June 26, 2025

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E-218
Washington, DC 20219

RE: Request for Information Regarding Community Bank Digitalization; Docket ID OCC-2025-0008

Dear Chief Counsel's Office,

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to respond to the Office of the Comptroller of the Currency's (OCC) Request for Information (RFI) on Community Bank Digitalization. The RFI seeks public comment to enhance the OCC's understanding of digitalization activities and support its supervisory efforts aimed at facilitating a safe, sound, and fair transition to digital banking. Specifically, OCC solicits input on the key challenges and barriers community banks face in adopting digital solutions, the degree to which digitalization is a strategic priority, and the factors influencing these decisions.

ICBA's Stance and Executive Summary

ICBA welcomes the OCC's attention to community bank digitalization. Among the wide array of bank digitalization products and services that are available, community banks prioritize technology that can help them serve their customers better.[2] But rather than develop this technology in-house, many depend on third-party relationships or partnerships. Nearly 80 percent of community banks "rarely" or "never" rely on in-house technology for nonlending digital banking products and services, and just over 70 percent for online loans.[3] Partnering with fintech companies can offer valuable relationships that help community banks enhance the customer experience.

Community banks seek solutions that can leverage new opportunities, such as the ability to forge deeper relationships with their customers and communities, target new markets, and keep pace with customers' expectations. Much of this value is enhanced through the adoption and use of technology. However, community

[1] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering ec
[2] FDIC Community Banking Study, Dec. 2020, at 6-4, stating, "When asked to describe the 'most promising opportunities facing your bank regarding new technology,' community banks focused more on their customers than on other potential benefits, such as cost savings and efficiency gains."
[3] See "CSBS 2020 National Survey of Community Banks," Sept. 2020 ("CSBS Survey"), Figures 56 and 57, at 42.

banks face significant barriers to adopting and implementing modern financial technologies. These challenges are primarily due to resource constraints, outdated or overly broad regulatory frameworks, lack of tailored guidance, and over-reliance on a small set of dominant technology vendors.

As the OCC considers challenges to community bank digitalization efforts, ICBA urges the OCC to consider the following recommendations, as discussed more fully in response to each question in the RFI:

- adopt a modernized and responsive regulatory framework that enables responsible innovation while preserving the safety and soundness of the financial system;
- leverage existing supervisory authority;
- facilitate industry-wide shared due diligence and standard-setting;
- reintroduce Frequently Asked Questions (FAQs) and supervisory highlights for real-time guidance;
- support responsible use of artificial intelligence (AI) and machine learning (ML);
- promote equitable oversight of third-party providers; and
- modernize restrictions that currently inhibit community bank participation in innovation ecosystems such as venture capital funds.

1. Planning for Digitalization: Primary Challenges Facing Community Banks

Community banks face several interconnected challenges as they pursue digital transformation. These challenges primarily stem from three critical areas: expense, limited internal experience, and unclear or inconsistent examiner expectations.

Expense is a major barrier to digitalization. Community banks operate on thinner margins compared to larger financial institutions, making the upfront and ongoing costs of digital transformation difficult to absorb. Investments in cybersecurity, digital banking platforms, compliance software, and advanced analytics tools are necessary but can significantly strain a community bank's operating budget. These expenses are compounded by the increasing demands of compliance and data security, and by the fact that smaller banks cannot benefit from the same economies of scale as larger institutions.

Limited internal experience with financial technology also complicates digital transformation efforts. Many community banks lack in-house technical expertise to evaluate and implement digital technologies. Unlike large national banks with dedicated innovation or IT departments, community banks must often rely on outside consultants or their core providers for implementation and ongoing support. This limits their ability to fully understand or leverage emerging technologies, leading to slower adoption rates and increased risk of vendor lock-in.

Examiner expectations are another significant hurdle. Community banks often cite uncertainty around regulatory expectations as a barrier to innovation. While prudent oversight is essential, the lack of clarity on how examiners will view novel technologies—especially when sourced from newer, less established fintechs—causes many banks to default to legacy vendors. This stifles competition and innovation, as banks fear examiner criticism for stepping outside well-trodden paths.

2. Board and Governance

Community bank boards are increasingly aware of the strategic necessity of digital transformation. However, limited familiarity with fintech trends and emerging technologies often prevents boards from confidently overseeing such initiatives. Directors may struggle to evaluate risk or identify opportunities, especially when proposals involve unfamiliar third-party vendors or complex digital infrastructure investments.

ICBA recommends that regulators support board engagement by encouraging or providing resources such as fintech-specific governance training, access to industry best practices, and sample oversight frameworks. Additionally, OCC-supervised banks would benefit from guidance on how to align digital transformation goals with board oversight obligations. A clear roadmap for board engagement would allow directors to support strategic digitalization while meeting their fiduciary responsibilities more confidently.

3. Due Diligence and Implementation

Due diligence for fintech partnerships or digital solutions is a resource-intensive and redundant process for community banks. Each institution must conduct its own review of potential vendors, including security assessments, financial viability, regulatory compliance, and operational resilience.

ICBA proposes a shared due diligence model supported by Standards-Setting Organizations (SSOs) and Certifying Organizations (COs). These entities would establish baseline criteria for technology partners and certify that certain due diligence requirements are met. For example, a fintech could be evaluated for adherence to data security protocols, consumer protection practices, and operational readiness. Regulators and banks alike could then rely on these certifications to streamline onboarding, minimize repetitive diligence efforts, and reduce time-to-market.

The creation of a fintech-focused SSO could significantly reduce friction in bank-fintech partnerships by establishing a shared set of expectations and technical benchmarks. Fintechs currently face lengthy due diligence processes—often taking 10 months or more with banks, compared to just days with non-bank partners. By certifying compliance with established standards, SSOs could help fintechs fast-track onboarding and regulatory review, especially if those certifications are recognized and upheld by regulatory agencies. This would create a more efficient and predictable pathway for innovation to enter the banking system.

An SSO model could play a key role in clarifying and distributing liability in cases of third-party failures. If a certifying organization (CO) affirms that a vendor meets agreed-upon standards but is later found to have been negligent in its review, the CO could share in the resulting liability. This structure places more "skin in the game" on certifiers, incentivizing them to prevent harm and be accountable for mistakes. Additionally, a well-structured SSO could improve transparency by requiring certified vendors to provide real-time updates about material changes, ensuring that banks and regulators stay informed and can respond proactively.

Such a system would be especially valuable in dynamic sectors like credit modeling, where algorithms and risk assessments are regularly updated. An SSO could serve as a centralized clearinghouse for these updates, notifying banks and regulators according to their preferred frequency (such as immediately, quarterly, or only when significant changes occur). This centralized oversight would enhance responsiveness, reduce information gaps, and support more informed risk management. Several industry groups are already exploring SSO frameworks, and ICBA encourages the OCC to help standardize and legitimize these efforts.

4. Digitalization Costs and Budget

Technology costs for community banks have significantly increased over the past decade, driven by the growing demands for cybersecurity, digital banking services, and regulatory compliance. Further, and unlike larger institutions with economies of scale, community banks face disproportionate costs in implementing digital solutions due to their smaller scale. Upfront expenses for cybersecurity, regulatory compliance, and core infrastructure strain limited budgets. The need to compete with fintechs and national banks has further intensified the pressure to adopt mobile apps, online lending platforms, and sophisticated data analytics. These investments are often cost-prohibitive for smaller banks. This surge in expenses has strained the operating budgets of many community banks, forcing difficult trade-offs. Resources that could otherwise support customer service, product innovation, or local lending must instead be allocated to maintaining baseline technological parity.

Moreover, dependence on legacy core processors with limited flexibility and high switching costs exacerbates the problem, locking banks into contracts that often don't meet their evolving digital needs. The result is a widening gap between the capabilities of community banks and those of their larger competitors, threatening the long-term viability of smaller institutions.

Beyond initial investments in hardware and software, banks must continually allocate resources to maintain, update, and secure their systems. Key cost categories include cybersecurity and data protection, infrastructure and integration, compliance and regulatory reporting, and customer-facing tools.

As cyber threats grow more sophisticated, community banks must constantly update their defenses. This includes intrusion detection systems, penetration testing, secure communication protocols, and 24/7 monitoring.

Integrating new digital tools often requires costly middleware solutions or customized APIs. Digitalization adds complexity to regulatory compliance, especially in areas like AML, BSA, and consumer data protection. Ongoing investments in compliance technology and staff training are essential. Finally, consumers increasingly expect digital account opening, mobile apps, and instant payment capabilities. Delivering these services requires not only the technology itself but also marketing, support, and ongoing UX refinement.

5. Use of Third Parties

> **Reverting to perceived safety of legacy providers.** While some start-up third parties can truly develop cutting-edge technology that can go toe-to-toe with the largest financial institutions, examiner expectations to this technology can make the partnership so daunting as to not justify the risk. As a result, it is sometimes easier for banks to partner with legacy third parties that receive less scrutiny, such as core service providers. However, the upside of partnering with a core service provider – less examiner scrutiny, and arguably, less risk – is offset by the downside limitations.
>
> There are only a handful of core service providers, creating an oligopoly market whereby the banks have limited bargaining power when negotiating service agreements. As a 2019 Congressional Research Service report found, "only a few large third-party service providers provide the majority of digital

products to the financial industry."[4] The report explains how this limited market eventually leads to higher prices for their services, "which small institutions may be less able to pay than larger institutions." Not only can this lead to a bank that is captive to the service provider, but it can also drain monetary resources that could be better allocated to other technology providers that might better serve the community bank. Further, many core service providers, themselves, are beholden to legacy technology, making it difficult or impossible for them to develop and offer the latest technological advancements. Finally, core service providers often lock banks into long-term contracts, charge high fees, and offer minimal customization. Due to perceived regulatory safety, banks often feel compelled to continue these relationships even when better solutions are available elsewhere.

Supervision of Third Parties

Transparency and regulatory scrutiny should follow risk, not legacy status. In contrast, innovative fintechs often face excessive scrutiny that deters community banks from engaging with them. Regulators should adopt a more balanced oversight framework that encourages competition and supports responsible innovation. This includes standardized onboarding processes and clearer examiner expectations.

This could be achieved through the expanded use of the Bank Service Company Act (BSCA) to supervise not just legacy core providers, but a broader set of third parties. Agencies should publish a list of Significant Service Providers (SSPs), distribute examination findings directly to banks, and include specialists in fields like consumer protection and liquidity in exam teams.

6. Competition and Market Trends

Perhaps the biggest benefit of digitalization and fintech partnerships is their promise to help community banks compete with large banks and non-bank fintech companies, which often have budgets or expertise that is not commonly available for smaller banks.

Fintech partnerships provide multiple benefits, including expanded reach, improved customer interfaces, and enhanced financial inclusion. These relationships enable banks to deliver services that might otherwise be out of reach and promote competition within the financial ecosystem.

Fintech partnerships can significantly enhance community banks' ability to serve their customers. They allow banks to reduce costs, expand product offerings, and better meet the needs of small businesses and consumers. ICBA believes innovation is vital to relationship banking, and regulatory frameworks should enable, not hinder, this progress.

Fintech partnerships represent one of the few realistic paths for community banks to compete with national banks and nonbank financial technology companies. These partnerships enable local institutions to expand

[4] "Technology Service Providers for Banks," Congressional Research Service, Jun. 20, 2019, *available at Technology Service Providers for Banks | Congress.gov | Library of Congress.*

reach, offer tailored digital services, and meet rising consumer expectations without losing their community focus.

Digitalization helps community banks remain competitive by lowering transaction costs, enabling remote service delivery, and improving data-driven decision-making. For example, online loan applications and automated underwriting can significantly reduce turnaround times, while AI-driven chatbots can provide 24/7 customer support.

The key barrier to realizing these benefits is regulatory inertia. ICBA urges the OCC to continue evolving its supervisory models and to recognize that fostering innovation at community banks helps preserve the diversity and resilience of the broader financial system.

7. Use of Artificial Intelligence and Machine Learning

Community banks are beginning to explore AI and ML for use in areas such as fraud detection, risk modeling, and customer engagement. These tools offer the potential to reduce operational costs, expand credit access, and improve compliance accuracy.

However, ICBA cautions that community banks often lack in-house expertise and must rely on third-party providers to implement AI solutions. This introduces additional vendor risk, especially when models are not explainable or introduce bias.

ICBA recommends that regulators align oversight with the NIST AI Risk Management Framework, avoid duplicative AI-specific regulations that could stifle innovation, promote shared-risk models for AI vendors and banks, and provide specific guidance on fair lending compliance and use of alternative data. These steps will enable responsible use of AI while ensuring consumer protections and regulatory clarity.

Community banks are exploring AI to automate operations, improve underwriting, and strengthen cybersecurity. ICBA supports regulatory clarity over new AI applications while cautioning against overly broad or duplicative regulations. Use cases include fraud detection, chatbots, and risk modeling. However, concerns remain about bias, data privacy, and third-party control.

Community banks use AI to automate back-office functions, detect fraud, support chatbots and virtual assistants, improve underwriting decisions, and bolster cybersecurity and anti-money laundering (AML) efforts. However, they face notable barriers: limited in-house expertise, heavy reliance on third-party vendors, regulatory scrutiny of those vendors, and lack of control over AI systems.

AI presents valuable opportunities to expand credit access, improve efficiency, and streamline compliance. But concerns remain around explainability (especially in credit decisions), bias in data, data privacy, and AI-enabled fraud. ICBA recommends safeguards such as fair lending protections (e.g., no-action letters), responsible use of alternative data, rigorous human oversight, and enhanced authentication practices.

8. Effect of Applicable Laws and Regulations

Use of NALs, Pilot Programs, and Sandboxes

Community banks continue to voice frustration in navigating a regulatory framework that is designed to be more deliberate and process-oriented, rather than nimble and responsive to innovation. While properly designed and tailored regulations certainly help consumers, overly broad or outmoded regulations create uncertainty and do not protect consumers. Compliance with third-party guidance and responses to examiner scrutiny have themselves become burdens to partnering with fintechs. To head-off any examiner criticism, community banks will sometimes subject fintechs to a full and thorough dose of due diligence, without regard to criticality, interconnectivity, or other factors that might dictate a less encompassing vetting.

Outdated or vague regulatory guidance often discourages community banks from pursuing innovative partnerships. ICBA urges the OCC to modernize its supervisory approach by reinstating and updating FAQs to address emerging issues in real time, publishing periodic "Supervisory Highlights" to share lessons and themes from recent exams, and expanding pilot programs, no-action letters (NALs), and sandboxes for testing new technologies.

Reinstatement of FAQs

Before the 2023 updates to the Third-Party Risk Management Guidance, the OCC would publish FAQs on third-party risk. The FAQs provided succinct clarity on concrete examples of how the OCC viewed novel issues unique to third parties. ICBA recommends that the OCC reinstitute the FAQs.

To improve upon the prior version of FAQs, however, ICBA recommends that OCC create a standing list of requested questions on the OCC's website, or by seeking FAQ ideas on a periodic basis. OCC should provide more issue-specific compliance guidance for novel issues that might not be addressed by existing guidance. Rather than waiting until the guidance is reviewed *en masse* to address novel issues, ICBA recommends that OCC seeks feedback and weigh-in on novel issues as they present themselves. For example, the FAQs provided insight into OCC’s view on artificial intelligence, treatment of data aggregators, alternative data, and other issues that were not even contemplated when the guidance was issued several years prior. A revised and reinstated FAQs would more rapidly provide the industry with reliable guidance, relevant to more timely issues.

Clear, timely, and issue-specific guidance is critical to helping community banks innovate responsibly. Without it, banks may avoid promising partnerships due to fear of regulatory reprisal. To address the slow pace of traditional rulemaking, ICBA recommends that the OCC institute programs and policies that are responsive to the agile nature of innovation. For example, federal banking agencies have introduced pilot programs, regulatory sandboxes, and NAL policies, designed to allow for in-market testing and evaluation of real-world scenarios. This can yield critical insights for improving financial products and consumer outcomes. ICBA sees promise in these types of programs, particularly NALs, as a means of encouraging responsible innovation while maintaining regulatory safeguards.

Additionally, shared due diligence among banks could streamline third-party risk assessments, providing efficiency and reducing duplicative efforts. A collaborative approach, supported by regulators, would enable especially smaller community banks to better evaluate fintech partners and make more informed decisions. This model also lessens the burden on fintechs, which currently face repetitive and redundant inquiries. Since regulators will never have the resources to examine every fintech, leveraging economies of scale through shared due diligence and pooled oversight is a pragmatic solution to improve supervision and risk management.

Many community banks report difficulty obtaining basic information from large vendors due to limited negotiating power. A shared diligence model backed by an SSO would allow banks to aggregate their influence, increasing their ability to secure necessary information. At the same time, SSOs can support early-stage fintechs by guiding them through the certification process, helping them compile the required documentation. This dual benefit enhances efficiency for banks while supporting smaller fintechs in becoming viable partners.

Finally, ICBA encourages OCC to undertake a risk-mapping exercise to determine which categories of third-party providers warrant direct supervision. By identifying those entities that pose significant risks to the banking system, regulators can prioritize their oversight efforts more effectively and reduce the need for banks to act as intermediaries in supervising their vendors.

This approach would lead to more efficient use of Agency resources, reduce burden on service providers, facilitate shared knowledge, and enable single examination reports.

Rescind OCC Bulletin 2021-54, Restricting Investment in Fintech Venture Funds

Over the past several years, community banks have funded several venture funds focused on making equity investments in independent fintechs. The funds are focused on investing in fintechs that directly strengthen community bank capabilities.

However, current policy limits broader participation and impact. While existing law allows community banks to make non-controlling equity investments in companies engaged in bank-permissible activities, the Biden administration has discouraged indirect investments through venture capital funds, dismissing them as "mere passive investments."[5] This view overlooks the strategic importance of these investments and their active role in advancing community bank innovation.

Equity investments through funds are the most efficient and impactful way for community banks to access fintech innovation at scale. Individually, most community banks lack the resources or specialized expertise to source, evaluate, and manage direct fintech investments. Fintech venture funds provide the scale, underwriting capabilities, and risk management necessary to identify high-potential opportunities.

[5] OCC Bulletin 2021-54.

While banks could theoretically invest directly in each fintech supported by the funds, doing so would be inefficient and burdensome. A collective investment model enables banks to pool resources, diversify risk, and access thoroughly vetted fintech solutions under the guidance of experienced fund managers. To ensure community banks remain competitive and technologically agile, we urge the administration to modernize and clarify policies that currently restrict their ability to invest collectively in innovation through capital funds.

9. Associated Risks: Cybersecurity and Operational Risk

Digitalization increases exposure to cybersecurity threats, especially as community banks depend more on external providers. These risks include data breaches, ransomware, and operational disruptions. ICBA supports stronger third-party risk management expectations, including regular cybersecurity assessments, service-level agreements and data handling protocols, incident response frameworks, and alignment of fintech oversight with bank standards. Risk mitigation also involves enhancing visibility into vendor operations and ensuring consistent regulatory treatment across entities that perform banking functions.

Cybersecurity is a growing concern, particularly in bank-fintech arrangements. Community banks, often with limited in-house resources, rely on vendors who may not be held to equivalent regulatory standards. ICBA recommends improved oversight and third-party risk management programs, including contractual protections and incident response protocols.

cybersecurity risks associated with third-party fintech partnerships are a growing concern for community banks. These institutions, which often have limited internal cybersecurity resources, may become vulnerable when fintech partners fail to maintain adequate security standards. The interconnected nature of these partnerships means that a breach in a fintech vendor’s system can expose sensitive customer data and bank operations to cyber threats. According to the ICBA, community banks "are increasingly reliant on third-party service providers for technology solutions," which can expand their attack surface and create dependencies on external security practices.

Another key risk identified by the ICBA is insufficient transparency and oversight of fintech vendors. Many fintechs operate with less regulatory scrutiny than traditional financial institutions, potentially leading to gaps in their risk management practices. ICBA has warned that "fintechs and nonbank providers may not be subject to the same rigorous regulatory oversight as banks," which increases the risk that data security, privacy, and compliance standards may not align with federal banking requirements. Without consistent due diligence and contractual protections, community banks may unknowingly inherit security vulnerabilities from their fintech partners.

To address these risks, the ICBA advocates for enhanced regulatory alignment and clearer vendor oversight frameworks. It supports policies that ensure fintechs adhere to equivalent data protection and operational resilience standards as banks, especially when handling customer data or accessing bank systems. Additionally, ICBA recommends that community banks implement strong third-party risk management programs that include cybersecurity assessments, service-level agreements, and incident response protocols. As ICBA President Rebeca Romero Rainey stated, “If these relationships are not properly managed, they can present significant risks to a bank’s operations and reputation.” By combining robust internal controls with strengthened industry guidance,

community banks can safely innovate while mitigating cybersecurity threats from third-party fintech engagements.

10. Data Sharing

Although the OCC does not have rulemaking authority under Section 1033 of the Dodd-Frank Act, the OCC still has the ability to provide guidance and considerations when banks share data with customers or third parties. Indeed, one of the OCC's FAQs on third-party risk management discussed responsible sharing of data.

Regardless of whether the CFPB reproposes 1033 or implements the currently finalized version, ICBA opposes mandates for open banking APIs or developer portals. Such mandates impose unnecessary costs and force banks to adopt specific technologies that may not serve their customer base. Instead, banks should be allowed to choose data-sharing technologies based on business needs and customer preferences.

A flexible approach protects innovation, ensures security, and avoids locking the industry into outdated solutions. ICBA also emphasizes that data-sharing relationships should be governed by contracts that specify liability, access rights, and privacy standards.

Virtually all banks today offer their customers access to online banking through web portals and/or mobile apps. In 2024, a significant majority (77%) of Americans reported using mobile or online banking most often to manage their bank accounts, with high approval rates (96% rated as 'Excellent,' 'Very Good,' or 'Good') for existing online and mobile banking products. This demonstrates that consumers already have easy access to information related to their financial products and services "in an electronic form usable by consumers".

Consumers can already digitally manage important account functions like automatic bill payments, peer-to-peer money transfers, reporting lost or stolen debit cards, and disputing fraudulent transactions.

In the context of the OCC's questions on data sharing and third-party reliance, ICBA's Section 1033 stance highlights the importance of regulatory flexibility. Mandating specific data-sharing mechanisms, beyond what is currently provided, would impose significant costs on community banks, particularly given their reliance on third-party vendors for digitalization initiatives.

Allowing financial institutions to manage consumer information sharing with other institutions through contractual relationships can limit access by less reputable third parties and reduce the risk of catastrophic data breaches. It also enables commercially interested parties to define terms related to data access pricing and liability in case of breaches or fraud.

Conclusion

ICBA appreciates the OCC's thoughtful approach in soliciting feedback on community bank digitalization. As outlined in this letter, community banks face a unique set of challenges—including high costs, limited internal expertise, regulatory uncertainty, and dependence on a narrow set of technology vendors—that must be addressed to ensure they can compete and innovate effectively. The OCC has an essential role to play in modernizing oversight, clarifying expectations, and enabling more efficient partnerships with fintechs and third-party providers.

By embracing a more responsive and risk-aligned regulatory framework, supporting industry-wide standards, facilitating shared due diligence, and enabling responsible use of AI and emerging technologies, the OCC can help unlock the full potential of community bank digitalization. Doing so will not only support individual

institutions but will also promote a more diverse, inclusive, and resilient financial system that remains responsive to the evolving needs of consumers and communities nationwide.

So that ICBA can aid your efforts and identify areas of collaboration, please contact me at Michael.Emancipator@icba.org. We would welcome an opportunity to meet with each of you and your teams.

Sincerely,

/s/

Michael Emancipator
Senior Vice President & Regulatory Counsel