Internal Audit Consulting Report

Payment Card Industry Security Standards Council Administration

October 31, 2021

City of Springfield, Missouri

BKD CPAs & Advisors

Table of Contents

City of Springfield, Missouri

Internal Audit Consulting Report of Payment Card Industry Security Standards Council Administration
October 31, 2021

BKD
CPAs & Advisors

910 E. St. Louis Street, Suite 200 | P.O. Box 1190 | Springfield, MO 65801-1190
417.865.8701 | Fax 417.865.0682 | bkd.com

Report Letter

Mr. David Holtmann, Director of Finance
City of Springfield
218 E. Central
Springfield, MO 65802

We have performed the procedures enumerated in the Section IV of this report, which were agreed to by you pursuant to our scope of work dated July 19, 2021, to perform an assessment of the City's Payment Card Industry Data Security Standard (PCI DSS) administration. This engagement was not an attestation of compliance (AoC) and was not designed to provide assurance as to the City's compliance with PCI DSS. While our services and reports may contain observations and recommendations related to PCI DSS requirements, management is responsible for continuously monitoring these requirements for changes and their impact on the information in this report. Management is also responsible for their operations and ensuring that all relevant IT and cybersecurity risk factors are adequately addressed. Had we performed additional procedures, other items of significance may have been reported to you. The sufficiency of the procedures is solely the responsibility of the parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described in Section IV of this report for the purpose for which this report has been requested or for any other purpose. In addition, our services cannot be relied upon to prevent, deter, or detect potential security breaches.

The observations and recommendations, in connection with the procedures performed, are located in Section III.

We were not engaged to, and did not, conduct an examination, the objective of which would be the expression of an opinion on the internal control systems management has in place. Accordingly, we do not express such an opinion. Our report is intended for use only by management solely for reporting results with respect to the procedures performed by us. This report is not intended to be, and should not be, used by anyone other than these specified parties.

BKD, LLP

BKD, LLP

October 31, 2021

II. Executive Summary

We are pleased to provide our report on *Payment Card Industry Security Standards Council (PCI DSS) Administration* performed by **BKD, LLP** (BKD) for City of Springfield (the City) commencing August 16, 2021 and ending October 31, 2021. The overall objective of this engagement is to assist the City with assessing PCI DSS Administration.

The procedures we developed, management approved, and we performed are included in Section IV. The results of our procedures were discussed with management at the conclusion of our engagement and are included in Section III.

PCI considers the City to be a Merchant. For the purposes of PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI Security Standards Council (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and/or services. The City completes Self-Assessment Questionnaires (SAQ) A, B, and B-IP per the instruction of the acquirer. The City has multiple departments that use a combination of e-commerce, telephone order, and card present payment channels.

Observations

An observation is an opportunity to enhance compliance with PCI requirements and may be considered a best practice. An observation may also be an item that we noted should be brought to management's attention that does not specifically relate to a SAQ question. The following observations were noted during our engagement.

The leadership of the City should evaluate the observations and recommendations and make cost/benefit decisions on whether improvements to processes would be beneficial. Management's responses were not subjected to the procedures we applied and, accordingly, we express no opinion on the responses.

III. Observations & Recommendations

Observation #1: Attestation of Compliance Questionnaire – Transaction Types

We noted payment associates sometimes perform Mail Order and Telephone Order (MOTO) transactions via direct keying of credit card information into POI devices as permitted by departmental procedure. However, the Attestation of Compliance (AoC) for the Self-Assessment Questionnaire (SAQ) B-IP do not list MOTO as being a used transaction type.

Recommendation:

To appropriately reflect transaction types performed by the City, we recommend management include in the attestation of compliance form that MOTO transactions are selected in any AOCs where such transactions are permitted.

Management Response:

This was an oversight when completing the most recent B-IP questionnaires. Going forward, City staff will ensure mail order and telephone order transactions are properly indicated in the attestation of compliance for the applicable locations.

Observation #2: Self-Assessment Questionnaire (SAQ) – Appendix A2

Appendix A2 was not completed on the SAQ completed by management for the B-IP. This appendix is required to be considered on SAQ B-IP and the City's compliance should be denoted and explained.

Recommendation:

We recommend management fill out and complete Appendix A2 to show compliance on the SAQ of record for the City.

Management Response:

Appendix 2 will be completed as required.

Observation #3: Expired PIN Transaction Security (PTS) Devices

We noted the City is using over 30 point of interaction (POI) devices that are listed on the PCI expired approvals PIN Transaction Security (PTS) device listing. Using expired devices could render the City ineligible to complete the SAQ B-IP which requires the use of devices with current PTS Approvals to be eligible, and the City may instead have to complete SAQ C or SAQ D which have additional PCI compliance requirements that the City would have to assess.

Recommendation:

We recommend management replace expired PTS POI devices with current ones to remain eligible to use SAQ B-IP.

Management Response:

The City used the SAQs assigned by our merchant bank. As the entity overseeing our compliance with PCI standards, we defer to the guidance provided by the merchant bank. The bank indicated the devices we were using were compliant and the B-IP questionnaires completed were appropriate.

As our credit card devices are replaced, we will purchase updated devices provided by our merchant bank.

Observation #4: Firewall and Router Policy and Standards

During our testing of policy and procedure around firewall and routers, we noted there is minimal written policy or standards in place for management of the firewall. Firewall policy and standards is an important part of setting clear expectations for network security as regards Requirement 1 of PCI DSS.

Recommendation:

We recommend management implement written firewall policy and standards that meet requirements set out by Requirement 1 for the relevant SAQs.

Management Response:

Information Systems agrees with the observation and will enhance the firewall policy with more clarity. We expect to have the enhanced policy in place by March 1, 2022.

Observation #5: Parks Department POI Device Setup

Due to a lack of network jacks at some facilities, Parks department POI devices are connected to workstations to give them access to complete transactions. This configuration renders the City ineligible to complete SAQ B-IP for these devices under the SAQ's eligibility requirements as the workstation security becomes scoped into the cardholder data environment. Per discussion with management, IT has a project underway to add additional network jacks to allow for the City's standard POI network configuration in the future.

Recommendation:

We affirm management's project to remediate device segmentation issues and recommend that they continue to work towards adequate segmentation of POI devices from other elements on the network in a timely manner.

Management Response:

Information Systems is having difficulty sourcing new network switches. As soon as they are available, we will procure these and get them installed to add additional network ports for Parks. Parks has agreed to purchase these when they become available.

The Parks Department, in conjunction with Information Systems, will continue to install needed data ports, switches, and cabling to accept new credit card readers. We will continue attaining all necessary infrastructure devices to make a quicker installment of new credit card readers when received. Parks is striving to acquire the new credit card readers; however, due to worldwide chip shortages and supply-chain issues, we are not able to secure the credit card readers. Our vendor has informed us that no timeline is available for receiving the credit card readers. We will continue to communicate with Active.net and stress to the company's representatives the urgency of this matter. We are in receipt of three compliant credit card readers, and they are scheduled for installment as soon as possible. We have also requested the remaining credit card readers needed for installation and will schedule those for installment as soon as possible upon receipt.

Observation #6: Internal Penetration Testing Scoping – Segmentation Testing

While the City has received an internal penetration test in the last year, the scope of the testing did not expressly test adequate segmentation of the City's cardholder data environment from the rest of the network. SAQ B-IP requires that penetration tests be scoped specifically to determine whether they can exploit network vulnerabilities to bypass segmentation controls protecting POI devices, which is not a part of a standard internal penetration test scope.

Recommendation:

We recommend the City coordinate an annual internal penetration test that specifically verifies adequate segmentation of POI devices from the rest of the network as required by Requirement 11 of PCI-DSS.

Management Response:

Information Systems is scheduled for the 2022 network penetration test in Spring 2022, and this requirement will be added to the scope of the penetration test.

Observation #7: PCI DSS Compliance Control Tracking

To track PCI compliance, management has department heads complete a subsidiary version of the printed SAQs and submits them to management where they are consolidated into single SAQs of record and used to complete the AOC for submission. However, many of the questions that department heads are answering they do not have the responsibilities or knowledge to attest to. In the absence of a QSA performing an AOC, it may be difficult to track compliance across multiple departments to ensure adequate compliance. This results in a risk that any areas that are truly not compliant that they are responsible for would not be caught. Payment departments are decentralized and fall under multiple individuals.

Recommendation:

We recommend management create a PCI compliance methodology that breaks down PCI requirements, controls, and control owners to ensure all necessary parties have sufficient understanding of the defined controls for which they are responsible.

Management Response:

We agree with the recommendation and will utilize the PCI compliance tracking spreadsheet provided by BKD to improve the process.

IV. Scope of Services

The objective of our procedures was to assist City of Springfield with an assessment of Payment Card Industry Security Standards Council (PCI DSS) administration.

The dates utilized for our testing were November 2020 through October 2021, unless otherwise noted.

Payment Card Industry Security Standards Council Administration

Mr. David Holtmann, Director of Finance
City of Springfield
218 E. Central
Springfield, MO 65802

Re: Scope of Payment Card Industry, Security Standards Council Assessment and Administration

The purpose of this document is to provide a detailed scope for Payment Card Industry, Security Standards Council (PCI DSS) administration. The scope of procedures, as outlined below, shall be limited to the most recent PCI SAQs completed by the City of Springfield and controls as they exist at the time of our walkthroughs, unless otherwise noted.

Our procedures will include, but may not necessarily be limited to the following:

1. Conduct interviews with personnel involved in the PCI DSS administration process
2. Evaluate current PCI Self-Assessment Questionnaires (SAQ)
3. Assessing the payment channels and aligning with the proper SAQ as determined by PCI DSS
4. Evaluate methods and timing of training staff for those responsible for credit card transactions
5. Assessing implementation of logical security requirements
6. Assessing inventory requirements
7. Assessing physical security requirements and controls
8. Assessing logging and monitoring processes
9. Assessing application and point of sale systems involved in card transactions
10. Assessing vulnerability scanning and remediation requirements by an Authorized Scanning Vendor (ASV)
11. Assessing vendor management policies and controls related to third-party vendors used for card processing
12. Obtain and analyze any written policies or procedures that govern PCI DSS requirements
13. Document gaps or opportunities for improvement noted during testing
14. Provide management with a written report, which will include, but may not necessarily be limited to:
    a. Results of our procedures
    b. Observations and recommendations resulting from our work
    c. Management responses