American Bankers Association

Deborah Whiteside
Senior Vice President, Vendor Evaluation
Office of Member Engagement
dwhiteside@aba.com

December 1, 2025

Margaret Colvin
Fintech Policy Specialist
Co-Chair, FFIEC Community Bank and Credit Union Digitalization Subcommittee
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E–218
Washington, DC 20219

Steven Winkeljohn
Financial Technology Analyst
Co-Chair, FFIEC Community Bank and Credit Union Digitalization Subcommittee
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Via Electronic Transmission

Re: Recommendations to Address Core Provider Impact on Banks' Ability to Digitalize

To Whom It May Concern:

Thank you for meeting with the American Bankers Association's Core Platforms Committee to discuss how core service providers impact community banks' ability to digitalize and innovate. In addition to the work that the FFIEC Community Bank and Credit Union Digitalization Subcommittee is doing on this subject, we appreciate Treasury Secretary Scott Bessent's commitment to conduct "a review of the core platform providers, including contract terms that prevent community banks from innovating for the future" as well as Comptroller Jonathan Gould's recent comments acknowledging his concerns regarding the dynamics between banks and "very large, oligopolistic core providers." [1]

To further support the banking agencies' work, this letter provides additional information about the challenges community banks face and recommends actions the agencies can consider to reduce these barriers and promote meaningful choice in the core provider marketplace. We will

[1] The U.S. Department of the Treasury, Remarks by Secretary of the Treasury Scott Bessent Before the Fed Community Bank Conference (Oct. 9, 2025), https://home.treasury.gov/news/press-releases/sb0276 and Office of the Comptroller of the Currency, Remarks by Jonathan V. Gould, Comptroller of the Currency, Women in Housing & Finance Public Policy Lunch (Nov. 6, 2025).

submit a separate letter responding to the OCC's Request for Information on Community Banks' Engagement with Core Service Providers and Other Essential Third-Party Service Providers.[2]

Core service providers are the technology backbone of modern banking. They power nearly every aspect of operations—from account opening and transaction processing to loan management, compliance, and reporting. Community banks typically operate with limited in-house technical resources and are particularly dependent on their core processors. As a result, a core provider significantly impacts a community bank's day-to-day operations as well as its ability to adapt to a rapidly evolving marketplace and technology landscape—both of which affect a bank's business strategy.

Community banks must have the ability to choose the right core platform and ancillary technology service providers, hold them accountable through enforceable service standards, and make changes as strategic needs evolve. Yet, community banks face significant challenges in doing so. Many of these obstacles are driven by core service providers. But others stem from longstanding regulatory practices that unintentionally hinder community banks from converting to a more forward-looking core provider.

Addressing these issues is essential to ensuring that community banks have the freedom to innovate, which is critical to preserving the long-term viability of the community bank model.

* * * * * * * * * *

I. Promote Competition and Market Transparency

Promote Competition and Choice. Even though there are approximately 25 core providers in the market, community banks report they often face implicit or explicit pressure from regulators to contract with one of the top three or four providers. This regulatory preference (actual or perceived) for incumbents reinforces concentration risk and limits a community bank's ability to contract with a core provider that it believes will better meet its business objectives and innovation goals. Regulators should encourage community banks to consider a broader range of core providers when evaluating new partnerships.

The top three core providers collectively control 72 percent of the bank core provider market (Fiserv 42 percent, Jack Henry 21 percent, and FIS 9 percent). FIS dominates among large banks, Jack Henry serves the most small banks, and Fiserv has a mix of both. This level of market concentration underscores the need for regulators to encourage banks to consider a broader range of core providers when evaluating new partnerships.

[2] Office of the Comptroller of the Currency, OCC Bulletin 2025-39, Bank Activities: Request for Information on Community Banks' Engagement with Core Service Providers and Other Essential Third-Party Service Providers (Nov. 24, 2025).

Expand the Universe of Core Service Providers Subject to Examination. Although the agencies do not publish a list of third-party service providers that have been examined under the Bank Service Company Act, evidence suggests that the majority of core service providers have not been examined. Rather, exams are limited to the largest cores. Visibility into these dominant firms may contribute to regulatory bias against smaller or emerging providers. Broadening examination coverage to include a wider range of core service providers would help reduce the systemic risk created by significant concentration in the core provider market.

II. Ensure Core Provider Resilience and Regulatory Readiness

Examine Core Processor Readiness to Support Bank Compliance with Laws, Regulations, and Industry Standards. Based on the limited information available about examinations of core processors, it appears that these reviews are focused primarily on information technology (IT) systems and cybersecurity. They do not appear to assess whether core processors are adequately preparing to support bank compliance with new or evolving regulatory requirements. This narrow exam scope overlooks a growing risk to banks: the inability of core providers to deliver timely updates and modifications in response to changing regulatory expectations.

There have been notable instances when core processors failed to update their systems in time for banks to meet compliance deadlines for new regulatory requirements. For example, core providers have struggled to support the Federal Reserve's FedNow real-time payment system and ISO 200022, a global messaging standard that modernizes how payment instructions and other financial messages are formatted and exchanged to allow for real-time payment processing. These delays have hindered banks' ability to offer modern payment services.

Additionally, when regulators began criticizing banks for charging multiple non-sufficient funds (NSF) fees for represented transactions, not all core processors could provide the necessary tools to help banks comply with new regulatory expectations. This exposed banks to regulatory criticism.

Currently, banks are relying on their core providers to make the necessary modifications to comply with the FDIC's new deposit insurance signage rules for mobile apps. Looking ahead, banks will similarly depend on their cores to support compliance with regulatory requirements pursuant to the CFPB's Small Business Lending Data Collection Rule and the Personal Financial Data Rights Rule. Without a broader and more rigorous examination framework for core providers that includes compliance support, banks may continue to face delays and regulatory exposure.

Enhance Resilience Testing and Incident Reporting Requirements. In addition to evaluating core processor readiness to support bank compliance, the agencies should expand the examination of core providers to include uniform resilience testing and standardized incident reporting. Timely and comparable data on outages, cyber events, and recovery performance will strengthen supervisory insight and improve operational continuity across the banking system.

For instance, the Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers mandates that bank service providers, including the cores, notify their bank clients as soon as possible after experiencing a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.[3] In practice, however, service providers often wait weeks, if not months, before informing banks of such incidents.

Improve Transparency Regarding Core Provider Performance. The agencies should strongly encourage core providers to provide standardized disclosure information regarding system performance, outage reporting, and change-management practices. The cores have access to operational and performance data that their client banks do not, yet client banks are highly dependent on these metrics. Enhanced transparency will address the current imbalance of information between core providers and the banks that depend on them, improve due-diligence outcomes, and foster market discipline among core providers.

III. Promote Data Portability and Enforceable Performance Standards

Encourage Data Access and API (Application Programming Interface) Interoperability Standards. Core service providers should be expected to support basic interoperability standards that allow banks to securely export their data and connect with other systems through APIs. APIs allow banks to integrate third-party solutions needed to provide the products and services that customers demand. But, core providers have restricted community bank access to APIs by charging high fees, requiring excessive implementation time, or failing to support API connections altogether. This problem is exacerbated by the fact that many banks—especially smaller ones—are unable to easily or cost effectively convert to another core that *does* provide data access and API capabilities. These barriers reduce competition and hinder community bank's ability to modernize to meet evolving customer needs.

Ensure Accountability Through Service Level Agreements (SLAs). Core providers are critical service providers and should be required to offer clear, enforceable SLAs. SLAs provide banks with measurable performance standards and recourse when vendors do not meet service expectations. Many community banks report difficulty obtaining SLAs from their core service provider due to the outsize market power that some cores wield. Even when SLAs are

[3] Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

successfully negotiated into contracts, banks often struggle to obtain the necessary cooperation from the core provider to assess whether the core is meeting the agreed upon performance standards. This lack of accountability is inconsistent with the *Interagency Guidance on Third-Party Relationships: Risk Management*, which states that contracts with third parties should include provisions that allow for the monitoring and enforcing of SLAs to ensure that the third party meets agreed-upon standards. The agencies should reinforce to core service providers that SLAs are a best practice and are consistent with the interagency guidance.

IV. Improve Visibility into the Supervision of Core Providers

Publish a List of Core Service Providers That Have Been Examined. Banks typically review their service providers—including their core providers—annually. Because regulators do not provide a list of service providers for which exam reports have been issued in a given year, banks must manually request a copy of the report from their regulator without knowing whether a core service provider has been examined since the bank's last review. The process appears to vary based on agency or examiner but often involves providing a copy of the entire vendor contract. These requests sometimes go unacknowledged, and banks must track and follow up on unfulfilled requests, particularly if a core service provider was not examined in a given year. This paper chase is time consuming and inefficient.

Provide Timely Examination Reports. Community banks report varying degrees of success in obtaining exam reports for their core service provider in a timely manner. Banks may factor these reports into how they manage their core provider. However, there is often a substantial delay between the date of the exam and the date the regulator provides the exam report to the bank. In some cases, the lag time has exceeded 12 months. When the reports arrive late, they are often outdated and provide little value for managing third-party risk.

V. Foster Innovation and Modernization

Support Due Diligence Standardization and Certification. Increasingly, a bank's ability to compete depends on its capacity to adopt new technologies and partner with third-party service providers. Due diligence for onboarding new vendors is often costly, inefficient, and time-consuming, especially for community banks. These challenges are exacerbated when banks must switch core providers. To address this, the agencies should support and actively participate in the creation of a consensus-driven standards setting organization that will establish third-party due diligence standards. We also support the creation of a process to confirm that a third party meets the identified standards. Given that regulators already examine core service providers, establishing consistent due diligence standards for the cores should be achievable.

Under this approach, banks would still conduct a risk assessment of the third party and monitor the third party on an ongoing basis. However, certifications or assessment reports would reduce the duplication of due diligence work that exists today.

Plan for Quantum Risk and Post-Quantum Cryptography. As quantum computing advances, it presents both transformative opportunities and significant cybersecurity risks for the financial sector. The G7 Cyber Expert Group is expected to release a joint statement and roadmap urging financial institutions to prepare for quantum threats by developing mitigation plans and transitioning to post-quantum cryptographic standards. These risks include the potential for quantum computers to break widely used encryption algorithms, exposing sensitive financial data to malicious actors.

Core service providers, as critical infrastructure partners, must begin developing and communicating their plans to address quantum-related risks. This includes adopting the National Institute of Standards and Technology's (NIST) post-quantum cryptography standards and ensuring that their systems are resilient to future quantum-enabled attacks. The transition to quantum-safe encryption is not a distant concern—it is an urgent priority for banks and their vendors today.

Regulators should incorporate quantum risk preparedness into core service provider examinations and encourage core providers to participate in coordinated innovation environments that support testing and migration to quantum-resistant technologies. This will help ensure the long-term security and resilience of the financial system as quantum capabilities mature.

VI. Conclusion

We appreciate the agencies' attention to the challenges posed by core service providers and their impact on banks' ability to digitalize. We encourage the agencies to take steps to address the concerns outlined above. We would be pleased to meet with you again to elaborate on these issues. Please contact me at dwhiteside@aba.com if you have any questions or would like to schedule a follow-up discussion.

Sincerely,
/s/ Deborah Whiteside
Deborah Whiteside
SVP, Vendor Evaluation
Office of Member Engagement