May 1, 2020

To the Board of Directors
American Network of Community Options and Resources
Alexandria, Virginia

In planning and performing our audit of the financial statements of American Network of Community Options and Resources (ANCOR) as of and for the year ended December 31, 2019, in accordance with auditing standards generally accepted in the United States of America, we considered ANCOR's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of ANCOR's internal control. Accordingly, we do not express an opinion on the effectiveness of ANCOR's internal control.

However, during our audit we became aware of the following matters that are opportunities for strengthening internal controls and operating efficiency.

Electronic Payments System

ANCOR uses a system that includes manual preparation of checks to pay bills. An electronic payment system can be particularly appropriate for vendor, utility, and expense reimbursement payments. Advantages of such a system include the elimination of manual handling, process, and storage of paper checks, reduced postage costs, and a reduction in the risk of check fraud or lost or stolen checks. We recommend ANCOR consider adopting an automated, electronic payment system, such as Bill.com and consider utilizing a third party expense reporting vendor, such as Expensify or Concur.

Consider Annual Cyber Security Training

As systems and processes move online, all organizations become more susceptible to cyber security threats from external sources. We recommend ANCOR implement an annual cyber security training to ensure staff are aware of the different types of cyber threats ANCOR could be exposed to. Topics to cover include the following:

- Malware: software that targets a specific device, system, or network with the goal of taking over a system
- Phishing: an email attack which involves deceiving the recipient into either disclosing sensitive information, downloading malware, or making unauthorized payments to the hacker
- Trojan: a type of malware which appears to be a legit software or source but then lets out a malicious code once within the system
- Ransomware: an attack on software which involves encrypting ANCOR's data and demanding payment in exchange for letting the user have full access to the data again

While not exhaustive, the list above are the most common cyber security threats that we recommend ANCOR consider on an annual basis. We also recommend ANCOR review its systems on an annual basis for the various threats discussed at the annual cyber security training.

We will review the status of these comments during our next audit engagement. We have already discussed these comments and suggestions with various ANCOR personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

This communication is intended solely for the information and use of management, the board of directors, and others within ANCOR, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

Wegner CPAs, LLP

Glenn Miller, CPA
Partner