TECHNOLOGY & INNOVATION
E-COMMERCE TRANSACTION
EFFECTIVENESS REVIEW
AUDIT 19-15
October 25, 2019

CITY OF TAMPA

Jane Castor, Mayor **Internal Audit Department**

Christine Glover, Internal Audit Director

October 25, 2019

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: E-commerce Transaction Effectiveness Review, Audit 19-15

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Technology & Innovation, E-commerce Transaction Effectiveness Review.

We thank the aforementioned management and staff for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Russell Haupert, Chief Technology Officer
Ernest Mueller, Senior Assistant City Attorney II
Don Disler, MIS Project Leader
Rob Edwards, MIS Project Leader

TECHNOLOGY & INNOVATION
E-COMMERCE TRANSACTION
EFFECTIVENESS REVIEW
AUDIT 19-15

/s/ Anthony D. Tiwari

Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION
E-COMMERCE TRANSACTION
EFFECTIVENESS REVIEW
AUDIT 19-15

BACKGROUND

Electronic commerce (e-commerce) refers to any type of business or commercial transaction that involves the transfer of information across the Internet. E-commerce has become a business-critical function of the Internet for virtually every enterprise[1]. The City of Tampa (COT) uses e-commerce functions to conduct daily, business-to-business and business-to-customer, online transactions. The Technology & Innovation Department (T&I) has a division designated to manage the technical aspects of COT's e-commerce functions.

The division oversees the technical processes and maintenance of the e-commerce infrastructure. The infrastructure allows for seamless credit card payment transactions between the customer and department that offer online payments for services.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY19 Audit Agenda. The objectives of the audit were to assess:

1. The effectiveness of internal controls for managing e-commerce applications.

2. The controls in place to protect and secure e-commerce transactions.

3. The number of failed e-commerce transactions.

4. The process to effectively identify and remediate failed e-commerce transactions.

STATEMENT OF SCOPE

The audit period covered 2018 and 2019. Both qualitative and quantitative assessments were performed to determine whether the management and staff of the division were fulfilling their stated duties and responsibilities in an effective and efficient manner. Original records as well as copies were used as evidence and verified through observation and physical examination.

[1] E-commerce & PKI Assurance, Control Objectives for Information and Related Technologies.

STATEMENT OF METHODOLOGY

We achieved our audit objectives by utilizing the following methods:

1. Conducted interviews with management to gain an understanding of the internal control environment.

2. Researched external frameworks to gain an understanding of the management of an e-commerce infrastructure.

3. Reviewed internal policy and procedures manuals to determine alignment with industry best practices.

4. Performed a data reliability analysis to determine completeness and accuracy of system-generated information used by management.

5. Reviewed contracts between COT and the vendor to gain an understanding of the agreement for services provided.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

NOTEWORTHY ACCOMPLISHMENTS

In order to mitigate the many risks associated with the management of e-commerce transactions, the division has implemented methodical processes to identify application issues and early detection of failed transactions.

AUDIT CONCLUSIONS

Based upon the audit work performed, our conclusions are as follows:

1. The internal controls for managing e-commerce applications are effective; however, there is a need for a risk-based approach to monitoring outsourced vendors that process e-commerce payments.

2. The controls in place to protect and secure e-commerce transactions are effective and aligned to T&I’s policies.

3. The number of failed e-commerce transactions are acceptable to industry standard.

4. The process to effectively identify and remediate failed e-commerce transactions are supported with automated and manual monitoring for full accountability between departments.

VENDOR RISK MANAGEMENT

STATEMENT OF CONDITION: The T&I administration has outsourced the e-commerce payment process, to third party vendors, for all credit card payments. The contract for services between the vendor and COT allows COT to monitor the vendor's security and overarching Payment Card Industry Data Security Standard (PCI-DSS) requirements. However, there has been no prior review of the vendors' independent auditor report on their PCI compliance, security, or business continuity measures.

CRITERIA: The T&I administration uses PCI-DSS framework standards, which require maintaining a program to monitor the service providers' compliance status at least annually. The guidelines further recommend that reports and records provided by the third party should be regularly monitored, and reviewed. This includes reviewing third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.

CAUSE: T&I's administration has not adopted best practices to utilize a formal third party risk management process. The contract between the vendor and COT in section 2.9 Reporting and Query Requirements, describes that the Statement on Standards for Attestation Engagements Statement report (SSAE 16) is available on a yearly basis, within 60 days after being published, by their independent auditors.

EFFECT OF CONDITION: The vendor may be exposed to data breaches, operational failure and business continuity issues described in an independent auditor's SSAE 16 report. Inadequate controls on the vendor's network could allow security threats to COT customers as the vendor has authorization to process PCI data.

RECOMMENDATION: T&I should select a risk-based program for monitoring third party relationships and reviewing the independent auditor's SSAE 16 reports; specifically those service organizations that involve critical activities with the potential to be exposed to significant risk. T&I should align the required policies, processes and guidelines to the objectives of the monitoring program.

MANAGEMENT RESPONSE: T&I recognizes the need for adequate monitoring of the controls for these third party payment processors. As part of our normal risk management process, we routinely monitor these providers, and handle general compliance for these under our respective comprehensive external financial, PCI, and Criminal Justice Information Services (CJIS) audits. In the past, we have and do review System and Organization Controls Report (SOC) reports when requested as part of the yearly external financial audit, as is currently the case with Oracle on Demand.

The City utilizes Cybersource and PlugandPlay as e-Commerce gateways. Cybersource has been in existence since 1994 and is a division of Visa Inc with over 400,000 merchants globally across major industries. Plug'n Pay Technologies has been providing e-commerce solutions to more than 40,000 merchants since 1996. While these are respected and well run organizations, we agree with the audit comments, and have requested the appropriate reports from each company for an immediate review.

While not previously requested by our external audits, we are adding these vendors to the appropriate external audit list items to ensure an annual review.

TARGET IMPLEMENTATION DATE: October 1, 2019 and immediate and ongoing from then.