THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 4, 2018

Mr. Brian Schultz
Chairman
Central New York Regional Transportation Authority
200 Cortland Avenue
P.O. Box 820
Syracuse, NY 13205-0820

Re: Compliance With Payment Card Industry Standards
Report 2018-F-5

Dear Mr. Schultz:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have followed up on the actions taken by officials of the Central New York Regional Transportation Authority to implement the recommendations contained in our audit report, "Compliance With Payment Card Industry Standards" (Report 2016-S-31).

Background, Scope, and Objectives

The Central New York Regional Transportation Authority (Authority) is a public benefit corporation that was created in 1970 to provide transportation services in Onondaga, Oswego, Cayuga, and Oneida counties. The Authority accepts credit cards as a method of payment from its customers for bus fares and parking fees. All organizations that accept credit cards as a method of payment, such as the Authority, must comply with Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council (Council).

The PCI DSS are a comprehensive set of technical and operational requirements designed to protect cardholder data. The requirements apply to all system components included in, or connected to, the Cardholder Data Environment (CDE), which is comprised of the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data. Entities that do not comply with the PCI DSS may be subject to fines and penalties, and lose the public's confidence and the ability to accept credit card payments. In calendar year 2017, the Authority reported 32,925 credit card transactions totaling about $866,500 in revenue.

Our initial audit report, which was issued on February 6, 2017, determined whether

the Authority complied with payment card industry security standards. The audit covered the period January 1, 2015 through June 24, 2016. We found the Authority did not have a developed Information Security Policy (Policy) that addressed all of the requirements in the PCI DSS, and the Authority could also improve certain other technical safeguards over the cardholder data it processes. As a result of the audit, the Authority took some actions to address the security over cardholder data. However, the Authority still needed to take additional steps to improve its overall information security program to ensure it met the PCI DSS.

The objective of our follow-up audit was to assess the extent of implementation, as of April 12, 2018, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

The Authority has made significant progress in implementing the recommendations identified in the initial audit report. Of the two prior audit recommendations, one has been implemented, and one has been partially implemented.

Recommendation 1

Develop strategies to enhance compliance with PCI DSS. This should include, but not be limited to:

- *Developing and disseminating a Policy and procedures that clearly define information security responsibilities for all personnel;*
- *Inventorying all assets related to payment card processing activities;*
- *Strengthening physical security over all systems that receive, process, transmit, and maintain cardholder data; and*
- *Meeting PCI DSS user account and password requirements.*

Status - Implemented

Agency Action - Authority officials have developed strategies to enhance compliance with the PCI DSS. In November 2017, the Authority hired a contractor to assist with a PCI DSS compliance review. The Authority also developed and issued an updated Employee Acceptable Use Policy to all staff, which includes defined roles and information security responsibilities for all personnel, as well as updated password guidelines that reflect PCI DSS requirements. Authority officials have created an inventory of assets used for payment card processing activities that includes device descriptions, functions, and locations. Additionally, we found Authority officials have taken steps to strengthen physical security, such as adding security cameras in some areas where credit card processing takes place.

Recommendation 2

Implement the recommendations detailed during the audit for strengthening technical controls over cardholder data.

Status - Partially Implemented

Agency Action - During our initial audit, we issued a preliminary report and a confidential draft report to the Authority. The reports contained a total of 17 recommendations. Our review found that, of the 17 recommendations, six recommendations have been implemented, six have been partially implemented, two have not been implemented, and three are no longer applicable.

Major contributors to this report were Brian Krawiecki, Jared Hoffman, Holly Thornton, and Christopher Bott.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues in this report. We thank the management and staff of the Central New York Regional Transportation Authority for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Nadine Morrell, CIA, CISM, CGAP
Audit Manager