June 23, 2023

Via Electronic Submission

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Sir or Madam,

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to provide comments on the Federal Trade Commission's request for information ("RFI") on the "business practices of cloud computing providers." ICBA advocates for technology and innovation that enables community banks to deliver customers innovative products and services while still providing relationship banking experiences. Cloud computing may help community banks provide these important services directly and indirectly through services providers. Because of cloud computing importance and its apparent ubiquity in the economy we support FTC's interest in learning more about the role cloud service providers ("CSPs") play throughout the sector and the economy at large.

Community banks, like others in the financial services industry, utilize a wide variety of third-party service providers to deliver the best customer experience possible. The FTC seeks input on the impact of CSPs on end users, customers, companies, and other businesses across the economy, and specifically the financial services industry. Like other critical service providers, such as the core banking service providers, CSPs play an important role in the efficient operations of community banks, as well as many of the other third-parties on which community banks rely.

[1] The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services. With nearly 50,000 locations nationwide, community banks employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding $5.8 trillion in assets, $4.8 trillion in deposits, and $3.8 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

As the FTC considers the role CSPs play in the national economy, ICBA encourages the FTC to consider the following recommendations:

- Explore the concentration risk posed by the current landscape of CSPs;
- Encourage CSPs to maintain cyber and data security standards that match the regulatory expectations of the industries they support and make the standards and monitoring thereof available to users;
- Examine the ability for small and medium sized businesses to fairly negotiate contracts with CSPs and encourage CSPs to negotiate contracts that are reasonable, fair, and clearly disclose fees; and
- Utilize existing research such as the U.S. Department of the Treasury's report on the Financial Sector's Adoption of Cloud Services.[2]

Concentration Risk

Concentration Risk from a competitive and a security standpoint deeply concerns community banks. For many years, community banks have been frustrated by the lack of competition in the core processing provider industry. In a 2021 survey, ICBA found that 71% of community banks were using only three core processors. The result of this concentration and lack of competition among core processors has led to an environment where community banks face increasingly difficult contract negotiations, limited access to new technologies within the core, and a sense that they are locked into lengthy contracts without meaningful bargaining position.

In the Treasury's report on CSPs in the financial sector, a similar environment was noted – with the added concern that many of the other third parties on which community banks rely are also heavily reliant on the same CSPs. Among all cloud service providers, just three companies comprised over 66% of the worldwide market share in infrastructure as a service.[3] Not only are similar issues among contract negotiations and access to new technology likely to occur, but such concentration within a critical service poses a threat to the resilience of any industry reliant on the CSPs. A critical issue for the FTC, federal banking regulators, and policy makers to ascertain moving forward will be how the CSPs are addressing this risk and what cascading impacts may be felt on community banks and the businesses and consumers they serve should a major outage occur.

[2] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

[3] Per the Treasury Cloud Report Infrastructure as a Service is defined as "Broad and scalable computing capabilities provided as a service including processing, storage, networks, and operating systems, enabling more control over deployed applications.

Security Standards
It is imperative that all companies who handle, store, or have access to financial data be subject to data security and privacy standards similar to those imposed on the financial services industry by the Gramm-Leach-Bliley Act ("GLBA").

Community banks are governed by some of the strictest data security laws and regulations set forth by the GLBA and its implementing regulations and Safeguards Rule.[4] These regulations require financial institutions to disclose their information-sharing practices to their customers, provide certain choices to consumers in how the data is used, safeguard sensitive data, and create robust data security. Protecting consumer financial data is central to maintaining public trust and key to long-term customer retention. Community banks are proud of the security they provide and believe existing laws and regulations appropriately mitigate risks to consumer financial data while that data is being held by community banks.

Further, community banks are required to ensure that any third-party vendor they partner with is following security standards that meet their risk management profile on an ongoing basis although obtaining the requisite diligence materials from the CSPs can present several challenges. ICBA believes that CSPs should work directly with community banks and other financial service providers to ensure that all products and services delivered to regulated entities meet the standards required of those entities.

Contract Negotiations
Through the negotiation of contracts, community banks are able to obtain answers and solutions to the problems listed above. However, as a result of the immense market concentration and sheer size of these companies, negotiations for small and medium-sized companies is often costly and problematic. The form contracts presented by the providers offer little room for revision or negotiation. For example, Amazon Web Services brought in $80 billion in revenue in 2022 making it unlikely to negotiate with a smaller dollar contract with a single community bank using the services provided.[5] This leaves community banks frustrated with the lack of flexibility in contract negotiations on the part of the CSP, particularly as they navigate the increasingly complex regulatory requirements within the financial services industry.

When working with entities in highly regulated industries, such as financial services, CSPs should offer fair and transparent contracts that include all necessary security measures required of the industry at a baseline level. The FTC and federal banking regulators should work together to ensure that CSPs are examined and held to the same security standards that they expect of all bank service providers.

---

[4] Interagency Guidelines Establishing Information Security Standards. 12 C.F.R. § 225 Appendix F. https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-225#Appendix-F-to-Part-225
[5] https://fourweekmba.com/aws-revenues/#:~:text=Amazon%20AWS%20(cloud)%20is%20the,%2418.5%20billion%20in%20net%20profits.

Utilize Existing Reports
When looking at the role CSPs play within the broader financial services industry, ICBA encourages the FTC to review the U.S. Department of the Treasury's report issued earlier this year on "The Financial Services Sector's Adoption of Cloud Services."[6] The report was developed by Treasury in collaboration with the banking regulators who make up the Financial and Banking Information Infrastructure Committee ("FBIIC") with input from the private sector, including ICBA. The report identifies six challenges, and notes that these challenges may be more acute for small and medium-sized financial institutions. These challenges are:

- Insufficient transparency to support due diligence and monitoring by financial institutions;
- Gaps in human capital and tools to securely deploy cloud services;
- Exposure to potential operational incidents, including those originating at a CSP;
- Potential impact of market concentration in cloud service offerings on the sector's resilience;
- Dynamics in contract negotiations given market concentration; and
- International landscape and regulatory fragmentation.

ICBA, and other members of the private sector will continue to work with Treasury and the FBIIC to address the challenges raised in the report and in implementation of the plan for future action and engagement provided. As the FTC continues its examination CSPs and the role they play across the economy, ICBA will continue to engage with Treasury when assessing the financial services industry.

If you have any questions, please do not hesitate to contact me at Steven.Estep@icba.org or (202)-821-4329.

Sincerely,

/s/

Steven Estep
Assistant Vice President, Operational Risk

[6] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.