



October 5, 2026

The Honorable Jonathan V. Gould
Comptroller of the Currency
Office of the Comptroller of the Currency
Attn: Comment Processing
400 7th St., SW
Washington, DC 20219

Re: Response to Notice of Proposed Rulemaking on the Disclosure of Confidential Supervisory Information

Dear Comptroller Gould,

On behalf of the American Fintech Council (AFC),¹ I submit this comment letter in response to the Office of the Comptroller of the Currency's (OCC) Notice of Proposed Rulemaking regarding the availability of OCC information, including the disclosure of confidential supervisory information (CSI) by OCC-supervised entities (Proposed Rulemaking).² AFC appreciates the OCC's effort to replace a disclosure framework that can impede legitimate information sharing with a more calibrated structure that permits supervised entities to disclose CSI in defined circumstances while preserving the confidentiality necessary for candid supervision.

AFC is a standards-based organization and the largest and most diverse trade association representing financial technology companies and innovative banks. On behalf of more than 150 member companies and partners, AFC promotes a transparent, inclusive, and customer-centric financial system by supporting responsible innovation in financial services and encouraging sound public policy. AFC's membership includes innovative banks, payments providers, technology companies, compliance providers, and other financial services firms that operate within complex bank partnership and third-party risk management frameworks. These institutions possess direct experience with the practical consequences that restrictions on supervisory information can have for due diligence, remediation, governance, corporate transactions, and the formation and oversight of responsible bank fintech partnerships.

AFC supports the OCC's effort to modernize its approach to CSI disclosure, particularly where the existing framework can impede legitimate information sharing necessary for effective due diligence, risk management, corporate governance, and responsible third-party relationships. In finalizing the rule, the OCC should ensure that the resulting framework provides regulated

¹ American Fintech Council's (AFC) membership spans banks, non-bank lenders, payments providers, EWA providers, loan servicers, credit bureaus, and personal financial management companies.

² Office of the Comptroller of the Currency, "OCC Rules Regarding the Availability of OCC Information," *Federal Register* 91, no. 149 (August 5, 2026): 50610–50642.

institutions with sufficient flexibility to share CSI where a legitimate business or supervisory purpose exists, while maintaining safeguards proportionate to the sensitivity of the information and the circumstances of the disclosure. In particular, AFC encourages the OCC to adopt a framework that facilitates appropriate information sharing throughout the full life cycle of bank relationships and corporate transactions, avoids replacing prior approval requirements with unnecessary procedural burdens, and provides clear pathways for appropriately structured aggregated analysis that can enhance understanding of supervisory practices without compromising institution-specific confidential information.

I. AFC Supports Expanding Permissible Business-Purpose Disclosures to Strengthen Due Diligence, Risk Management, and Responsible Bank Partnerships

Modern banking relationships increasingly depend upon the ability of regulated institutions to exchange information with affiliates, prospective business partners, advisers, and specialized service providers before a relationship is formally established. Effective due diligence often requires decision makers to understand material supervisory concerns, remediation obligations, operational weaknesses, compliance limitations, and other matters that may bear directly on whether a contemplated relationship can be structured consistently with applicable regulatory expectations. For that flexibility to be meaningful, however, the final rule must address both the range of relationships eligible for disclosure and the circumstances under which relevant information may be shared. A framework that fails to accommodate contemporary banking relationships, or that becomes meaningfully more permissive only after those relationships have been established, risks withholding important information at precisely the stage when prudent risk management requires it most.

As a threshold matter, the effectiveness of the proposed disclosure framework depends upon whether the definition of a service provider adequately reflects the structure and operation of contemporary bank-fintech partnerships. Although the proposed definition encompasses entities hired by or partnered with a supervised institution, its reliance on functions performed “for or on behalf of” the institution may create uncertainty for arrangements involving integrated and reciprocal responsibilities. Bank-fintech partnerships frequently involve program managers and other entities that coordinate directly with supervised institutions to deliver financial products and services, administer customer relationships, and perform significant operational, technological, and compliance functions. These relationships cannot always be characterized as conventional arrangements in which a vendor performs discrete services on behalf of a bank. Accordingly, the final rule should expressly recognize that qualifying service providers may include program managers and other bank partners whose responsibilities are integrated with those of the supervised institution, regardless of whether the relationship conforms to a traditional vendor model.

AFC therefore encourages the OCC to revise the proposed definition to expressly encompass these arrangements or adopt the broader alternative definition contemplated in the Proposed Rulemaking. The alternative definition, which focuses on contractual relationships involving products, services, advisory functions, and technological infrastructure supporting the institution’s financial activities, offers a more functional approach to identifying entities with legitimate operational responsibilities. Whichever approach the OCC adopts, the final rule should

clarify that the relevant inquiry is the substantive nature of the relationship and the functions performed, rather than the contractual characterization of the parties or whether services flow exclusively in one direction. Such clarification would ensure that the proposed disclosure exceptions remain effective as banking relationships and financial service delivery models continue to evolve.

The proposed exclusion of financial counterparties from the service provider definition presents a related concern. Although a distinction between traditional financial counterparties and entities performing operational functions may be appropriate, a categorical exclusion risks overlooking relationships that exhibit characteristics of both. In specialty finance and other bank partnership arrangements, a financial counterparty may also undertake loan servicing, compliance, operational administration, or other responsibilities that require ongoing coordination with the supervised institution. The existence of a financial relationship should not, by itself, preclude an entity from qualifying as a service provider when its substantive responsibilities otherwise satisfy the applicable criteria. Absent such clarification, institutions may be required to seek individualized OCC approval for disclosures involving established partners whose operational responsibilities and legitimate need for CSI are comparable to those of qualifying service providers.

To address this concern, AFC recommends that the OCC limit the financial counterparty exclusion to relationships that are predominantly transactional and do not involve ongoing operational integration or qualifying service functions. Alternatively, the OCC should establish a separate disclosure exception for financial counterparties that maintain an ongoing contractual relationship with the supervised institution, demonstrate a legitimate business or supervisory need for the information, and satisfy appropriate confidentiality requirements. At a minimum, the final rule should provide clear criteria for classifying hybrid relationships and confirm that an entity's status as a financial counterparty does not independently disqualify it from receiving CSI in connection with separate qualifying service functions. This functional approach would provide greater regulatory certainty while preserving appropriate limitations on the disclosure of sensitive supervisory information.

Beyond clarifying which relationships qualify for the proposed exception, the OCC should ensure that permissible disclosures extend to prospective service providers where an OCC-supervised institution reasonably determines that disclosure is necessary or appropriate to conduct due diligence, evaluate risk, structure a potential relationship, or assess whether a prospective partner can satisfy the institution's regulatory and operational requirements. Limiting disclosure authority to relationships that have already been contractually established would invert the ordinary sequence of third-party risk management. Banks ordinarily evaluate a prospective partner's capabilities, controls, compliance posture, and risk profile before entering into an agreement. Where CSI is materially relevant to that assessment, institutions should be permitted to consider it, subject to appropriate confidentiality protections and need-to-know limitations.

The importance of timely disclosure extends in both directions, particularly where a prospective relationship involves integrated operational or compliance responsibilities. In those circumstances, a bank may need access to information concerning supervisory findings,

remediation responsibilities, operational resilience, or compliance deficiencies before determining whether to proceed. Permitting such disclosure only after execution of a contract would place the prospective bank in the position of making a consequential risk decision without information that may materially affect that judgment. Allowing relevant supervisory information to inform diligence before the institution assumes contractual, operational, or reputational exposure would reinforce the reciprocal information sharing necessary for responsible bank-fintech partnerships.

Beyond third-party relationships, the final rule should also provide sufficient flexibility for disclosures made in connection with legitimate corporate transactions. Merger and acquisition activity, investments, strategic combinations, changes in control, and similar transactions frequently require sophisticated diligence involving legal, compliance, operational, and supervisory considerations. Where CSI bears materially on the risks associated with a transaction, prospective counterparties and their professional advisers should be permitted to receive that information under appropriately tailored confidentiality protections. Restricting access to such information can impair the ability of parties to identify supervisory concerns, appropriately value regulatory risk, negotiate contractual protections, and determine whether a transaction should proceed at all.

Providing meaningful access to supervisory information during transaction diligence also requires greater clarity regarding the scope of information that qualifying counterparties may receive. Subject to applicable safeguards, permissible disclosures should encompass information reasonably necessary to evaluate the institution's supervisory condition, including reports of examination, supervisory ratings, outstanding supervisory findings, remediation plans, relevant supervisory correspondence, and pending enforcement matters. The final rule should also recognize that customary representations, warranties, covenants, and indemnification provisions may appropriately address the institution's regulatory condition and remediation obligations without disclosing the specific contents of CSI. As such, AFC encourages the OCC to distinguish between contractual provisions that improperly disclose confidential supervisory findings or purport to dictate supervisory outcomes and those that allocate regulatory risk through appropriately structured transaction protections. Additionally, the OCC should further clarify that good faith negotiations may be established through a bona fide expression of transactional interest and appropriate confidentiality commitments, without requiring the parties to have negotiated material terms or executed a definitive transaction agreement.

The need for timely access to supervisory information should also extend to prospective senior executive officers and other individuals assuming significant governance responsibilities. Incoming leaders may be expected to assume responsibility for remediation efforts, supervisory commitments, governance deficiencies, or other matters that cannot be responsibly evaluated without some understanding of the institution's supervisory posture. The final rule should therefore permit disclosure where the information is reasonably necessary for the candidate to assess the responsibilities associated with the position and where access is subject to appropriate confidentiality obligations. The OCC should further clarify that disclosure may occur during preliminary discussions with a serious prospective candidate, before formal interviews commence, where the institution has determined that access is reasonably necessary to evaluate the contemplated appointment and appropriate confidentiality and governance safeguards have

been satisfied. More broadly, the OCC should construe permissible business purposes with sufficient breadth to reflect the range of legitimate functions through which regulated institutions manage risk and satisfy supervisory expectations. Qualifying purposes should include, among other activities, third-party due diligence and monitoring, enterprise risk management, internal and external audit, legal and regulatory compliance, corporate governance, transaction evaluation, operational resilience, cybersecurity assessment, and remediation planning. Illustrative examples could provide useful clarity without converting a flexible standard into an exhaustive list that may quickly become outdated.

Taken together, these considerations underscore the importance of a disclosure framework that accommodates functionally similar relationships without imposing unnecessary distinctions based on contractual form or recipient classification. Whether the recipient is an established or prospective service provider, a hybrid financial counterparty performing qualifying operational functions, a transaction counterparty, a senior executive candidate, an affiliate, or a professional adviser, the relevant considerations should include the recipient's legitimate need for the information, the business or supervisory purpose served by the disclosure, and the confidentiality protections applicable to its use. Applying these principles consistently, while preserving safeguards appropriate to each disclosure context, would provide greater regulatory certainty and enable institutions to manage risk across the full range of their business relationships.

Finally, greater consistency among the federal banking agencies would materially improve the administrability of CSI requirements for institutions operating across multiple supervisory regimes. Banks, fintech companies, service providers, and advisers frequently interact with institutions subject to different prudential regulators, and materially divergent CSI disclosure rules can complicate otherwise routine diligence and risk management. Although each agency retains distinct statutory and supervisory responsibilities, greater alignment on core concepts such as permissible recipients, legitimate business purposes, confidentiality safeguards, and treatment of prospective relationships would reduce unnecessary fragmentation without diminishing supervisory protections.

II. AFC Supports Proportionate Confidentiality and Recordkeeping Safeguards that Protect CSI Without Recreating Prior-Approval Burdens

The practical success of the final framework will depend substantially on whether its safeguards can be incorporated into ordinary legal, compliance, and third-party risk management processes. Confidentiality protections should remain rigorous where the sensitivity of the information warrants them, but the final rule should avoid transforming each authorized disclosure into a separate regulatory exercise. A framework that formally eliminates prior approval while replacing it with bespoke agreements, duplicative logs, individualized access schedules, and expansive attestations could preserve much of the administrative friction that the proposal is intended to alleviate.

As a starting point, a written confidentiality agreement provides an appropriate foundation for disclosures to external recipients. The final rule should, however, permit the required protections to be incorporated into existing nondisclosure agreements, engagement letters, service agreements, transaction confidentiality agreements, or other contractual instruments rather than

requiring a separate stand-alone CSI agreement. The relevant inquiry should be whether the governing agreement restricts use to the authorized purpose, prohibits unauthorized onward disclosure, confines access to individuals with a legitimate need to know, establishes appropriate treatment of the information when the authorized purpose concludes, and preserves the OCC's ability to enforce applicable restrictions. Allowing institutions to satisfy these substantive protections through documentation suited to the underlying relationship would provide meaningful safeguards without imposing unnecessary formalities.

Certain service provider provisions warrant additional refinement. In particular, requiring every service provider that receives CSI to acknowledge and consent to OCC regulation and enforcement to the same extent as if the relevant service were performed by the supervised entity, together with a separate acknowledgment of institution-affiliated party status, could create substantial contractual resistance without materially strengthening the confidentiality of the information. The OCC already possesses statutory authority to examine certain services performed for regulated depository institutions under the Bank Service Company Act. Consequently, receipt of CSI should not depend upon a contractual concession that could be understood to alter or enlarge the scope of otherwise applicable regulatory authority. For service providers already subject to OCC examination authority under the Bank Service Company Act or other applicable law, the final rule should permit a streamlined acknowledgment confirming the scope of that existing authority without requiring consent to regulation or examination equivalent to that of the supervised institution. Any required acknowledgment should be expressly limited to authority conferred by applicable law and should not operate as an independent contractual expansion of the OCC's jurisdiction.

Beyond ensuring that confidentiality agreements accurately reflect the OCC's existing supervisory authority, the final rule should provide sufficient flexibility for service providers to share CSI internally with personnel whose responsibilities are reasonably related to the underlying supervisory concern. In integrated bank-fintech partnerships, effective remediation frequently requires coordination among compliance, technology, product development, operations, and senior management personnel. Limiting access exclusively to individuals directly responsible for remediation may prevent other personnel with essential operational responsibilities from obtaining information necessary to identify underlying deficiencies, implement corrective measures, or prevent their recurrence. AFC therefore recommends permitting access by individuals with a reasonable need to know in connection with remediating the supervisory concern or managing the service provider's relationship with the supervised institution, subject to appropriate confidentiality and access controls. Such an approach would facilitate coordinated remediation without authorizing unrestricted internal dissemination of CSI.

Consistent with this functional approach to confidentiality and access controls, recordkeeping requirements should remain principles based and capable of being satisfied through records maintained in the ordinary course of business. A supervised entity should be permitted to demonstrate compliance through executed confidentiality provisions, access-control records, engagement documentation, due diligence materials, board or management records, and other documentation sufficient to identify the recipient, the general category of CSI disclosed, and the legitimate purpose for the disclosure. Requiring transaction-by-transaction legal analyses or separate entries each time an authorized recipient accesses CSI within the scope of an established

relationship would add substantial administrative burden without producing a corresponding supervisory benefit. For continuing relationships, a category-level record tied to the relevant recipient and authorized purpose should ordinarily provide an adequate compliance record.

For much the same reason, the final rule should avoid requiring a contractual appendix identifying every individual who may access CSI under a qualifying confidentiality agreement. Personnel assignments routinely change over the course of sophisticated legal, compliance, technology, audit, and consulting engagements. Institutions and their service providers generally manage those changes through role-based permissions, engagement teams, identity-management systems, and internal confidentiality controls. Requiring amendments to the underlying agreement whenever personnel are added or removed would convert an access-control obligation into an ongoing contracting exercise. A more functional approach would require the recipient to limit access to personnel with a legitimate need to know and to maintain records sufficient to demonstrate that those access controls are operating as intended.

Governance requirements should likewise reflect the nature and sensitivity of the particular disclosure. Board-level approval may be appropriate in especially consequential circumstances, including certain disclosures involving senior leadership candidates or significant strategic transactions. It should not, however, become a universal prerequisite for routine disclosures to service providers, affiliates, professional advisers, or other recipients acting within established business relationships. Institutions should retain the ability to allocate approval authority through risk-based governance structures that account for the sensitivity of the CSI, the identity of the recipient, and the purpose for which the information is being disclosed. Such an approach would preserve accountability while avoiding unnecessary delay and displacement of ordinary management responsibilities.

Finally, the OCC should reconsider categorical reliance on U.S. incorporation as a proxy for adequate confidentiality protection in the service provider context. Modern banking organizations frequently rely on global technology, cybersecurity, audit, data, and compliance firms whose corporate structure or personnel footprint may not conform neatly to a domestic-incorporation requirement, even where the institution can impose robust contractual, technical, and access controls. In particular, the final rule should distinguish between the jurisdiction of incorporation of an ultimate parent company and the location, legal structure, and operational responsibilities of the entity receiving CSI. A U.S.-based operating subsidiary of a foreign-incorporated company should not be categorically excluded where the relevant operations and personnel are subject to appropriate domestic legal and contractual safeguards. Accordingly, the OCC should adopt a more risk-sensitive approach that considers whether the recipient is subject to an enforceable agreement governed by U.S. law, maintains controls commensurate with the sensitivity of the CSI, and can comply with applicable return, destruction, and onward-disclosure restrictions, rather than relying exclusively on its jurisdiction of incorporation. The OCC would retain authority to restrict or condition disclosures where a particular jurisdiction, recipient, or arrangement presents heightened confidentiality or supervisory concerns.

III. AFC Supports Proportionate Confidentiality and Recordkeeping Safeguards that Protect CSI Without Recreating Prior-Approval Burdens

Aggregated analysis of supervisory information can provide meaningful insight into regulatory practices without revealing the confidential affairs of individual institutions. Trade associations, research organizations, and other qualified entities are uniquely positioned to identify recurring supervisory themes, areas of regulatory uncertainty, and broader implementation challenges that may not be apparent when supervisory information is viewed solely on an institution-by-institution basis. When appropriately structured, that analysis can improve the quality of public policy discussions and facilitate more informed engagement between regulators and supervised institutions.

Importantly, the usefulness of aggregated analysis would depend on whether the final framework provides a workable path for obtaining and analyzing relevant information. Authorization should therefore extend beyond circumstances in which information has already been reduced to a fully aggregated form before disclosure. In many cases, meaningful aggregation requires access to institution-specific information at the analytical stage so that recurring themes can be identified, compared, and synthesized. If a qualifying entity may receive only information that has already been aggregated by the supervised institutions themselves, the utility of the framework could be substantially diminished and the resulting analysis may fail to capture broader supervisory patterns. For that reason, the final rule should permit qualifying entities to receive institution-specific CSI for the limited purpose of producing aggregated analysis, provided that robust safeguards prevent disclosure of identifiable supervisory information in the resulting work product. Those safeguards should include appropriate confidentiality agreements, restrictions on secondary use, limitations on access to personnel engaged in the analysis, and a prohibition on publishing or otherwise disseminating information in a manner that would permit the identity of a particular supervised entity to be reasonably ascertained. This approach would protect the confidentiality of individual institutions while allowing aggregation to occur in a manner that is analytically meaningful.

At the same time, the OCC should avoid adopting an aggregation standard so restrictive that it effectively prevents useful analysis. A requirement that no institution could ever be identifiable under any conceivable set of circumstances may be difficult to administer and could discourage responsible entities from engaging in the very work the framework is intended to facilitate. A more practical standard would focus on whether the published or disseminated analysis is reasonably designed to prevent identification of a particular supervised entity, taking into account the size of the dataset, the degree of aggregation, the nature of the information, and the context in which the analysis is presented.

Similarly, the definition of qualifying not-for-profit entities should be sufficiently flexible to encompass organizations that engage in legitimate policy analysis, advocacy, research, and industry education. Trade associations frequently serve as intermediaries between supervised institutions and regulators by identifying common implementation challenges, synthesizing member experiences, and presenting policy recommendations informed by those experiences. Excluding such organizations, or subjecting them to unduly narrow eligibility criteria, could limit the practical value of the aggregation framework and reduce opportunities for constructive supervisory dialogue.

The final rule should also make clear that appropriately aggregated findings may be used in regulatory advocacy, comment letters, policy research, educational materials, and other forms of public engagement, so long as the underlying CSI remains protected. The ability to identify broader supervisory trends has limited value if organizations are unable to use those findings to inform discussions regarding regulatory policy and supervisory administration. Permitting responsible use of de-identified, aggregated conclusions would advance transparency without compromising the confidentiality interests the CSI framework is designed to protect.

Finally, the OCC should consider establishing a clear and administrable standard for when aggregated information no longer constitutes CSI for purposes of downstream use. Once information has been sufficiently de-identified and combined so that it no longer reveals, or reasonably permits the identification of, the supervisory affairs of a particular institution, continued treatment of that information as CSI may unnecessarily constrain its value for research and policy analysis. Providing greater certainty on that point would encourage responsible aggregation while preserving strong protections for institution-specific supervisory information.

* * *

AFC appreciates the OCC's effort to modernize a disclosure framework that no longer reflects the complexity of contemporary banking operations. The final rule should preserve the proposal's movement toward purpose-based information sharing while ensuring that the available exceptions are broad enough to function in real-world third-party relationships, corporate transactions, governance processes, and industry-wide analysis. In particular, AFC respectfully encourages the OCC to clarify the treatment of integrated bank-fintech partnerships and hybrid financial counterparties, permit appropriate disclosure during prospective third-party diligence, extend equivalent authority to parent holding companies where the same substantive safeguards apply, broaden transaction and leadership-candidate exceptions where a legitimate need is demonstrated, streamline confidentiality and recordkeeping requirements, and preserve a durable pathway for aggregated analysis and advocacy.

These refinements would reduce unnecessary administrative friction, improve risk identification and remediation, and promote more informed decision making without compromising safety, soundness, or the confidentiality and integrity of the supervisory process. AFC welcomes continued engagement with the Office of the Comptroller of the Currency and stands ready to serve as a resource as the agency considers next steps in this rulemaking.

Sincerely,



Ian P. Moloney
Chief Policy Officer
American Fintech Council