DELAWARE RIVER
PORT AUTHORITY

STEWARDSHIP. SERVICE. COMMUNITY.

One Port Center
PO Box 1949
2 Riverside Drive
Camden, NJ 08101

(856) 968-2000
(856) 968-2001 Fax
www.drpa.org

David J. Aubrey, CIA, CFE
Acting Inspector General
Office of the Inspector General

OIG Memorandum

TO: J. M. White, Chief Financial Officer

FROM: D. J. Aubrey, Acting Inspector General

SUBJECT: Review of Service Organization Controls (SOC) Reports for NJ E-Z Pass

DATE: May 31, 2018

As part of the Office of the Inspector General (OIG) IT audit focus, we have reviewed the most current and available Service Organization Controls reports for the New Jersey E-Z Pass service provider (see attachments; the attached reports are noted as "*restricted use",* please handle accordingly). This review was performed by R. McReynolds, IT Auditor, with reports provided by Patricia Griffey, Manager, Revenue Audit. The objective of this review is to provide Authority management with reasonable assurance that the third-party service providers for the New Jersey E-Z Pass system have controls in place to mitigate risk regarding security, availability, processing integrity, confidentiality, privacy, and that the controls have been tested and any material issues remediated. The New Jersey E-Z Pass system has two service providers: 1) Conduent provides the application and transaction processing services, and 2) Atos provides the supporting datacenter services. Conduent and Atos provide third-party system support for processing the Authority's bridge E-Z Pass toll transactions. To accomplish this review OIG has reviewed the following audit reports:

- Conduent SOC1 Report (SOC1);
- Atos SOC1 Report (SOC1);
- Conduent SOC Bridge Letter through December 31, 2017;
- Atos SOC Bridge Letter through December 31, 2017;
- 2017 New Jersey E-Z Pass SOC 1 Audit Exceptions; and,
- 2016 Xerox NJ PCI DSS ver3.1 AOC.

The scope of the SOC reports provided and reviewed were valid from October 1, 2016 through September 30, 2017 with a “bridge letter” for the period October 1, 2017 through December 31, 2017. The PCI / DSS (Payment Card Industry / Data Security Standards) attestation report provided for Xerox State & Local Solutions Inc. State Government Transportation New Jersey E-Z Pass (currently doing business as Conduent) was dated October 14, 2016.

These independent audit reports are control attestations provided by the third-party service provider to provide assurance to their clients (in this case, the Authority) that the contracted services and facilities have an adequate control environment in place to protect our data. The reports also document the testing and results of the controls by the independent attesting organization. The referenced reports were completed by the independent attesting organization, Ernst & Young from Rochester, NY and Dallas, TX, and Cadence Assurance, Salt Lake City, UT.

The New Jersey E-Z Pass application service provider’s (Conduent & Atos) policies and procedures were evaluated for system access and operations controls. The service providers’ locations were reviewed for adherence to policy and procedures for logical access to systems, physical security, network security, environmental protection, power backup, fire alert and suppression capabilities, application hosting, and data backup. Based on review of the reports provided, it was disclosed that the independent attesting organization, Ernst & Young, did not opine on the service providers’ disaster recovery plan or the payment card industry (PCI) standards.

For the period October 1, 2016 through September 30, 2017, Ernst & Young reported three exceptions resulting from their testing of the controls for the New Jersey E-Z Pass system (see attached report, “2017 New Jersey E-Z Pass SOC 1 Audit Exceptions”); two of the exceptions were financial management related, and the other exception was associated with the logical security of IT controls. Specific details of the reported exceptions are noted below:

1. “For 12 of 25 days, the Supervisor/Team Lead at the Camden WIC did not initial the Till Log when the bank was returned to the safe.” Management Response: “*As of October 4, 2017, Management has re-enforced the process related to the daily Till Logs, including appropriately initialing and signing documentation, with process owners.”*

2. “For one (1) of 25 days sampled, the Supervisor did not initial the Reconciliation Sheet upon completing the reconciliation. Per inspection of the Reconciliation sheet, it was determined that the Supervisor appropriately completed the review and reconciliation upon the bank being returned, as evidenced by tickmarks and notes.” Management Response: *“As of October 4, 2017, Management has re-enforced the process related to the daily reconciliations, including appropriately initialing and signing documentation, with process owners.”*

3. “For one (1) of four production databases supporting the NJ E-ZPass® CSC, the database password minimum length requirement within was not configured in accordance with Conduent policy.” Management Response: *“On October 30, 2017, Atos updated the password configuration for the referenced Oracle database to bring the password minimum length requirement into compliance with Conduent policy.”*

The reported exceptions were addressed by Conduent in a timely and effective manner.

The bridge letters from Conduent and Atos state that the controls have not changed from October 1, 2017 through December 31, 2017. Based on our review of the reported results from the independent attesting organization, OIG concurs with the conclusion that an appropriate control environment exists at Conduent and Atos. Ernst and Young did not opine on the service providers’ disaster recovery plans and PCI standards compliance. The PCI / DSS attestation report for standards compliance provided for Conduent (formerly Xerox) was attested by Cadence Assurance as of October 14, 2016.

OIG has discussed the results of this review with CFO J. White and P. Griffey, Manager, Revenue Audit, who agreed with the reported results, and have actively reached out to their contacts at the New Jersey Turnpike requesting additional information related to disaster recovery and system / data back-up practices, as well as the current status of PCI standards compliance for the third-party service providers for New Jersey E-Z Pass services.

Our Office will continue to work with Authority management in review of externally hosted system and datacenter controls as the annual SOC audits are conducted and reports made available.

Attachments (*restricted use*)
(Note: The noted attachments have not been included due to their proprietary and confidential nature.)

cc: R. Boyer
J. Nash
E. DePasquale
R. Taylor
S. Murphy
A. Nelson
J. Hanson
R. Santarelli
M. Wing
K. LaMarca,
P. Griffey
R. McReynolds