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
Inspector General
Office of the Inspector General

OIG Memorandum

TO: J. M. White, Chief Financial Officer

FROM: D. J. Aubrey, Inspector General

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

DATE: November 4, 2019

The Office of the Inspector General (OIG) recently performed a review of 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. 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); and,
- Conduent SOC Bridge Letter.

The scope of the SOC report provided and reviewed was valid from November 1, 2017 through October 31, 2018, with a "bridge letter" for the period November 1, 2018 through December 31, 2018.

The independent audit report is a control attestation 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 report also documents the testing of the controls and the results by the independent attesting organization. The referenced report was completed by the independent attesting organization, Ernst & Young from Rochester, NY.

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 report 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 November 1, 2017 through October 31, 2018, Ernst & Young reported several exceptions resulting from their testing of the controls for the New Jersey E-Z Pass system (see attached report, "E18-073 (Qualified) New Jersey E-Z Pass SOC 1 Report"); three of the exceptions were management related, and the other exceptions were associated with the logical security of IT controls. Specific details of the reported exceptions are noted below:

1. **Control Activity Affected**:
   Control Objective 2: Controls provide reasonable assurance that transactions which are generated by home and away agencies are received, reconciled, summarized and posted to the respective customer accounts.

   Control Activity 2.2: On a monthly basis, TRXN00Q15 report, showing transactions that were not successfully processed, is reviewed to help ensure that received transactions have been processed.

   Issue Reported by Ernst & Young:
   For 2 of 2 months sampled, the analyst did not accurately document the results of their review. Per inspection of the VECTOR application and the TRXN00Q15 report, the rejected transaction count reconciled and were accurately processed.

   Conduent Management Response:
   The deviations noted were related to the use of an incorrect formula. The formula was corrected the same day the error was found. Going forward, all spreadsheets will be reviewed by Finance Management before moving to production

2. **Control Activity Affected**:
   Control Objective 5: Controls provide reasonable assurance that incoming and outgoing customer correspondence are properly routed and processed.

   Control Activity 5.5: Scanned correspondence is uploaded into VECTOR as an open service request and are processed by the correspondence clerks based on

oldest date and CSR skill set. Using the SRV0328 report, the correspondence supervisor updates the correspondence backlog report and sends an email to management to report on the department's productivity.

Issue Reported by Ernst & Young:
For (Three) 3 of 25 sampled days, documentation to support the review and communication of the correspondence backlog report was not available. Per inquiry of the customer care supervisor, the correspondence was tracked and communicated to management.

Conduent Management Response:
While the reports were not generated and distributed, Management still performed the review of the department's productivity. Conduent was able to provide the data from VECTOR that was used to support the review management to report on the department's productivity.

3. **Control Activity Affected**:
Control Objective 6: Controls provide reasonable assurance that tags are properly tracked in inventory.

Control Activity 6.1: Upon receipt of new tags, the packing slip is compared to the number of boxes delivered and the number of units per box and signed by the Team Lead (Tag Distribution Department).

Issue Reported by Ernst & Young:
For twelve (12) of 27 sampled packing slips, the packing slips were not manually signed by the Team Lead (Tag Distribution Department) upon receipt.

Conduent Management Response:
While the packing slips were not signed upon receipt, the number of tags received agreed with the number of tags entered into VECTOR for each shipment.

4. **Control Activity Affected:**
Control Objective 9: Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances and protect data from unauthorized changes.

Control Activity 9.6: Developers do not have the ability to migrate code to the production environment.

Issue Reported by Ernst & Young:
Access to system accounts on the Oracle database, which permits make changes to the database, and add/modify transactions and user profiles, is not limited to authorized and appropriate Conduent IT personnel. Additionally, the activity of these accounts was not monitored throughout the period.

Conduent Management Response:
Conduent personnel, including developers, were utilizing Linux and Oracle system accounts to access the production database for problem determination purposes. In December 2018, Conduent installed a new tool, the PCI Trigger which, if enabled, would record access to these accounts and if so configured would block such access. This technology will be fully enabled by March 31, 2019. Additionally, a formal access exemption process was implemented along with the PCI Trigger to document the approval of the use of these system accounts. When any unauthorized credential usage is identified, personnel involved are counseled that such usage is prohibited by Conduent's policies and procedures. A factor mitigating risk is the relational nature of the Oracle databases supporting the VECTOR application, which makes it inherently difficult to maliciously alter data without detection. Conduent's day-to-day control operations, including the QA Department's review and service request process, detected no unauthorized changes or transactions resulting from this access.

5. Control Activity Affected:
Control Objective 10: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

Control Activity 10.2: Access to the VECTOR application and database is restricted to authorized users.

Issue Reported by Ernst & Young:
Access to system accounts on the Oracle database, which permits make changes to the database, and add/modify transactions and user profiles, is not limited to authorized and appropriate Conduent IT personnel. Additionally, the activity of these accounts was not monitored throughout the period.

Conduent Management Response:
Conduent personnel, including developers, were utilizing Linux and Oracle system accounts to access the production database for problem determination purposes. In December 2018, Conduent installed a new tool, the PCI Trigger which, if enabled, would record access to these accounts and if so configured would block such access. This technology will be fully enabled by March 31, 2019. Additionally, a formal access exemption process was implemented along with the PCI Trigger to document the approval of the use of these system accounts. When any unauthorized credential usage is identified, personnel involved are counseled that such usage is prohibited by Conduent's policies and procedures. A factor mitigating risk is the relational nature of the Oracle databases supporting the VECTOR application, which makes it inherently difficult to maliciously alter data without detection. Conduent's day-to-day control operations, including the QA Department's review and service request process, detected no unauthorized changes or transactions resulting from this access.

6. **Control Activity Affected:**
Control Objective 10: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

Control Activity 10.3: Terminated employees access to the VECTOR application and Windows domain is disabled upon notification.

Issue Reported by Ernst & Young:
For four (4) of 9 terminated employees sampled, the employees' access to the Windows domain was not disabled upon notification.

Conduent Management Response:
While Windows Active Directory access had not been removed timely, VECTOR and database access was. Additionally, the four users' computers were returned on the last day of employment. Management further verified their last logins to the Windows domain was prior to their termination dates.

7. **Control Activity Affected:**
Control Objective 10: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

Control Activity 10.7: Passwords for the systems are required to comply with established Conduent or client policies. The password requirements include:
• Expiration ·Minimum Length ·History ·Complexity ·Lockout after unsuccessful login attempts.

Issue Reported by Ernst & Young:
For fifteen (15) of 1,465 accounts with access to the Active Directory, the accounts' password expiration settings were not set in accordance with Conduent policy.

Conduent Management Response:
Conduent and Atos have reviewed all Active Directory accounts with non-expiring passwords and have determined which are valid system/service accounts. For any remaining accounts, Conduent has taken appropriate action to disable or monitor the accounts for disabling as appropriate.

8. **Control Activity Affected:**
Control Objective 10: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

Control Activity 10.9: Developers do not have functional end-user access into the production VECTOR application, database or job scheduler.

Issue Reported by Ernst & Young:
Access to system accounts on the Oracle database, which permits make changes to the database, and add/modify transactions and user profiles, is not limited to authorized and appropriate Conduent IT personnel. Additionally, the activity of these accounts was not monitored throughout the period.

Conduent Management Response:
Conduent personnel, including developers, were utilizing Linux and Oracle system accounts to access the production database for problem determination purposes. In December 2018, Conduent installed a new tool, the PCI Trigger which, if enabled, would record access to these accounts and if so configured would block such access. This technology will be fully enabled by March 31, 2019. Additionally, a formal access exemption process was implemented along with the PCI Trigger to document the approval of the use of these system accounts. When any unauthorized credential usage is identified, personnel involved are counseled that such usage is prohibited by Conduent's policies and procedures. A factor mitigating risk is the relational nature of the Oracle databases supporting the VECTOR application, which makes it inherently difficult to maliciously alter data without detection. Conduent's day-to-day control operations, including the QA Department's review and service request process, detected no unauthorized changes or transactions resulting from this access.

All reported exceptions are being addressed by Conduent management.

Ernst and Young has opined in the report that “Control Objective 9 and Control Objective 10” were not suitably designed to achieve the control objectives. Ernst and Young continues, that beside the control objectives stated, in all material respects, the system description fairly represents the system and the control objectives were suitably designed so that the control objectives would be achieved.

OIG concurs with the Ernst and Young’s opinion and suggests that Authority management follow up with Conduent to: 1) determine the current state of Conduent’s disaster recovery plan and PCI standards compliance which are both critical areas and were not opined upon by Ernst and Young, as well as, 2) determine the remediation status of reported issues associated with both Control Objectives 9 and 10 due to their sensitive nature (the issues are summarized within this report and detailed within the referenced SOC 1 Report).

The bridge letter from Conduent states that the controls have not changed from November 1, 2018 through December 31, 2018.

OIG has discussed the results of this review with CFO J. White and P. Griffey, Manager, Revenue, who agreed with the reported results and recommendation, and will reach out to their contacts at the New Jersey Turnpike (lead agency for the NJ E-Z Pass Group) prior to November 29, 2019, requesting additional information related to disaster recovery and system / data back-up practices, the current status of PCI standards compliance for the third-party service providers, and remediation efforts regarding reported issues

pertaining to Control Objectives 9 and 10. The CFO agreed to forward the responses to these inquiries to OIG once received.

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