INTERNATIONAL BANCSHARES
CORPORATION

October 18, 2021

Via email and electronic submission:

Board of Governors of the Federal Reserve System
Ann Misback, Secretary
Attn: Docket No. OP-1752
20th Street and Constitution Avenue NW
Washington, D.C. 20006
regs.comments@federalreserve.gov

Federal Deposit Insurance Corporation
James P. Sheesley, Assistant Executive Secretary
Attn: RIN 3064-ZA026
550 17th Street NW
Washington, D.C. 20429
comments@fdic.gov

Office of the Comptroller of the Currency
Chief Counsel's Office
Attn: Comment Processing, Docket ID OCC-2021-0011
400 7th Street SW, Suite 3E-218
Washington, D.C. 20219
https://regulations.gov

Re: Comments on Proposed Interagency Guidance on Third-Party Relationships: Risk Management: Docket Nos. OP-1752, and OCC-2021-0011; RIN 3064-ZA026.

Dear Sirs and Madams:

The following comments are submitted by International Bancshares Corporation ("IBC"), a publicly-traded, multi-bank financial holding company headquartered in Laredo, Texas. IBC maintains 186 facilities and 281 ATMs, serving 87 communities in Texas and Oklahoma through five separately chartered banks ("IBC Banks") ranging in size from approximately $400 million to $12 billion, with consolidated assets totaling over $15 billion. IBC is one of the largest independent commercial bank holding companies headquartered in Texas.

This letter responds to proposed interagency guidance on third-party relationships ("Proposal") by the Federal Reserve Board ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC," collectively, the "Agencies"). The Proposal includes adoption by the Agencies of the OCC's 2013 guidance on third-party relationships and related risk ("2013 Guidance"), and

P.O. DRAWER 1359, LAREDO, TEXAS 78042-1359 (956) 722-7611

seeks comment on to what extent the OCC's 2020 frequently asked questions guidance ("2020 FAQs") should be incorporated into the final version of the guidance ("Guidance").

IBC recommends the 2013 Guidance be lightly revised to include several of the 2020 FAQs, in order to more appropriately reflect the Agencies' position and the realities of the modern banking landscape. This includes issues regarding fintechs, standard-setting or certifying organizations ("SSOs" and "COs"), collaborative negotiation, and the restraints and restrictions of engaging certain third-party service providers.

Comments to Specific Requests

General

1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?

2. What other aspects of third-party relationships, if any, should the guidance consider?

Scope

3. In what ways, if any, could the proposed description of third-party relationships be clearer?

4. To what extent does the discussion of "business arrangement" in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?

5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third-parties?

Tailored Approach to Third-Party Risk Management

6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?

7. In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?

IBC Comment: The Agencies note that banks may not, and frequently do not, have the ability to negotiate favorable or ideally appropriate terms with large third-party service providers, such as AT&T, Microsoft, public utilities, and end user license agreements that

in most cases are non-negotiable click-thru documents. To these large entities, banks represent a mere fraction of their customer base, and most lack financial services experience and expertise. While banks strive to educate these service providers regarding the comprehensive regulatory requirements bank face, most service providers are hesitant (if not outright hostile) to the idea of negotiating contract terms to provide sufficient protection and compliance of the banks. Even where a third-party service provider exclusively serves banks, its sheer size and service offerings may put it in a position of negotiating dominance. For example, Fidelity Information Services is a large provider of financial services to banks, yet it maintains strict control over its contracts and their negotiations. In many cases, banks are unable to negotiate appropriate indemnity and liability terms, while also failing to get a representation and warranty from the third-party that it (and its products/services) will comply with the applicable law and/or regulation. Thus, banks are unable to protect themselves either proactively or reactively and must ultimately make a risk decision.

Where contractual terms are not legally required on behalf of the third-party, the Agencies should provide support and guidance for negotiating and terms. Third-party service providers, while not necessarily directly regulated by the Agencies, should understand the importance of negotiating with a regulated institution. Moreover, the Agencies should consider creating and fostering a collaborative negotiation tool for banks which would allow them to engage in cooperative negotiations that can pool the resources and bargaining power of multiple banks, especially against large third-party service providers.

IBC recommends the following 2020 FAQs be included in the final Guidance: 5 (limited negotiating power), 12 (collaboration), 14 (report/audit reliance), 24 (SOC).

To the extent the Agencies do not wish to be so "hands on," IBC recommends the Agencies support some type of collaborative negotiating or ongoing management effort or group (e.g. SSO/CO) to allow financial institutions to pool leverage and resources to negotiate against sophisticated third-parties. The 2013 Guidance and 2020 FAQs, as well as recent proposed and published guidance, support the broader implementation and use of SSOs/COs and centralized organizations and repositories in order to assist with regulatory requirements and oversight related to third-party service providers. If SSOs and COs were used more broadly, banks could rely on such independent testing/verification/certification in order to more quickly and efficiently negotiate with and engage third-party service providers in a compliant manner. This would still allow flexibility and autonomy to both third-parties and banks that wish to negotiate and implement unique/non-standard terms, as such SSO/CO involvement or standards would not need to be required, but rather one option. But having such SSO/CO involvement would at least provide banks a set, good faith negotiating position to begin with or fall back to in the event of third-party push back.

8. In what ways could the proposed description of critical activities be clarified or improved?

IBC Comment: IBC recommends the Agencies confirm what "significant customer impacts" means in its list of "critical activities." (Proposal at 20) Are significant customer

impacts monetary damages to customers? Do they include service downtime? Would they include non-substantive disclosure errors (e.g. information was disclosed in 9-point, non-bolded font, when it was required to be in 10-point, bolded font)? Or is a "significant" impact only measured by how many customers are affected? It is not clear from the 2013 Guidance what would be considered a "significant customer impact," and there are many possible interpretations that could result in almost all of a bank's service providers supporting "critical activities." IBC asks the Agencies to clarify what they consider significant customer impacts.

Third-Party Relationships

9. What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third-parties?

10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

IBC Comment: IBC believes that third-party assessment requirements should be tiered and categorized based on both the type of risk and the type of products/services provided, including the amount of data and type of information that is shared with third-party service providers. For example, a bank may have one third-party handle its lockbox services generally, but may engage another for its healthcare customers specifically. The general lockbox provider likely receives more data and more different types of data, but the latter vendor would almost certainly present more risk given the specific type of data it would be handling. Any third-party service provider assessment requirements should acknowledge that pure data volume, data type categories, and specific product and service information may not capture the entire risk profile individually, but need to be considered in context and as a whole.

IBC also urges the Agencies to consider the reality of the aggressively evolving cybercrime landscape, including ransomware and other security exploits. The 2013 Guidance states that "[i]ncreased risk often arises from greater complexity, ineffective risk management by a banking organization, and inferior performance by the third-party." (Proposal at 18) While that is true, it is also only part of the story. For all their efforts, banks are not, and never will be, primarily technology businesses. They will never be capable of fully understanding and anticipating technological threats, nor should they be. Banks rely on third-party expert relationships in order to protect their technological assets and offerings, and to mitigate related risks. Banks also rely on industry-standard auditing, testing, and reporting, including through SSOs and COs. Even if a bank was solely focused on technology, even the most advanced fintechs and IT consultants cannot fully foresee and protect against every emerging or potential technological threat. Even herculean efforts cannot eliminate the risk that any company and industry has the potential to be significantly impacted in a negative way by the most recent cyber threat. While cyber security risk is certainly increased by bad oversight, management, and performance, there will also be risks that simply cannot be protected against or eliminated

in all cases. The imperative to adopt and integrate more and more technology into the financial services space will always carry risk. IBC urges the Agencies to not punish banks with post-hoc analyses of cyber security events that could not have been prevented or foreseen in any practical manner. Hindsight is 20/20, but predicting and staying ahead of the next cyber threat is extraordinarily challenging. The Agencies should be careful in evaluating cyber events implicating third-parties, including what caused the event and what, if anything, could have been done to prevent it. Broader support and adoption of SSOs and COs would help banks and third-party services providers more efficiently and effectively work together to best prevent and protect against existing and emerging cyber threats.

IBC also strongly recommends the Agencies issue additional voluntary guidance regarding a bank's relationships with start-up companies, especially in situations where limited information about the start-up is available. 2020 FAQ 16 provides that:

> In assessing the financial condition of a start-up or less established fintech company, the bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third-party's overall financial stability. Assessing changes to the financial condition of third-parties is an expectation of the ongoing monitoring stage of the life cycle. (Proposal at 78)

While this guidance is helpful on its face, it functionally provides no substantive direction, leverage, or protection for banks to use in evaluating, negotiating against, or managing start-up service providers. The problem with start-ups is not necessarily a lack of projections and cash flow, but rather the stability and accurateness of the available information. Fintech start-ups are so ubiquitous now, there is nearly a standard/expected set of documents that typically supports the relationship. The issue is a bank, that correctly and appropriately relies on such documentation and information, may still face regulatory backlash when such forward-looking documentation proves inaccurate. What steps can a bank take to sufficiently protect itself and comply with what regulators expect? What information would be sufficient in the eyes of the Agencies?

IBC recommends the following 2020 FAQs be included in the final Guidance: 16 and 17 (start-ups).

11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?

12. What risk management practices do banking organizations find most effective in managing business arrangements in which a third-party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?

IBC Comment: IBC recommends the Agencies consider additional guidance related to third-party relationships between banks and other highly regulated industry partners, such as credit reporting bureaus, insurers, and debt servicers. The Agencies should look for ways for banks and other highly-regulated third-party partners to leverage their regulatory oversight in order to negotiate, implement, and maintain their relationships more efficiently and safely. The Proposal states that:

> Whether activities are performed internally or outsourced to a third-party, a banking organization is responsible for ensuring that activities are performed in a safe and sound manner and in compliance with applicable laws and regulations. (Proposal at 20)

The Proposal also states that "on-site visits may be useful to understand fully the third-party's operations and capacity." (Proposal at 25) However, banks are frequently unable to negotiate for invasive audit and oversight powers due to the strict regulations on the third-party. For example, a bank would almost never have the right to an on-site review of a credit reporting bureau. The Agencies should provide guidance related to highly-regulated third-party partners and how banks might rely on other regulators and oversight to ensure that their third-party partners are performing in a safe and sound manner and in compliance with applicable laws. For example, banks often contract with credit reporting bureaus to provide and receive consumer information for any number of reasons, including identity authentication and verification and credit underwriting. The "big three" credit reporting bureaus are large, powerful, and highly regulated. There is typically little room for negotiation, and very little insight or oversight provided to the bank. But that does not mean that the relationship is an unacceptable risk per se, because the credit bureaus are so highly regulated. The Agencies should make clear what a bank's obligations are regarding such third-party partners, and to what extent such regulation and government oversight can be relied upon when contracted with such third-parties.

Why not ask vendors to provide a recap of their consumer complaints?

Due Diligence and Collaborative Arrangements

13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?

14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?

IBC Comment: In addition to the SSO/CO recommendations contained herein, IBC recommends the Agencies take two actions to clarify and streamline their due diligence and collaboration expectations: (1) create and maintain a central database similar to the Beneficiary Ownership Model (created and maintained by FinCEN) for third-party service

providers; and (2) expand the number of third-party service providers audited by the Agencies and make such related reports available in a timely manner.

Both suggestions could be voluntary for third-party service providers, but at least the existence of a database and available audit reports would provide banks leverage in working with third-party service providers and a greater ability to manage and oversee the third-party relationship. 2020 FAQ 2020 states that:

> [Technology service providers' ("TSP")] reports of examination are available only to banks that have contractual relationships with the TSPs at the time of the examination. Because the OCC's (and other federal banking regulators') statutory authority is to examine a TSP that enters into a contractual relationship with a regulated financial institution, the OCC (and other federal banking regulators) cannot provide a copy of a TSP's report of examination to financial institutions that are either considering outsourcing activities to the examined TSP or that enter into a contract after the date of examination....
>
> The OCC may, however, proactively distribute TSP reports of examination in certain situations because of significant concerns or other findings to banks with contractual relationships with that particular TSP....
>
> Although a bank may not share a TSP report of examination or the contents therein with other banks, a bank that has not contracted with a particular TSP may seek information from other banks with information or experience with a particular TSP as well as information from the TSP to meet the bank's due diligence responsibilities. (Proposal at 86)

IBC supports the Agencies' attempt to harmonize and clarify third-party relationship guidance. However, IBC believes the Agencies should focus on how they can more fully engage with and oversee third-party service providers, or at the very least allow third-parties a way to "opt in" to increased oversight in order to provide a safe harbor of third-parties with which banks can engage. FinCEN is developing a comprehensive corporate registry that banks can use, rely on, and add to, in order to comply with the Beneficial Ownership Rule. Even if the Agencies do not believe they currently have the authority to mandate such a registry, they should endeavor to create or advocate on behalf of such authority and should consider creating a voluntary database. The Agencies should also consider whether it is possible to broaden the Agencies' authority to "proactively distribute" TSP reports in the event of "significant concerns or other findings." Currently, the Agencies (and the OCC specifically) are empowered to make such a proactive distribution to banks that have contractual relationships with the particular TSP. The Agencies should be able to distribute such TSP report, or specific concerns and findings, to the public generally, especially in the case of elevated or systemic concerns. The Agencies should also consider clarifying what information a bank can provide to another bank about a TSP as part of due diligence responsibilities. The Agencies may consider creating an abbreviated TSP report summary or simply identifying specific information that may be shared about TSPs between banks.

Subcontractors

15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?

16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?

IBC Comment: Financial Institutions have limited impact on the number, location, use, or management of third-party service providers' subcontractors. The Agencies should consider any tool available to them to help empower banks to negotiate appropriate subcontractor terms in their third-party service provider agreements, or, at the very least, help banks require third-party service providers to bind subcontractors to any obligations and standards of the third-party. It would also be immensely helpful if banks had a way to require the disclosure of who the subcontractors are and report any changes. Given the ability to provide technological services from anywhere on the globe, fintechs and other TSPs typically look to maximize efficiency by engaging foreign subcontractors to assist in providing services. These third-parties generally fail to appreciate the highly regulated nature of the financial service industry and the incredibly onerous oversight required at every step in the chain. Banks need all the leverage the Agencies can provide in order to negotiate appropriately protective terms regarding subcontractors into their third-party service provider contracts.

IBC recommends the following 2020 FAQs be included in the final Guidance: 11 (subcontractors).

Information Security

17. What additional information should the proposed guidance provide regarding a banking organization's assessment of a third-party's information security and regarding information security risks involved with engaging a third-party?

IBC Comment: The Proposal states that banks should "assess the information security program of third-parties, including identifying, assessing, and mitigating known and emerging threats and vulnerabilities."

For all their efforts, banks are simply not able to "mitigate" known and emerging threats and vulnerabilities for third-parties. The banks may be able to, and should, structure their relationships to account for the potential compromise or failing of a third-party service provider, but they simply cannot actually mitigate the risk for the third-party. When a bank assesses a third-party service provider and identifies a potential emerging threat or

vulnerability, it is documented and discussed, but it is up to the third-party to address and mitigate the issue. It is up to the bank to accept the vulnerability and related risk, or to terminate the relationship and risk service-related issues.

Moreover, while banks implement comprehensive security and technology programs to address and protect against known and emerging threats and vulnerabilities, banks are not technology companies. Banks are not fintechs. Banks may not be on the cutting edge of sophisticated threats. Banks rely on third-parties, and third-party service providers, to provide that guidance and monitor their respective industries accordingly. Banks rely on these parties to be on the vanguard in those areas. The sheer volume of new and emerging technologies, protocols, apps, and codes make it impossible for a bank to efficiently manage not only its banking business, but also all of the technology available to banking customers. Banks must engage third-parties to manage those risks.

Finally, even when a bank is able to contract for broad insight and oversight regarding a third-party's information security program, it is typically almost impossible to negotiate breach terms referenced by the Agencies. The Proposal states that third-party service provider contracts should sufficiently address a "third-party's procedures for *immediately notifying* the banking organization whenever service disruptions, security breaches, compliance lapses, enforcement actions, regulatory proceedings, or other events pose a significant risk to the banking organization…." (Proposal at 37, emphasis added) Third-party service providers will virtually never agree to "immediate" notification of a cyber breach, and will typically agree to notice within seventy-two (72) hours or within a reasonable time. The Agencies should not expect contracts to require immediate notification, or should make such notification required so as to provide banks the leverage required to negotiate for such notice. To the extent the Agencies believe immediate notification is required for "significant risks," IBC recommends expressly clarifying what would constitute a significant risk.

<u>OCC's 2020 FAQs</u>

18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

IBC Comment: As discussed herein, and because of their unique guidance and clarity, IBC recommends the Agencies include the following 2020 FAQs in the final Guidance: Cloud computing (3), data aggregator (4), limited negotiating power (5), collaboration (12), report/audit reliance (14), start-up (16, 17), SOC (24),

Thank you for the opportunity to share IBCs views on these matters.

INTERNATIONAL BANCSHARES CORPORATION

Dennis E. Nixon
President and CEO