NEW YORK STATE OF OPPORTUNITY. | Thruway Authority

ANDREW M. CUOMO
Governor

JOANNE M. MAHONEY
Chair

MATTHEW J. DRISCOLL
Acting Executive Director

December 18, 2017

Honorable Andrew M. Cuomo
Governor
NYS Executive Chamber
State Capitol, 2nd Floor
Albany, New York 12224

Honorable Thomas P. DiNapoli
Comptroller
Office of the New York State Comptroller
110 State Street
Albany, New York 12201

Dear Sirs,

On behalf of Chair Mahoney, this letter is in response to the NYS Office of the State Comptroller's (OSC) Audit Report 2017-S-11, which assesses the New York State Thruway Authority's (Authority) *Compliance With Payment Card Industry (PCI) Standards* conducted for the period of March 1, 2017 through June 5, 2017. In accordance with Section 170 of the Executive Law, within ninety days of the release of the final report, we are advising you and the leaders of the Legislature and fiscal committees of the Authority's progress to date regarding the recommendations contained in the report.

The Authority is a public benefit corporation that is required to, and fully complies with, all NYS Office of Information Technology Services (ITS) policies and standards. These ITS policies define security controls, requirements, protocols, and processes that protect systems, network, and data. In addition to these ITS policies, the Authority has developed, documented, and distributed procedures and guidelines that support these policies.

Over 99.9% of the Authority's customer credit card activity is processed directly by our contracted E-ZPass vendor and was in full compliance with PCI Data Security Standards (DSS). This audit focused on less than 0.1% of our credit card activity and did not find that any of the Authority's credit card data had been lost, stolen, or compromised in any way. The Authority has never stored, nor do we ever intend to store, any customer's credit card information on any of our network servers.

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.

Response: The Authority implemented supplementary measures that further enhanced its existing PCI DSS compliance with the following actions:

- The Authority has completed inventorying all assets related to its payment card processing activities including completely defining its Cardholder Data Environment (CDE);
- The Authority has completed a PCI Self-Assessment Questionnaire (SAQ) to evaluate its compliance with PCI DSS. This included a risk assessment and identifying security vulnerabilities to its CDE;
- The Authority developed and disseminated additional policies and work unit procedures that more clearly define information security responsibilities for all personnel regarding PCI DSS;
- The Authority has continued to ensure all personnel with access to customer cardholder data are appropriately trained in PCI DSS compliant work unit procedures; and
- The Authority further strengthened its physical security over all systems that receive, process, transmit, and maintain cardholder data.

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.

Response: Based on the findings and detailed recommendations of the audit, the Authority has implemented supplement measures that further enhanced its existing technical controls over customer cardholder data, including those outlined above.

The Authority has addressed and implemented all recommendations.

Sincerely,

Matthew J. Driscoll

CC: Senator John J. Flanagan, Temporary President and Majority Leader
Senator John A. DeFrancisco, Deputy Majority Leader for Legislative Operations
Senator Jeffrey D. Klein, Independent Democratic Conference Leader
Senator Catharine M. Young, Chair, Finance Committee
Senator Andrea Stewart-Cousins, Democratic Conference Leader
Senator Liz Krueger, Ranking Democratic Member, Finance Committee
Assemblymember Carl E. Heastie, Speaker
Assemblymember Joseph D. Morelle, Majority Leader
Assemblymember Helene E. Weinstein, Chair, Ways and Means Committee
Assemblymember Brian M. Kolb, Minority Leader
Assemblymember Bob Oaks, Ranking Member, Ways and Means Committee
Mr. Brian Reilly, Audit Director, Office of the State Comptroller