue and does serve to mitigate them. The final guidance should affirm this.

Where a provider's profile limits the diligence an institution can perform, such as a newer firm without a multi-year financial history, the final guidance should confirm that other factors may offset those limitations and that an incomplete file is not by itself grounds for declining the relationship. In addition, proportionality should apply to the frequency of review as well as its depth, with reassessment driven by changes in the relationship rather than a fixed calendar.

Coordination with Section 1033

The proposal confirms that it "does not set forth enforceable standards or prescriptive requirements," consistent with the agencies' 2021 rule codifying that supervisory guidance does not have the force and effect of law.[8] Guidance of that kind does not alter obligations established by statute. Section 1033 of the Dodd-Frank Act reflects Congress's determination regarding consumer access to financial data, and FDATA asks the agencies to confirm that this guidance provides no basis for denying, degrading, or conditioning access a consumer has authorized.

FDATA encourages the agencies to coordinate with the CFPB, which Congress directed under Section 1033 of the Dodd-Frank Act to prescribe rules governing consumer access to financial data, particularly as the CFPB reconsiders its Personal Financial Data Rights rule. Absent such coordination, institutions and the examiners who review them may come to treat third-party risk management expectations as the operative standard for consumer-permissioned data access, a role this guidance was not designed to serve. A consumer's ability to share their data would then depend on each institution's risk assessment rather than on the framework Congress directed.

Shared Assessments and Standard-Setting Organizations

FDATA welcomes the agencies' recognition that banking organizations may draw on co-ventures, consortia, standard-setting organizations, and other external resources to manage third-party risk. Such arrangements can reduce duplicative review, particularly for institutions that lack the capacity to conduct it alone. FDATA agrees with the agencies that reliance on these arrangements does not displace an institution's own judgment, and that risk management must continue to reflect the institution's particular circumstances.

FDATA asks the agencies to confirm that an institution may rely on a shared assessment or recognized standard as a meaningful input to its risk assessment, rather than as supplementary material that leaves the underlying review unchanged. The weight given to such evidence should depend on factors such as timeliness, credibility, relevance to the risk being assessed, and transparency about its scope and limitations. For risks the evidence covers, institutions should be able to rely on the work already performed and direct any additional review to material gaps or relationship-specific exposures.

Specifically, where an institution conducts due diligence, conformance with a recognized technical and security standard for consumer-permissioned data access, or a current independent certification against such a standard, should create a rebuttable presumption that the information security element is satisfied. Evidence developed through a provider's own oversight of the firms that receive data through it should also be considered where it addresses the security and governance of consumer-permissioned access. No single certification, standard-setting

[8] 91 Fed. Reg. at 58539–40; Role of Supervisory Guidance, 86 Fed. Reg. 18173 (Apr. 8, 2021).

organization, or proprietary assessment should become mandatory; standards should support interoperability, diverse participation, and objective criteria.

Practical Contracting and Residual Risk

FDATA has long advocated a transition away from reliance on complex bilateral data access agreements. Individually negotiated bilateral agreements are an inefficient way to handle consumer-permissioned data access because they lack uniformity, transparency, and insight. Requiring every institution to execute an agreement with every data access platform creates an uneven playing field. Some customers end up with more data rights than others, based on the terms of an agreement their bank executed and to which they have no visibility.[9]

The final guidance should therefore confirm that it does not require, or create a supervisory expectation of, a data access agreement between a banking organization and a customer-authorized representative as a condition of access a consumer has authorized. Where institutions and providers choose to enter into such agreements, or where a banking organization procures services under a contract, the following principles should apply.

Where an institution can obtain credible evidence through an independent assessment or shared review, as discussed above, the final guidance should confirm that it may focus contractual negotiations on uncovered risks and the circumstances of its own relationship. In such cases, standard-form terms and appropriately scoped service levels should generally suffice, with targeted audit or monitoring provisions reserved for material risks the available evidence does not address. Broad indemnification provisions should not be treated as a substitute for effective security, incident response, operational resilience, data protection, or, where relevant, customer-funds controls.

FDATA appreciates the agencies' acknowledgment that they "do not expect banking organizations to eliminate third-party risk" and that "[s]ome residual risk is unavoidable." This acknowledgment allows banking organizations to document and accept reasonable residual risk, rather than treating an inability to obtain every requested term as a reason to decline a relationship.

FDATA also asks that the final guidance clarify that it does not itself reallocate liability among the parties to a relationship. As the agencies rescind and replace existing guidance and

[9] FDATA, Comment Letter on Proposed Interagency Guidance on Third-Party Relationships: Risk Management, Docket ID OCC-2021-0011 (Oct. 2021); FDATA, Comment Letter on Personal Financial Data Rights Reconsideration, Docket No. CFPB-2025-0037 (Oct. 21, 2025).

supplemental resources, FDATA encourages them to preserve useful operational safeguards and to explain how institutions may apply the new flexibility consistently.

Conclusion

FDATA supports the agencies' effort to establish a proportionate, risk-based framework for third-party risk management. The clarifications requested in this letter would preserve the framework's focus on material risk while ensuring that the final guidance does not reach the consumer-permissioned data access on which consumers, and the providers they choose, rely every day. Clear expectations also serve the agencies' own objectives: institutions of every size can partner confidently, and risk management resources can be directed to the relationships that present real risk.

Thank you for considering our comments. FDATA and our member companies welcome the opportunity to provide further insights and to serve as a resource to the agencies as they finalize this guidance.

Sincerely,



Steve Boms
Executive Director