THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

September 27, 2019

Ms. Joanne M. Mahoney
Chair
Thruway Authority
200 Southern Blvd.
Albany, NY 12201

Re: Compliance With Payment Card Industry Standards
Report 2019-F-14

Dear Ms. Mahoney:

Pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Article II, Section 2803 of the Public Authorities Law, we have followed up on the actions taken by officials of the Thruway Authority to implement the recommendations contained in our audit report, *Compliance With Payment Card Industry Standards* (Report 2017-S-11).

Background, Scope, and Objective

The Thruway Authority (Authority) operates and maintains a toll superhighway (Thruway) throughout New York State. Most of the toll points along the Thruway only accept cash and E-ZPass charges as toll payment. All Thruway E-ZPass customers have prepaid accounts, from which tolls are electronically deducted when the vehicle passes through toll points. Most E-ZPass accounts are automatically replenished with the customer's credit card on file, and the Authority contracts with a third-party vendor to manage E-ZPass accounts. The Authority directly handles in-person credit card payments for E-ZPass tags at its administrative headquarters in Albany and at an outreach center in Nyack, as well as at special events throughout the State. The Authority also accepts credit card payments over the phone, online, and in person for other costs (e.g., unpaid tolls, accident reports, commercial accounts). From January 1, 2018 through December 31, 2018, the Authority reported processing approximately 86,000 credit card transactions totaling about $1.7 million.

All organizations that accept credit cards as a method of payment must comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council. The PCI DSS is 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, which is composed of the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.

Our initial audit report, issued on September 19, 2017, examined whether the Authority complied with PCI DSS. The audit covered the period March 1, 2017 through June 5, 2017. We found the Authority did not have a developed information security program, including policies, risk assessments, and inventories, to satisfy all PCI DSS requirements. As a result of the audit, the Authority took various actions to bolster security over cardholder data. However, the Authority still needed to take additional steps to improve its overall information security program to ensure it meets PCI DSS.

The objective of our follow-up audit was to assess the extent of implementation, as of August 23, 2019, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

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

Follow-Up Observations

Recommendation 1

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

- *Inventorying all assets related to payment card processing activities;*
- *Conducting a PCI risk self-assessment;*
- *Developing and disseminating policies and procedures that clearly define information security responsibilities for all personnel; and*
- *Strengthening physical security over all systems that receive, process, transmit, and maintain cardholder data.*

Status – Partially Implemented

Agency Action – Authority officials have developed strategies to enhance compliance with the PCI DSS. For example, the Authority created an inventory of assets used for payment card processing activities and has started to conduct risk assessments. However, while the Authority partially completed self-assessment questionnaires for 2017 and 2019, it did not do so for 2018. Further, the Authority developed a policy for protecting credit card information and issued it to all staff. The policy covers security responsibilities for all personnel who use cardholder data and requires annual on-the-job training for all such employees. Additionally, Authority officials developed specific PCI DSS-related policies and procedures for the three

departments that directly handle cardholder data. Finally, we found Authority officials have taken some steps to strengthen physical security over credit card systems.

Recommendation 2

Implement the recommendations detailed during the audit, but not addressed in this report due to confidentiality reasons, for strengthening technical controls over cardholder data.

Status – Implemented

Agency Action – During our initial audit, we issued two preliminary reports and a confidential draft report to the Authority. Of the reports' 17 total recommendations, 14 were implemented, 1 was partially implemented, and 2 were no longer applicable.

Major contributors to this report were Brian Krawiecki, Renee Boel, Melissa Davie, Christopher Bott, and Nicole Tommasone.

We thank the management and staff of the Thruway Authority for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Nadine Morrell, CIA, CISM
Audit Manager

cc: Matthew J. Driscoll, Executive Director