

ALZHEIMER'S COMMUNITY CARE, INC. AND SUBSIDIARY
REPORT TO MANAGEMENT
FOR THE YEAR ENDED JUNE 30, 2025

March 6, 2026

To the Management of
Alzheimer's Community Care, Inc. and Subsidiary
West Palm Beach, Florida

In planning and performing our audit of the consolidated financial statements of the Alzheimer's Community Care, Inc. and Subsidiary (the Organization) as of and for the year ended June 30, 2025, we considered the Organization's system of internal control over financial reporting (internal control) for a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Organization's internal control. Accordingly, we do not express an opinion on the effectiveness of the Organization's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Organization's consolidated financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses. Given these limitations, during our audit we did not identify any deficiencies in internal control during our 2025 audit procedures that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

However, as discussed below, we identified certain matters involving the internal control and other operational matters that are presented for your consideration. This letter does not affect our report dated March 6, 2026 on the financial statements of the Organization. We will review the status of these comments during our next audit engagement. Our comments and recommendations, all of which have been discussed with appropriate members of management, are intended to improve the internal control or result in other operating efficiencies. We will be pleased to discuss these comments in further detail at your convenience, perform any additional study of these matters, or assist you in implementing the recommendations. Our comments are summarized as follows:

Current Year Comments

Lease Agreement

Comment

During our audit, we noted that there was no lease between Alzheimer's Community Care, Inc. and Alzheimer's Community Care Foundation. This is currently done under a verbal agreement concerning all aspects of the leasing arrangement.

Current Year Comments, Continued

Lease Agreement, Continued

Recommendation

We recommend that a lease be created in order to protect both parties and to eliminate potential issues that can arise from verbal agreements. The lease agreement should identify the parties involved, the detailed terms of the lease.

Management Response

Management will take this recommendation to the Board of Directors for approval.

Server Room

Comment

During our walkthrough, we observed that the server room was uncomfortably warm. Additionally, a sprinkler head was positioned directly above or very close to the cabinet.

Recommendation

We recommend carefully considering the risk of equipment being compromised. Although most data resides in cloud-based applications and the risk to data may be minimal, there is still potential for operations to be disrupted due to equipment damage. Furthermore, despite most documents being stored in Microsoft 365, some users still maintain information on the local file server.

Management Response

Management will take this recommendation to the Board of Directors for approval.

Prior Year Comments

Information Technology and Cybersecurity

Comment

During our audit procedures, we conducted interviews with members of management and staff and reviewed detailed information regarding information technology systems, protocols and cybersecurity. Our consideration of these procedures led us to provide the following recommendations as they relate to cyber threats, penetration testing, data storage and backup and cybersecurity training.

Recommendations

We recommended the Organization contract with an external specialist to periodically perform Information Technology (IT) security/access and network vulnerability testing and review the results with the appropriate management. Such a process will assist the IT department in determining gaps and areas of improvement as well as validate the effectiveness of its IT security efforts.

Top cybersecurity priorities for all industries include:

- Use managed detection and response services.

Prior Year Comments, Continued

Information Technology and Cybersecurity, Continued

Recommendations, continued

- Confirm information system resilience on a continual basis.
- Conduct diagnostic assessments of technical architecture.

Ransomware attacks have intensified worldwide, especially targeting internet of things (IoT) connected devices. There is a further significant increase in socially engineered spear-phishing attacks using fictitious emails and websites including fake CDC information, malicious webinar links, and fake government and healthcare issues. Threat environment examples through common business emails include:

Business executive receiving or initiating a request for a wire transfer

- The email accounts of C-level business executives are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests.
- In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular scenario has been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Business Executive Impersonation

- This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business.

Penetration Testing

Given the threat landscape, it is essential to know your Organization, data, and users are secure. This can be done by engaging an IT security firm for penetration testing, of which there are external and internal options. External penetration testing is the most common and simulates a hacking attempt by outsiders, whereas internal testing assumes some level of knowledge over current systems and is a bit more involved in costs, planning and execution. At a minimum, we recommend organizations undergo external penetration testing annually. If feasible, internal tests may also be beneficial.

2025 Status

The Organization has not conducted any form of penetration testing over the last two years. Given the threat landscape, it is essential to know your organization, data, and users are secure. This can be done by engaging an IT security firm for penetration testing, of which there are external and internal options. External penetration testing is the most common and simulates a hacking attempt by outsiders. Whereas internal testing assumes some level of knowledge over current systems and is a bit more involved in costs, planning and execution. At minimum we recommend firms undergo external penetration testing annually. If feasible, an internal test may also be beneficial.

Prior Year Comments, Continued

Information Technology and Cybersecurity, Continued

Microsoft 365

Currently, data storage, files, documents, spreadsheets, and the like, are split between the Microsoft 365 (M365) cloud environment and the local server environment. We strongly encourage the Organization to finish migrating any on premises data to M365.

This should be followed by a policy mandating the use of the cloud storage application. The policy should be further bolstered by the continued use of an external M365 backup as well as any supplemental content filtering and monitoring. Although data storage is better protected in the cloud, they still are susceptible to malicious actors, and additional security measures are recommended.

2025 Status

The migration of data to M365 is in progress. We strongly encourage the Organization to finish migrating any on premises data to M365. This should be followed by a policy mandating use of the cloud storage application. The policy should be further bolstered by the continued use of an external M365 backup as well as any supplemental content filtering and monitoring. Although data stores are better protected in the cloud, they still are susceptible to malefactors and the additional security measures are strongly advised.

Cybersecurity Training

Security awareness has become a critical piece of today's IT framework. Most ransomware and malware often originate via phishing emails, texts and other communications making end users a critical point in the Organization's security. A security training package such as KnowB4 is recommended. Such applications allow organizations to establish simulated phishing campaigns that can serve as a teaching experience. Such packages are bolstered by security training modules that can be required for all employees together with refresher training for anyone failing a phishing test. We recommend the Organization implement a formal program for cybersecurity training and testing.

2025 Status

This comment has been addressed. The Organization has made significant progress in addressing cybersecurity concerns with the introduction of native Microsoft Phishing tools. Furthermore, to comply with the requirements of a major funder, the group is transitioning to a more comprehensive testing tool, Ninjio. This new tool will enhance their ability to manage testing campaigns, conduct simulations, and provide follow-up training more effectively.

Capitalization Policy

Comment

During our audit, we noted the Organization capitalizes acquisitions of fixed assets using a threshold of \$2,500 in accordance with the Organization's current fixed assets policy.

Prior Year Comments, Continued

Capitalization Policy, Continued

Recommendation

The Internal Revenue Service provides guidelines that can be used to assist with establishing the policy of capitalizing purchases, and the Organization may consider increasing its current threshold to \$5,000. The increased capitalization threshold amount will assure that only significant assets with a useful life in excess of one year are maintained in the financial records.

2025 Status

This comment has been addressed.

Expanded Whistleblower Policy

Comment

During our audit, we noted the Organization has adopted a whistleblower policy. The purpose of a whistleblower policy is to provide a mechanism for employees to raise concerns regarding unethical conduct; questionable accounting, internal controls or auditing matters; or the reporting of fraudulent information. This policy is also intended to reassure employees they will be protected from harassment, discrimination, retaliation or victimization for whistle blowing in good faith. Such a policy should include but not be limited to:

- The confidential, anonymous submission by employees of complaints or concerns regarding illegal or unethical conduct; accounting, internal controls and auditing matters; and fraudulent financial reporting;
- The receipt, retention, investigation and resolution of all such complaints;
- The establishment of a committee and/or ethics hotline where such complaints will be taken seriously and addressed promptly, discreetly and professionally. The individuals charged with this oversight should be able to determine whether the complaint pertains to alleged illegal or unethical conduct; accounting, internal controls and auditing matters; or fraudulent financial reporting, and when possible, acknowledge receipt of the complaint to the sender;
- Questionable practices relating to accounting, auditing, internal financial controls, and financial fraud;
- Concerns regarding questionable or unethical banking practices;
- Direct or indirect offer, payment or promise to give money or anything of value to anyone to improperly influence the recipient's behavior;
- A conflict of interest;
- Misappropriation (for one's own use) of funds that have been entrusted to a person for care or management;
- Falsification, fabrication, forgery, or unauthorized alteration of a record, including accounting records, expense reports, customer invoices, time sheets, or other electronic hard copy School records providing false or misleading information to third parties;

Prior Year Comments, Continued

Expanded Whistleblower Policy, Continued

- The act of stealing; specifically, the unauthorized taking and/or removing of property with intent to deprive the rightful owner of it; and,
- Any other unethical business practice or illegal activity.

Recommendation

We recommend the Organization enhance the adopted whistleblower policy as follows:

- Establish a method for confidential communication of whistleblower complaints;
- Identification of an individual or committee who will receive and investigate whistleblower complaints;
- Establish the procedures for receipt, documentation, investigation, and resolution of whistleblower complaints.

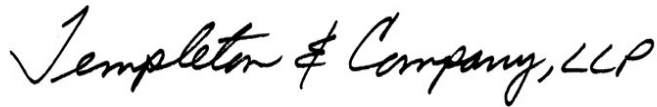
Status

This comment has been addressed.

We thank the Organization and management for their assistance and the many courtesies extended to us during our audit. We sincerely appreciate this opportunity to serve the Organization.

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

Very truly yours,

A handwritten signature in black ink that reads "Templeton & Company, LLP". The signature is written in a cursive, flowing style.

Templeton & Company, LLP