

The April 2020 Arizona Department of Education special audit found that the Department needs 21 staff for Program workload, should improve customer service and timely processing of Program applications, and better protect personally identifiable information. We made 26 recommendations to the Department, and its status in implementing the recommendations is as follows:

## Status of 26 recommendations

Implemented	13
Implemented in a different manner	3
Partially implemented	1
No longer applicable	1
<b>Not implemented</b>	<b>8</b>

As of our 36-month followup issued in September 2023, 8 recommendations were not yet implemented, including several recommendations related to identifying misspending violations and providing quality and timely customer service to Program participants. As part of our assessment of the Department's efforts to implement these 8 outstanding recommendations, during this 48-month followup, we planned to conduct work in the following specific key areas to assess the Department's efforts to:

1. Conduct a risk-based review of ClassWallet transactions and Program accounts using various risk factors it has developed to guide its selection of these transactions and accounts for review to help ensure the appropriateness of Program expenditures and identify unallowable purchases and/or instances of misspending. Additionally, as of September 2023 and as reported in our 36-month followup, the Department had a backlog of more than 366,000 Program purchases/transactions that were awaiting review, and we planned to assess the Department's efforts to reduce this backlog.
2. Implement controls to prevent/detect fraud in response to a State Grand Jury indicting several individuals, including former Program employees, for allegedly engaging in fraud, money laundering, and other crimes related to the Program.<sup>1</sup>
3. Address an information technology (IT) security issue that occurred in the summer of 2023 related to sensitive Program data and information.<sup>2</sup> According to the Arizona Department of Homeland Security, a parent was able to access personally identifiable information of other Program parents and students in ClassWallet, including names of the students, home shipping addresses, and information that could be used to infer that a student may have a learning disability.

However, the Department failed to respond to multiple requests made over a 4-month period to provide us with information and documentation to conduct our work, as follows:

<sup>1</sup> On February 29, 2024, the Arizona Attorney General announced a State Grand Jury indictment of 5 individuals, including 3 Department staff and 2 family members of 1 of these staff, charging them with the following 40 felony counts: conspiracy (1), fraudulent schemes and artifices (1), illegally conducting an enterprise (1), computer tampering (1), money laundering (5), and forgery (31).

<sup>2</sup> We revised this sentence to include the word "issue" to more closely align our reporting to language referenced by the Department and the Arizona Department of Homeland Security's Cyber Incident Executive Summary regarding an IT security issue that occurred in 2023. This report version issued on July 18, 2025 replaces the report originally issued on and dated November 1, 2024.

- **June 2024**—We initiated our 48-month followup and requested that the Department provide a response and supporting documentation by July 8, 2024.
- **July 2024**—3 days prior to the deadline, the Department requested a 2-month extension to provide its response, citing its inability to meet the original deadline because of competing priorities.<sup>3</sup> We agreed to extend the deadline for its response to September 13, 2024, and requested that the Department provide a timely and comprehensive response, including supporting documentation.
- **September 2024**—The Department failed to provide a response by September 13, 2024, and requested a meeting to discuss alternative approaches for responding to our request and providing documentation. We subsequently met with Department officials on September 24, 2024, and they agreed to begin incrementally providing us with information/documentation necessary for our follow-up work starting the first part of October 2024.
- **October 2024**—As of October 22, 2024, the Department had provided only 4 documents—all related to the ClassWallet contract—some of which were already publicly available.

Given the Department's failure to meet several deadlines for providing a response, some of which the Department specifically requested, and our need to transition team members assigned to conduct this followup to other planned follow-up work, we are concluding this 48-month followup.

We will initiate another followup with the Department by January 2025 to assess its efforts to address the recommendations from our April 2020 report, including reviewing its continued implementation of recommendations we previously determined to be implemented, if warranted. We will also assess its efforts to reduce the backlog of Program purchases/transactions needing review, its implementation of controls to prevent/detect fraud, and steps it has taken to address the 2023 IT security issue.<sup>4</sup>

<sup>3</sup> The Department reported it was focused on responding to inquiries received from the Arizona Attorney General's Office related to areas of the Program potentially not authorized by statute and modifying some of its day-to-day operations to implement changes required by newly passed legislation.

<sup>4</sup> We revised this sentence to include the word "issue" to more closely align our reporting to language referenced by the Department and the Arizona Department of Homeland Security's Cyber Incident Executive Summary regarding an IT security issue that occurred in 2023. This report version issued on July 18, 2025 replaces the report originally issued on and dated November 1, 2024.