3811 Ponce de Leon Blvd
Suite 1300
Coral Gables, FL 33134
404-822-6575

**FEDERAL RESERVE SYSTEM**
**[Docket No. OP-1752]**

**FEDERAL DEPOSIT INSURANCE CORPORATION**
**RIN 3064-ZA26**

**DEPARTMENT OF THE TREASURY**
**Office of the Comptroller of the Currency**
**[Docket ID OCC-2021-0011]**

**Re: Proposed Interagency Guidance on Third-Party Relationships: Risk Management**

Below, please find commentary from ACI Worldwide Inc. in response to
**Regarding the Proposed Interagency Guidance on Third-Party Relationships – Fed Docket No. OP-1752; FDIC RIN 3064-ZA26; Docket ID OCC-2021-0011**

Proposed guidance - Section IV C. Risk Management, Item 3, Contract Negotiations (p. 34)

*"A material or significant contract with a third party typically prohibits assignment, transfer, or subcontracting by the third party of its obligations to another entity without the banking organization's consent"*

While we understand the need to get the consent of the banking organization in case the third-party provider explicitly and contractually ***assigns*** or ***transfers*** its contractual obligations with a banking organization to another party, we think the ***subcontracting*** should not be included in such obligation. Third party providers utilize subcontractors to enable access to better and more efficient services. Such services may include, for instance, outsourcing of parts of its software engineering, usage of robust network providers, etc. Moreover, such services may be used to serve many banking organizations, potentially thousands. Obtaining approval from all of them in a leveraged environment to subcontract services to a third party is logistically unsustainable and is unlikely to ever result in unanimous approval by all customers. We suggest that subcontracting be removed completely from the Guidance.

Proposed guidance – Section IV C. Risk Management, Item 3c, Responsibilities for Providing Receiving, and Retaining Information (p. 37)

*"Notification to the banking organization before making significant changes to the contracted activities, including acquisition, subcontracting, offshoring, management, or key personnel changes, or implementing new or revised polices, processes, and information technology"*

Service providers must be nimble and move quickly to successfully accommodate the needs of their customers. Service providers undergoing acquisitions are often not at liberty to notify customers of such acquisitions until they have already been publicly announced. Similarly, policies, processes, and information technology are constantly and continually refreshed by service providers and notifications of these activities each time they occur is logistically unsustainable. Suggest this provision of the Guidance be removed or at least modified to indicate that such notifications may occur at regular intervals (such as semi-annually) of that they may occur within a reasonable timeframe as determined by the service provider.

Proposed guidance – Section IV C. Risk Management, Item 3c, Responsibilities for Providing Receiving, and Retaining Information (p. 37)

*"The ability of the institution to have unrestricted access to its data whether or not in the possession of the third party;"*

This provision of the Guidance is vague and unclear, particularly when caveated as "unrestricted" access to data. Providing unrestricted access increases the complexity of securing connectivity into the service provider environment and/or poses risks to the service provider around ensuring appropriate protection of data interchange methods. Identity and Access Management (IAM) processes needed to properly address this guidance could have an impact to the service provider's ability to provide services in a timely manner. Suggest the addition of a more granular definition for "unrestricted access." Additional clarification requested on the definition of what constitutes "data."

Proposed guidance – Section IV C. Risk Management, Item 3c, Responsibilities for Providing Receiving, and Retaining Information (p. 37)

*"The ability for the banking organization to access native data and to authorize and allow other third parties to access its data during the term of the contract."*

This provision of the Guidance potentially causes grave concern for a service provider's ability to properly protect the customer data with which it is entrusted. Additionally, what is the definition of "native data?" Is native data restricted to only the data provided directly by the customer – and in only the format provided by the customer? Allowing other third parties to access customer data may be a violation of the service provider's data protection agreements, as contractual terms, with data protection controls must be in place and validated before any third party is provided with customer data. This provision of the Guidance creates a potential third-party situation that may directly violate service provider standards or other terms of the customer contract that address data protection and is therefore recommended for removal from the Guidance.

Proposed guidance – Section IV C. Risk Management, Item 3j, Operational Resilience and Business Continuity (p. 41)

*"Include provisions for transferring the banking organization's accounts, data, or activities to another third party without penalty in the event of the third party's bankruptcy, business failure, or business interruption."*

Introduction of 'without penalty' into the requirement will necessitate new provisions be included into suppliers' contracts with financial institutions. Applicable language is not currently in place in existing contracts and would likely create a gap until addressed. Suggest this requirement provide time reference associated with effective date.

We thank you for your consideration of our comments.

Mohammed Mortajine

Head of Compliance, Security, & Risk Management

Brad Mullman

Head of Enterprise Risk & Compliance