Warren Averett
CPAs AND ADVISORS

2500 Acton Road
Birmingham, AL 35243
205.979.4100
warrenaverett.com

July 18, 2016

Lisa A. Snyder
Director of the Professional Ethics Division
AICPA
1211 Avenue of the Americas
New York, NY 10036
By email: lsnyder@aicpa.org

Re: Exposure Draft—*Hosting Services* (Proposed Interpretation)

Dear Ms. Snyder:

Warren Averett, LLC appreciates the opportunity to provide comments on the American Institute of Certified Public Accountants' (AICPA) Professional Ethics Executive Committee's (PEEC) Proposed Interpretation regarding hosting services. Our comments on the Proposed Interpretation follow.

We do not support the position taken by the PEEC that the providing of hosting services, including business continuity and disaster recovery, necessarily involves having custody or control of data or records that the client uses to conduct its operations which creates a "management participation threat" to independence, or that this creates a "self- review" threat to independence that cannot be reduced to an acceptable level through the application of safeguards.

When a member is engaged to provide a hosted platform, we believe that, as the AICPA has defined both self-review and management participation threats, a properly provisioned and properly operated hosting environment is, by consequence of design, capable of satisfying independence requirements and does not involve the assumption of custody and control of the data and records. We are certain that if self-review threats were created there are acceptable safeguards available. These safeguards can be implemented in any applicable hosting environment in order to ensure that there is no opportunity for the appearance of an attest client impairment to independence to exist.

A hosting provider of any size or type must have acquired a facility from which to operate, and a platform from which to provide a service. Platforms consist of physical hardware to include network devices for communication, computing devices for processing of information, and storage devices for the housing of information. The combined facility and platform is referred to as a datacenter. There are no physical attest client assets in a datacenter used for hosting. Only raw data is hosted. The data itself is not usable without additional resources to convert it from its raw form into meaningful and interpretable information. In a hosting engagement, the role of the member firm is to provide the datacenter platform for the client to use in accessing, viewing, interpreting, creating, and editing data. The client maintains custody of its assets, to include applications, operating systems, and licenses, and uses the hosted platform for access and presentation of information. The member or member firm's role is to maintain a usable, secure, and reliable platform for the client's access. Consequently, self-review threats are presented at levels that can be reduced with the application of safeguards.

Business continuity plans entail many aspects and components that are not relative to the backup and recovery of information systems. The information technology component of a business continuity plan is an aspect of consideration that can only be addressed by management. It is our experience that no

management responsibilities are assumed by the member as it relates to the process of backing up and restoring data.

We are concerned with the unintended implications of a blanket policy as it relates to the ability of the member or member firm to assist an attest client with data recovery.

The **"General Requirements for Performing Non Attest Services" (AICPA, Professional Standards, ET sec 1.295.040)** explains the main safeguards that need to be applied whenever members provide non attest services to their attest clients.

Safeguards are defined as controls that partially or completely eliminate threats or diminish the potential influence of a threat. We believe safeguards, if needed, can be implemented and applied to reduce a perceived threat to an acceptable level for those hosting services as described in the proposed interpretation.

If a threat were to exist it is considered to be "at an acceptable level" when the significance of the threat combined with the safeguards applied reduce the risk of the threat to a level where a reasonable and informed person would likely conclude that the service could be performed with integrity and objectivity.

Examples of safeguards implemented by an attest client that would operate in combination with other safeguards:

a. The attest client has personnel with suitable skill, knowledge, and/or experience who make all managerial decisions with respect to the delivery of non-attest services by the member to the attest client
b. A tone at the top that emphasizes the attest client's commitment to fair financial reporting
c. Policies and procedures that are designed to achieve fair financial reporting
d. A governance structure, such as an active audit committee, that is designed to ensure appropriate decision making, oversight, and communications regarding a firm's services
e. Policies that dictate the types of services that the entity can hire the audit firm to provide without causing the firm's independence to be considered impaired

Examples of specific safeguards implemented by the member relative to hosting services:

a. Firm leadership that stresses the importance of independence and the expectation that members of attest engagement teams will act in the public interest
b. The use of different partners, partner equivalents, and engagement teams that have separate reporting lines in the delivery of permitted non-attest services to an attest client, particularly when the separation between reporting lines is significant
c. Policies that limit physical access to the hosting premises (datacenter) to non-attest partners, partner equivalents, and engagement teams
d. Use of a datacenter facility owned and operated by a 3rd party
e. Use of a datacenter facility located on physical premises separate from facilities housing attest partners, partner equivalents, and engagement teams
f. Physical controls of datacenter meeting standards of access and operation of SOC II or comparable levels
g. Policies that require the use of technologies ensuring comprehensive logging, alerting, and regular review of access to the hosting environment and the attest client systems
h. Policies ensuring the attest client physical access to the datacenter at any time

Additional Comments related to areas the PEEC needs to address

1) Clarify the definition and meaning of “custody or control” as it relates to the meaningful use of client data and systems.
2) Clarify the definition and meaning of “data or records the client uses to conduct its operations”
3) Distinguish between physical and logical assets as it relates to custody and control.
4) Expand upon the implications of having different platforms in the “hosting” arena.
5) The implications, if any, when a member establishes an affiliated entity to provide hosting services to the firm’s attest clients.
6) The meaning and definition of “member’s servers” and clarify the difference with servers located at a third party data center.
7) The definition and meaning of “production environment” and discuss the implications of having “access to”, versus “custody and control of”, the data and records.

By creating an absolute rule we believe the PEEC would be undermining the principles that recently became effective as outlined in the Conceptual Framework for Members in Public Practice and are concerned that the proposed interpretation will have inappropriate and unintended consequences.

We ask that the PEEC give further consideration to whether hosting services expressly imply the assumption of custody and control of assets as we do not believe this occurs under circumstances wherein practical safeguards are implemented and IT systems are provisioned according to industry standards. We also respectfully request further review and analysis as to the opinion of independence relative to business continuity and disaster recovery services.

We appreciate the PEEC’s efforts to provide enhanced guidance related to situations where independence with respect to an attest client may become impaired. We urge the PEEC defer this proposal until further discussion and analysis can be completed.

We would be pleased to discuss our letter with you. If you would like to discuss our comments please contact Jim Lamphron (205-769-3431) David Kasuba (205-769-3231) or John Mastin (334-260-2366).

Respectfully,

Warren Averett, LLC

Warren Averett, LLC