Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

September 11, 2026

Joint Statement on Community Banks' Engagement with Core Service Providers

The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement to provide clarity on their risk-based supervision of certain services provided to community banking organizations (CBOs).

The agencies believe there is a need for additional clarification regarding a subset of CBOs' third-party relationships, based on the agencies' supervision of CBOs and their service providers, and reinforced by the agencies' outreach to CBOs and other relevant stakeholders.[1] This subset consists of third parties that provide the critical systems applications and infrastructure that support the operation and essential functions of one or more of a CBO's lines of business, including, for example, through the provision of transaction processing, account management, payments processing, customer relationship management, compliance and reporting, online banking, and other material functions. For purposes of this statement, the agencies refer to these entities broadly as core providers. These relationships are essential to the safe and sound operations of CBOs, yet certain core provider business practices and market dynamics may pose obstacles to a CBO's ability to efficiently and effectively identify, assess, and address the attendant risks.

[1] *See*, *e.g.*, OCC, Request for Information Regarding Community Banks' Engagement With Core Service Providers and Other Essential Third-Party Service Providers, 90 FR 54882 (Nov. 28, 2025).

As such, the agencies are issuing this statement to address (1) select aspects of how CBOs engage with core providers, (2) the extent to which the agencies will take these aspects into consideration when determining the level of supervisory oversight of core provider services, and (3) the agencies' supervisory and enforcement authorities where a core provider engages or causes a CBO to engage in unsafe or unsound practices or violations of law or regulation.

Background

CBOs are vital to the strength of the U.S. economy. To support their role, the agencies are committed to prioritizing reforms targeted at reducing the supervisory and regulatory burden for CBOs and tailoring supervisory and regulatory frameworks to better fit their business models and unique risks. These reforms will better position CBOs to serve their communities and drive economic growth.

Most CBOs rely on core providers to support their ability to operate effectively and compete in today's rapidly evolving marketplace. The agencies recognize the significant benefits these relationships offer. Core providers represent CBOs' most material, complex, and highest-risk third-party relationships. A core processing platform's availability, integrity, and security are vital to nearly all banking operations. Beyond the core processing platform, these providers often deliver additional services such as payment processing, card programs, loan management systems, or online banking. While use of core providers can create operational efficiencies, it also creates heightened risk, especially if the core provider experiences financial distress, operational failures, or security compromises.

The agencies are also aware that a significant percentage of the core provider market is represented by just a few large providers, which limits CBOs' negotiating power. Given these constraints, CBOs report they often experience challenges obtaining reasonable due diligence

information, negotiating contract terms, or conducting effective ongoing monitoring. These challenges may make it difficult for CBOs to hold core providers accountable for delivering quality services.

Risk-Based Supervision of Core Providers

Each banking organization is responsible for operating in a safe and sound manner and in compliance with applicable laws and regulations. An important aspect of this responsibility is adopting third-party risk management practices that are commensurate with the organization's size, complexity, and risk profile and with the nature of its third-party relationships.

As part of standard supervisory processes, the agencies examine a banking organization for its management of third-party risk and its operations involving third parties. The agencies also conduct risk-based examinations of certain third parties' provision of services, including those of certain core providers.[2] These supervisory activities are prioritized based on the risks that core providers pose to their client banking organizations and may include joint examinations with other financial regulators and targeted or full-scope examinations of varying frequency.[3]

Based on the agencies' supervisory experience and stakeholders' input, the agencies have determined that core provider business practices that unreasonably limit CBOs' ability to conduct due diligence and ongoing monitoring or to negotiate contract terms that address their business needs are associated with greater risks to the CBOs and a reduced ability of CBOs to identify, assess, and address such risks. Accordingly, the agencies will consider the following factors when making supervisory allocation decisions relevant to core providers who provide services to CBOs (*e.g.*, decisions regarding the nature, extent, and frequency of supervisory

[2] *See* 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1).

[3] *See* FFIEC, IT Examination Handbook: Supervision of Technology Service Providers (Oct. 2012).

activities applicable to core providers; the contents of examination reports provided to core providers' client financial institutions; and whether to add a core provider to the agencies' service provider examination program):

- **Transparency:** As part of safe and sound third-party risk management, banking organizations collect information from their third-party service providers through due diligence, contractual mechanisms, and ongoing oversight, tailored to the banking organization's size, complexity, and risk profile, as well as the nature of its third-party relationships. CBOs that are unable to collect this information are more likely to face challenges effectively and efficiently managing their third-party risks, which, given the criticality of core providers, may be more difficult to mitigate, compared to other less critical third parties. These informational gaps also may present challenges for the agencies' supervision of these CBOs.

  As such, the agencies will take into consideration the level of a core provider's transparency with CBOs in making supervisory allocation decisions regarding core provider examinations.[4] This will be determined through an assessment of a core provider's (1) willingness to provide reasonably relevant and timely due diligence information necessary for a CBO to decide whether to enter into a core provider relationship and engage in ongoing monitoring thereafter,[5] (2) contractual provisions that limit a CBO's reasonable attempts to compare the core provider's offerings with those of

[4] Any such consideration will balance a core provider's reasonable bases for limiting disclosure of certain information, including as it relates to confidentiality, information security, or other legal or risk-based needs, against the potential risk management benefits to a CBO in seeking to collect the information.

[5] Examples may include, as appropriate to the nature of the third-party relationship, SSAE 18 SOC Reports (Statement on Standards for Attestation Engagements 18 System and Organization Controls Reports), audit reports, security program reports, including penetration testing reports, and industry standard assessments (*e.g.*, Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO)).

other providers, (3) use of, transparency regarding, and compliance with service level agreements using measurable performance standards that reflect a CBO's individual needs and risk profile, along with provisions that enable a CBO to monitor and enforce the agreements, (4) transparency and timely disclosure regarding operational issues and security incidents impacting the delivery of services,[6] and (5) use of complex billing practices that are difficult to reconcile to the services CBOs are receiving.

- **Contract Features:** As part of effective management of third-party risks, a CBO may determine that it either needs to exit a relationship with a core provider that does not meet its needs or has failed to perform adequately or seek supplemental services from alternative providers. However, core provider contract provisions may act as obstacles to a CBO seeking such an exit or supplemental services. As a result, CBOs may be forced to acquiesce to suboptimal core provider relationships wherein CBO needs are less likely to be adequately met and CBOs may have a limited ability to manage third-party risk.

  In making supervisory resource allocation decisions, the agencies will take into consideration a core provider's business practices and use of contract terms that make it difficult for CBOs to manage their core provider relationships in a manner that aligns with the CBO's business needs, such as by seeking an alternative core provider or supplementary services. Such contract terms and practices include, for example, (1) opaque pricing structures and practices, (2) opaque billing practices, including extensive "back billing" windows during which the core provider may issue retroactive charges for items missing from prior invoices, (3) unsupported or contractually undefined core

[6] This includes, among other things, mandatory computer security incident notifications. *See* 12 CFR part 53; part 225, subpart N; and part 304, subpart C.

deconversion fees, especially in instances in which the core provider breached contractual terms, provided inadequate services as measured by service level agreements, or violated or may have caused the CBO to violate any laws or regulations, and (4) excessive limitations on the ability of unaffiliated service providers to integrate with the core platform.

- **Technology:** Core providers that fail to invest in maintaining up-to-date technological solutions may be more likely to experience data breaches or service outages or disruptions, which CBOs have limited ability to oversee or mitigate.

  As such, the agencies will take into consideration a core provider's technology investments and capabilities in making supervisory allocation decisions. This includes, for example, (1) the number and severity of computer security incidents,[7] (2) appropriate management of end-of-support and end-of-life assets that enable client CBOs to transition to updated platforms, and (3) lack of demonstrated operational resilience capabilities.

Supervisory and Enforcement Actions

The agencies monitor services that core providers deliver to CBOs to identify issues related to safety and soundness or violations of law. When such issues are identified, the agencies may bring the appropriate actions against core providers and/or the CBO pursuant to their statutory authorities.[8] This does not eliminate or reduce a CBO's responsibility for ensuring activities are consistent with safe and sound banking practices and in compliance with applicable laws and regulations, regardless of whether they are outsourced to a third party.

[7] *See supra* note 6.

[8] *See*, *e.g.*, 12 U.S.C. 1818 and 1867.

Among other bases for bringing appropriate actions against core providers, the agencies may have a reasonable basis to determine that certain core providers qualify as "institution-affiliated parties" (IAP) under the Federal Deposit Insurance Act[9]—specifically, as "persons . . . who participate[] in the conduct of the affairs of an insured depository institution."[10] This determination reflects the operational reality of the CBO-core provider relationship. While CBOs contract with core providers for services, many of the services provided by core providers address unique features of a CBO, are integral to the functioning of the institution and its delivery of banking products and services, and directly impact the customer banking experience. Many CBOs are wholly reliant on core providers for their back-end operations, as well as some of their customer interfaces and other functions.

In these arrangements, core providers undertake the most central operational aspects of banking for the CBO, and CBOs often could not provide their services otherwise. Because core providers are integral to carrying out the business of banking and the functions of CBOs, they may be held liable for the practices or violations of a CBO as an institution-affiliated party.

[9] 12 U.S.C. 1813(u).

[10] 12 U.S.C. 1813(u)(3).