ORLANDO VENUES

PCI COMPLIANCE REVIEW

Exit Conference Date: May 1, 2019

Release Date: June 7, 2019

Report No. 19-14

City of Orlando
Office of Audit Services and Management Support

George J. McGowan, CPA
Director

Co-source Partner
RSM

CITY OF
ORLANDO

MEMORANDUM OF TRANSMITTAL

To: Clyde Boutte, Venues Business Division Manager

From: George J. McGowan, CPA
Director, Office of Audit Services and Management Support

Dates: Exit Conference: May 1, 2019
Release: June 7, 2019

Subject: Orlando Venues PCI Compliance Review (Report No. 19-14)

At your request, the Office of Audit Services and Management Support, with major assistance from our co-source partner RSM, performed a review of Orlando Venues' service providers serving the Amway Center to evaluate adherence to the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS is a set of security standards designed to ensure that all companies which accept, process, store, or transmit credit card information maintain a secure data environment. It should be noted that this report is not a formal Report on Compliance (ROC) under the PCI guidelines, but a report for internal use by City of Orlando for remediation of identified security issues.

This review consisted of inquiries of City personnel and service providers (Ticketmaster, Orlando Magic, Levy/Orlando Foodservice Partners, OuiVend, and CenturyLink) and examinations of supporting documentation. It is less in scope than an audit made in accordance with internal auditing standards. The following was included within the scope of our assessment: an evaluation of each of the City's vendors' data controls and business application environment, infrastructure and performance; an assessment of data security and PCI DSS controls; an evaluation of the existing policies and procedures that govern the point of sale (POS) systems for each service provider; and a review of the security of cardholder data environment (CDE) for each provider. This report contains the results of the review procedures and recommendations for your consideration.

We appreciate the cooperation and courtesies extended by the management of the Venues Business Division and the associated service providers during the course of this review.

GJM

c: The Honorable Buddy Dyer, Mayor
Allen Johnson, Chief Venues Officer
Jody Litchford, Deputy City Attorney
Chris McCullion, Chief Administrative Officer
Rosa Akhtarkhavari, Chief Information Officer
David Billingsley, Chief Procurement Officer

CITY OF ORLANDO

PCI Compliance Review

June 2019

RSM

TABLE OF CONTENTS

RSM

EXECUTIVE SUMMARY

Background

The City of Orlando's Venues Department oversees activities at the Amway Center. The Amway Center is a major entertainment venue, home to the Orlando Magic basketball team and hosting other professional sports events and concerts. With a seating capacity of up to 18,000, the total attendance in 2017 was 1.32 million visitors for 231 events. Several service providers serve the Amway Center through ticket sales, food service, and merchandise:

- Ticketmaster – An internationally recognized brand, Ticketmaster sells tickets to events hosted at the Amway Center.
- Levy – A food concessions vendor serving the Amway Center during all major sports and entertainment events.
- Orlando Magic – A professional basketball team located in Orlando. The Amway Center is the team's home location.
- OuiVend – A preferred vendor selling merchandise during major sports and entertainment events at the Amway Center.
- CenturyLink – A third party providing IT infrastructure and network support

Each of these vendors accept, process, store or transmit credit card information. This presents a risk to the City of Orlando in the event of a breach due to the close association with these third parties.

Overall Summary / Highlights

The observations and associated risk ratings identified during our review are summarized on the next few pages. We have assigned a relative risk or value factors to each observation. Risk ratings are the severity of the concern and potential impact on the operations of each item. Starting on page 7, the detailed observations are listed including management action plans, estimated completion dates, and responsible parties.

Objective and Scope

The primary objective of this internal audit was to review the City of Orlando's service providers to evaluate adherence to the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS is a set of security standards designed to ensure that all companies which accept, process, store, or transmit credit card information maintain a secure environment. These standards were created by the major credit card brands and are accepted as standard practice within the industry.

The vendors included within the scope of this assessment were Ticketmaster, Levy, Orlando Magic, OuiVend and CenturyLink.

The scope of this review included:

- Evaluation of each of the City's vendors, critical and highest value data controls and business application environment, infrastructure and performance.
- Assessment of data security and PCI DSS controls considering the City's risk profile, business drivers, and strategic objectives.
- Evaluation of the existing policies and procedures that govern the point of sale (POS) systems for each service provider.
- Review of the security of cardholder data environment (CDE) for each provider through interviews, review of existing PCI documentation, and identifying if cardholder data is stored and/or transmitted.

Note - This report was not a formal Report on Compliance (ROC) under the PCI guidelines, but a report for internal use by City of Orlando for remediation of identified security issues.

Summary of Observations	Risk Rating
1. PCI Compliance Contract Requirements	Moderate
2. Vendor Management Program	Moderate

We would like to thank all City team members who assisted us throughout this review.

BACKGROUND

Business Services Department

The City of Orlando's Venues Department oversees the Amway Center, Camping World Stadium, Harry P. Leu Gardens, and the Mennello Museum. Within the Venues group, the Business Services Department oversees activities specifically at the Amway Center. Opened in 2010, the Amway Center is a major entertainment venue, home to the Orlando Magic basketball team and hosting other professional sports events and concerts. With a seating capacity in excess of 18,000, the total attendance in 2017 was 1.32 million visitors for 231 events.

Vendor Summaries

Several vendors serve the Amway Center, through infrastructure, ticket sales, merchandise, and food service. The focus of our review include the vendors which process, store, or transmit credit card information credit card information.

Ticketmaster LLC
Ticketmaster is a ticket retailer for concerts, games, and other events at the Amway Center. Ticketmaster sales take place online and in person at the Amway Center box office.

Levy / Orlando Foodservice Partners
Levy is food concessions provider at City Hall, Camping World Stadium, and the Amway Center for major entertainment events. Levy utilizes City Owned equipment and infrastructure for transactions at the Amway Center. Orlando Magic oversees the IT Network.

Orlando Magic
Orlando Magic is a team in the National Basketball Association, and home team at the Amway Center. As a major sports team, Orlando Magic is a major factor to the success of the Amway Center attendance and revenue. Attendance for the 2017/2018 season exceeded 725,000 visitors for home games.

OuiVend
OuiVend is the City's preferred merchandise retailer at the Amway Center, providing merchandise sales for non-Orlando Magic events at the Amway Center. OuiVend contracts directly with show promoters for sales agreements, and provides its own sales equipment and infrastructure for its sales.

CenturyLink
The City partners with CenturyLink to provide infrastructure services for service use at the City-owned Amway Center. CenturyLink is responsible for the segmentation of the network between the City of Orlando network and the vendors in the Amway Center, and for the firewalls and Access Control Lists (ACL) in place to segment the network properly.

BACKGROUND (CONTINUED)

Payment Card Industry (PCI) Overview

PCI DSS is a set of security standards designed to ensure that all companies which accept, process, store, or transmit credit card information maintain a secure environment. PCI standards are not law; however, the standards were created by the major credit card brands to protect against the rapidly increasing amount of credit card fraud and are accepted as standard practice within the industry. Lack of compliance can lead to fines, costly forensic audits, and brand damage. Although vendors for the City of Orlando are not storing credit card data, the PCI DSS standards still apply to these organizations. The City's vendors use third party payment processors, such as First Data, to process their credit card data. While this may reduce the vendors' risk exposure and reduce the effort to validate compliance, the PCI DSS standards are still applicable to these organizations. For purposes of compliance, organizations are either identified as merchants or service providers. Orlando Magic/Levy, OuiVend, and Ticketmaster are defined as merchants as each organization accepts credit card payments. CenturyLink would be classified as a service provider as they are providing the IT infrastructure on which the certain credit card transactions are processed, stored, or transmitted.

The PCI DSS merchant levels are rankings of merchant transactions per year broken down into four levels. The payment card industry uses merchant levels to determine risk from fraud and to ascertain the appropriate level of security for their businesses. Merchant levels determine the amount of assessment and security validation required for the merchant to pass PCI DSS assessment. The merchant level conditions are defined the credit card brands. The table below lists Visa and Mastercard's merchant levels for illustrative purposes:

PCI DSS Merchant Level Compliance

Level	Level Conditions	Validation Requirements	Vendor Compliance
1	Process more than $6,000,000 Visa or MasterCard transactions annually *Or* Systems have been attacked or compromised *Or* Visa, Mastercard, or any other card association designates the vendor as a Level 1 merchant	*Quarterly*: • Vulnerability Scans *Annually*: • Penetration Test • Completing an annual On-site PCI ROC • AOC Form (approved compliance with PCI DSS)	Ticketmaster – Complaint CenturyLink – Compliant
2	Process $1 million to $6 million Visa or MasterCard transactions annually	*Quarterly*: • Vulnerability Scans *Annually*: • Completing an annual SAQ • AOC Form (approved compliance with PCI DSS)	Orlando Magic/Levy – Compliant OuiVend – Compliant
3	Process $20,000 to $1 million Visa or MasterCard transactions annually	*Quarterly*: • Vulnerability Scans *Annually*: • Completing an annual SAQ • AOC Form (approved compliance with PCI DSS)	
4	Process less than $20,000 Visa or MasterCard transactions annually	*Quarterly*: • Vulnerability Scans *Annually*: • Completing an annual SAQ • AOC Form (approved compliance with PCI DSS)	

Vulnerability Scans and Penetration Tests

An ongoing requirement of the PCI compliance process involves having the vendor's payment card environment to be scanned for security vulnerabilities. These scans must be performed quarterly by an Approved Scanning Vendor. The PCI Security Standards council provides a list of these approved scanning vendors on their website. PCI security scans apply to all merchants that carry out internet-facing transactions. Annual Penetration tests are required as well as vulnerability scanning for only vendors that fall under the level 1 merchant compliance level.

Self-Assessment Questionnaire (SAQs) and Report on Compliance (ROC) for PCI

For Level 1 merchants, compliance with the PCI DSS requires submission of an Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA), also known as a Level 1 onsite assessment, or internal auditor if signed by officer of the company; a quarterly network scan by Approved Scanning Vendor is also required as is an Attestation of Compliance form.

Typical compliance requirements for Level 2, Level 3 and Level 4 merchants include submission of an Annual Self-Assessment Questionnaire (SAQ), a quarterly network scan by an ASV and an Attestation of Compliance form; however, Level 4 merchants may not be subject to all these requirements.

Attestation of Compliance (AOC) for PCI

An AOC is a certificate showing the organization has performed the appropriate Self-Assessment and attests to compliance with PCI DSS. Organizations use an AOC to show compliance with PCI to prevent disclosing of sensitive information contained in an SAQ, ROC, or vulnerability scans. An AOC is the only valid method for recognizing PCI DSS compliance validation. No other forms, certificates, or documents are acceptable to recognize PCI DSS compliance other than the AOC from the PCI Security Standards Council.

OBJECTIVES AND SCOPE, APPROACH AND REPORTING

Objectives and Scope

The primary objective of this internal audit was to review the City of Orlando's service providers to evaluate adherence to the Payment Card Industry (PCI) Data Security Standard (DSS).

The following vendors were included within the scope of our assessment:

- Ticketmaster
- Orlando Magic/Levy
- OuiVend
- CenturyLink

Approach

RSM assisted the City of Orlando with the following:

- Evaluation of each of the City's vendors, critical and highest value data controls and business application environment, infrastructure and performance as it relates to the PCI DSS control requirements.
- Assessment of data security and PCI DSS controls considering the City's risk profile, business drivers, and strategic objectives with regards to protecting customer data.
- Evaluation of the existing policies and procedures that govern the point of sale (POS) systems for each service provider.
- Review of the security of cardholder data environment (CDE) for each provider, by understanding their environment through:
    - Interview staff that supports the business and technical process of the service providers to review the PCI DSS requirements and identify potential gaps within the cardholder environment.
    - Review existing PCI documentation (i.e. Self-Assessment Questionnaires) to identify any concerns or gaps in responses or areas requiring additional documentation.
    - Identify if each service provider is processing, storing and/or transmitting credit card data.
    - Assess if each service provider have compliant POS systems, terminals and necessary software to protect customer data.

Reporting

At the conclusion of our analysis, we summarized the results of our procedures into a report and conducted an exit conference with the Business Services Division Manager and Office of Audit Services to discuss the details of our findings.

We have assigned relative risk ratings to each observation. This is the evaluation of the severity of the concern and the potential impact on operations. There are many areas of risk to consider including financial, operational, and/or compliance, as well as, public perception or ‘brand’ risk when determining the relative risk rating. Items are rated as High, Moderate, or Low.

- *High Risk Items* are considered to be of immediate concern and could cause significant issues when considering the above identified risk areas, if not addressed in a timely manner.
- *Moderate Risk Items* may also cause operational issues and do not require immediate attention, but should be addressed as soon as possible.
- *Low Risk Items* could escalate into operational issues, but can be addressed through the normal course of conducting business.

OBSERVATIONS

1	PCI Compliance Contract Requirements
Moderate **Observation**	Vendors do not have any language embedded in their respective contracts with the City to describe the security roles and responsibilities and for each vendor to provide ongoing proof that they are maintaining PCI compliance. This is a key requirement (12.8) within the PCI DSS guidelines. Without a PCI compliance requirement in place, the City may not be able to effectively monitor the vendor's PCI compliance. Understanding that certain PCI vendors use the City's IT infrastructure, the City limits its legal recourse in the event that a vendor or the Amway Center's IT infrastructure environment were to get compromised. The specifics around each vendor are listed below: OuiVend - OuiVend is a preferred vendor for the City; therefore, there is no contract in place between OuiVend and the City. Without a current contract in place, OuiVend does not have any contractual obligations with regards to PCI compliance. Orlando Magic/Levy - While there is a contract in place with the Orlando Magic, there is no PCI compliance requirement language within the contract. Ticketmaster - Being a level 1 merchant, Ticketmaster is required to have an annual ROC and is willing to furnish the City with their AOC. However, there are no terms in the contract with Ticketmaster that require PCI compliance. CenturyLink - The contract in place with CenturyLink states the requirements of network security for which CenturyLink is responsible, however there are no specifics within the contract around PCI compliance.
Recommendation	We recommend creating an addendum to the existing and/or a new vendor contracts of the requirement that the vendor must comply with PCI applicable requirements by the PCI Security Standards Council. The vendors should agree and accept responsibility to maintaining PCI compliance. See Appendix A for PCI Compliance Contract Agreement sample.
Management Response	Response: Orlando Venues (OV) will work with the Procurement Department to review and identify existing contracts that could possibly be amended to include PCI requirement language. In addition OV will review with Procurement the addition of recommended PCI language in new vendor contracts. Responsible Party: Clyde Boutte Estimated Completion Date: November 30, 2019

OBSERVATION MATRIX (CONTINUED)

2	**Vendor Management Program**
Moderate **Observation**	The City of Orlando does not have a comprehensive vendor management program in place that includes actively monitoring PCI compliance from their service providers. Without an effective vendor management program in place, the City risks overlooking the PCI compliance status of a vendor. Monitoring of vendors' PCI compliance status is an integral component in maintaining compliance that allows the entity to determine whether a change in status requires a change in the relationship. A vendor that is not compliant with PCI increases the significant risk of credit card data loss and the reputation of the City. The specifics around each vendor are listed below: OuiVend - OuiVend is currently PCI compliant. OuiVend currently carries out an SAQ and vulnerability scanning. Orlando Magic/Levy - With the Orlando Magic carrying out an SAQ and vulnerability scanning, they are complying with PCI requirements for their respective merchant level. With complete segmentation from the Orlando Magic Infrastructure, the City is not responsible for the infrastructure or any of the cardholder data environment used by the Orlando Magic. Please refer to Appendix C to see high-level segmentation of the Amway Center Ticketmaster – Being a Level 1 merchant, Ticketmaster is required to obtain a ROC annually. As noted in the AOC provided, we noted that Ticketmaster PCI compliant. Ticketmaster also carries out the required scanning and testing on their environment. CenturyLink - We noted that CenturyLink is a critical vendor in the PCI compliance, since this vendor manages the IT infrastructure on behalf of the City of Orlando for the Amway Center. CenturyLink is also responsible for ongoing segmentation of the cardholder data environment as detailed in Appendix C. CenturyLink is SOC 1 & 2 compliant as well as PCI compliant for managed firewalls and Network Intrusion Detection (NID) services that are carried out on behalf of the City.
Recommendation	We recommend creating a vendor management program that includes vendor PCI compliance. This program will hold the vendors accountable for complying with PCI requirements. Within this program, the city should request and review the AOC from Ticketmaster; the SAQ from OuiVend and Orlando Magic/Levy; and the SOC 1 & 2 from CenturyLink on an annual basis.
Management Response	Response: Orlando Venues (OV) will utilize Event Booking, a program currently utilized to track event schedules, insurance requirements, contracts and other information as a vendor management tracker for PCI compliance tracking. An account for each vendor will be setup and an individual will be assigned to receive automatic electronic reminders to follow-up on an annual basis to obtain and review the AOC from Ticketmaster; the SAQ from OuiVend and Orlando Magic/Levy; and the SOC 1 & 2 from CenturyLink. Responsible Party: Clyde Boutte Estimated Completion Date: August 1, 2019

APPENDIX A – PCI COMPLIANCE CONTRACT AGREEMENT SAMPLE

Below is a sample addendum for applicable vendor contracts:

> *Vendor agrees to comply in all material respects with applicable requirements of the Payment Card Industry (PCI) Data Security Standard (DSS), as amended or updated by the PCI Security Standards Council. Vendor agrees to and accepts the responsibility of maintaining the security of sensitive data and environments hosting sensitive data or operations; additionally maintaining the confidentiality of sensitive data accessed as necessary or incidentally accessed.*

APPENDIX B – PCI COMPLAINCE MONITORING

Developing a Third-party Service Provider Monitoring Program[1]

A Third-party Service Provider (TPSP) monitoring program should be fully documented. This ensures there is a common understanding of its elements across the organization, facilitates delegating portions of the process if required, and allows review of the process by outside parties when necessary. The elements of the program should include processes, policies, and procedures, and assignment of responsibility for those elements to specific people within the organization. The program documentation should be revisited on a regular basis in order to make corrections and improvements as the business processes and TPSP relationships evolve. It is recommended that program documentation be reviewed at least on an annual basis and is approved by management. Below is an example of a TPSP inventory to maintain consistency of this monitoring:

Third-Party Service Providers Inventory

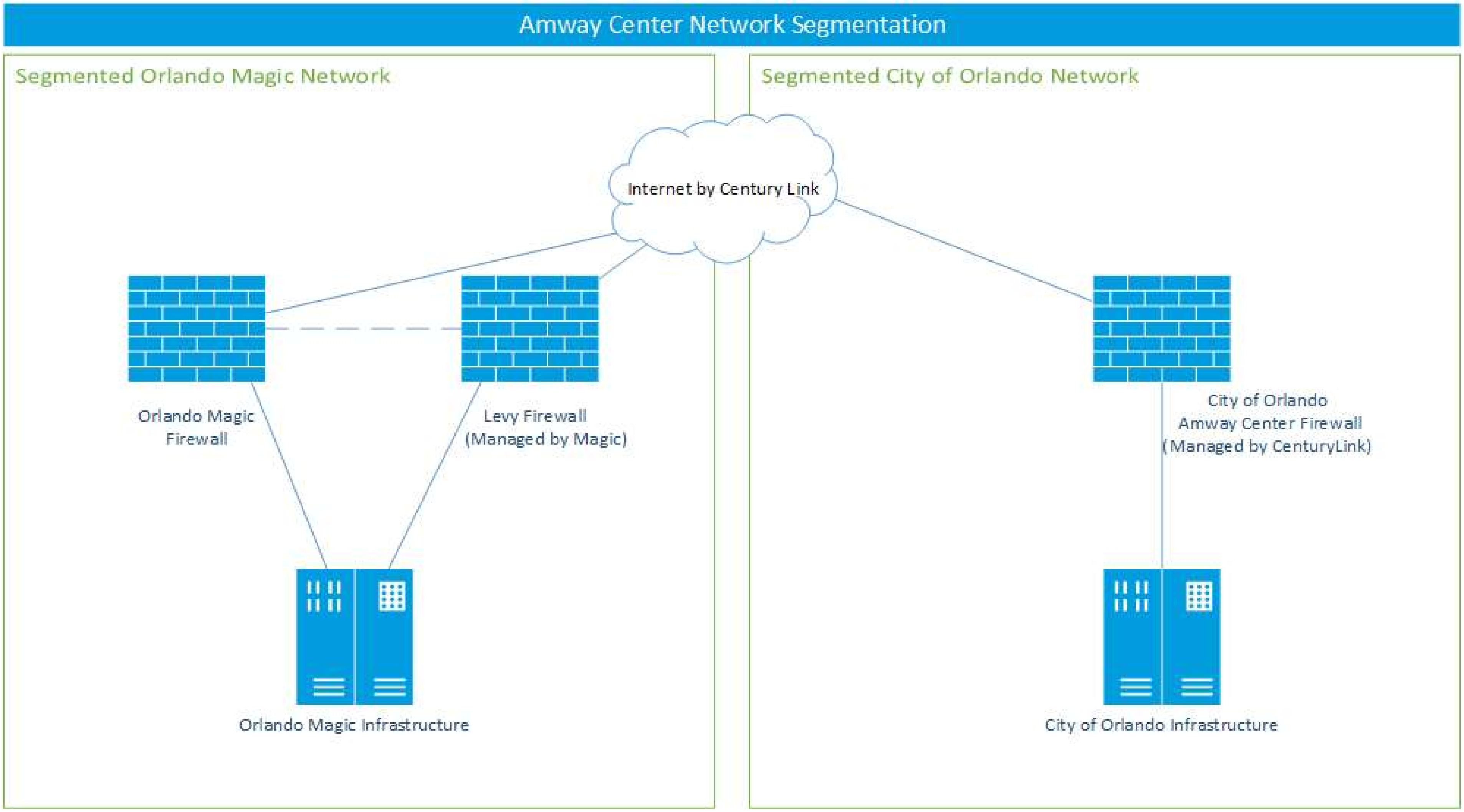
Define the procedures to maintain an inventory of all TPSPs, including the information elements deemed critical. The following are suggested elements that may be included in the inventory:

- Name and primary points of contact at the TPSP
- Specific service(s) being provided
- If cardholder data is shared, what elements are shared (sensitive authentication data, PAN, expiry, etc.)
- Location of the data—is the data stored internally in the organization, by the third party in one of its locations, or by an external hosting provider
- What system components are included in the review
- TPSP risk-assessment results
- Frequency of monitoring cycle
- Last date of review
- Contract renewal/expiry
- Documentation/evidence required
- Any nested TPSPs leveraged to provide the services
- Any third-party payment applications used to provide the services
- Volume of cardholder data that is stored/processed/transmitted/impacted by the TPSP
- Logical access to the entity’s network
- Any designations the TPSP holds that support its PCI DSS compliance attestation (ISO, PCI QIR, PCI PTS, FIPS 140, e

[1] PCI Security Standards Council, Information Supplement: Third-Party Security Assurance, https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf

APPENDIX C – AMWAY CENTER HIGH-LEVEL DIAGRAM

The City of Orlando relies on CenturyLink to manage the segmentation of the City of Orlando infrastructure. This segmentation prevents the Orlando Magic network from being able to communicate with the City of Orlando Network. This segmentation is done by firewalls that creates a virtual wall between the two networks. This keeps the Cardholder Data Environment (CDE) separate from the City of Orlando, leaving the Magic CDE responsibility to the Orlando Magic. The high-level diagram below shows how the two networks are segmented by firewalls owned by the respective entities:


Amway Center Network Segmentation
Segmented Orlando Magic Network
Segmented City of Orlando Network
Internet by Century Link
Orlando Magic Firewall
Levy Firewall (Managed by Magic)
City of Orlando Amway Center Firewall (Managed by CenturyLink)
Orlando Magic Infrastructure
City of Orlando Infrastructure

RSM US LLP
800 North Magnolia Avenue, Suite 1700
Orlando, Florida 32803
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.