MAYOR JIM GRAY

LEXINGTON

BRUCE SAHLI
DIRECTOR
OFFICE OF INTERNAL AUDIT

MANAGEMENT ACTION PLAN PROGRESS REPORT

DATE: January 24, 2018

TO: Jim Gray, Mayor

CC: Sally Hamilton, Chief Administrative Officer
Glenn Brown, Deputy Chief Administrative Officer
Aldona Valicenti, Chief Information Officer
Geoffrey Reed, Commissioner of General Services
William O'Mara, Commissioner of Finance & Administration
Rusty Cook, Director of Revenue
Monica Conrad, Director of Parks & Recreation
Phyllis Cooper, Director of Accounting
Susan Straub, Communications Director
Urban County Council
Internal Audit Board

FROM: Bruce Sahli, CIA, CFE, Director of Internal Audit
Chris Ensslin, CIA, CFE, CGAP, Deputy Director of Internal Audit

RE: Payment Card Industry Data Security Standard US Bank MAPPR

Background

On September 22, 2017 the Office of Internal Audit issued the Payment Card Industry Data Security Standard (PCI-DSS) US Bank Review. The 2017 audit review contained four findings which are in the chart below.

This review is provided for management information only. It is not an audit and no opinion is given regarding controls or procedures. At the conclusion of this review, the Deputy Director of Internal Audit completed an SAQ A & B with Attestation of Compliance for all the LFUCG merchants which are processed through US Bank. SAQ A with attestation of compliance was completed on January 19, 2018 and SAQ – B with attestation of compliance was completed on October 31, 2017. The next Attestation of Compliance will be due by October 31, 2018. The Deputy Director of Internal Audit also spoke with US Bank/Elavon personnel, who agreed to give LFUCG a credit of $810 for the two months LFUCG has been in PCI-DSS compliance. This will save LFUCG $4,860 in PCI-DSS non-compliance fees for the next year, and for each year going forward that LFUCG remains in compliance.

A summary of the findings from the original audit report and a summary of the results of our follow-up are provided in the table below. The original findings, management's original responses, and details of the results of this follow-up are contained in the **ORIGINAL AUDIT RESULTS AND FOLLOW-UP DETAILS** section of this report.

Finding	Summary of Original Finding	Follow-Up Results
Finding #1 High Priority	**Maintain a List of Payment Devices**	**The Division of Revenue and the Division of Parks and Recreation are maintaining lists of payment devices and inspection reports. This finding has been resolved.**
Finding #2 High Priority	**Lack of an Incident Response Plan**	**The Division of Revenue and the Division of Parks and Recreation are maintaining Incident Response Plans. This finding has been resolved.**
Finding #3 High Priority	**Lack of Annual Security Training for Employees**	**The Division of Revenue and the Division of Parks and Recreation have conducted annual security training for employees. This finding has been resolved.**

Finding #4 High Priority	**SAQ – B & D Need to be Completed**	**An SAQ A & B with attestations of compliance has been completed by the Deputy Director of Internal Audit. This finding has been resolved.**

ORIGINAL AUDIT RESULTS AND FOLLOW-UP DETAILS

Original Finding #1: Maintain a List of Payment Devices
Priority Rating: High

Condition:
There is no up-to-date list of payment devices, nor is an inspection log maintained with inspection dates and inspector's initials.

Effect:
The addition of a card skimmer to the payment devices, or an act of substitution (e.g. swapping a payment device) could go undetected if inspections are not performed.

Recommendation:
Maintain an up-to-date list of payment devices. The list should include the following: make & model of device, location of device, personnel with access, and the device serial number or other method of unique identification.

In addition, a separate inspection log should be kept with inspection dates which are initialed by the inspector. The inspection should include looking for signs that a device might have been tampered with or substituted. Evidence of substitution includes unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings or device characteristics.

Director of Revenue Response:
Revenue concurs that an up to date list of payment devices should be maintained as well as inspection logs. Revenue believes the list should be maintained in Finance as Finance is responsible for banking and credit card payment devices. Inspections for Revenue's devices should be handled by the Processing Supervisor in Revenue periodically as well as

by staff daily as their shift starts. The Division would provide any assistance to Finance with developing this process.

Commissioner of Finance & Administration Response:
We appreciate Internal Audit's review and education of best practices in this area which Finance was not knowledgeable of. A list has been completed for the Division of Revenue's payment devices and will be verified monthly by the Revenue Supervisor. An inspection log has also been created and will be completed monthly, with completed logs being sent to the Department of Finance quarterly from all Divisions having payment devices for retention. Copies of the logs have been completed for Revenue, which would also go into effect for any future Divisions who gain payment devices.

Director of Parks & Recreation Response:
Parks and Recreation will maintain an up-to-date list of payment devices effective August 2017. The list includes the following: make & model of device, location of device, personnel with access, and the device serial number.

Parks and Recreation will also inspect these payment devices on a monthly basis and keep a separate inspection log with inspection dates which is initialed by the inspector effective August 2017. The inspection will include looking for signs that a device might have been tampered with or substituted.

Commissioner of General Services Response:
I concur with the Director's response.

Follow-Up Detail Results:
A Finance & Investment Analyst in the Department of Finance and Administration provided inspection logs that are maintained by the Director of Revenue and Revenue Supervisor. Inspection reports for the Division of Parks and Recreation were provided by an Information Systems Specialist. The Division of Revenue and the Division of Parks and Recreation are both maintaining a list of payment devices.

This finding has been resolved. No management response required.

Original Finding #2: Lack of an Incident Response Plan
Priority Rating: High

Condition:
There is no incident response plan related to US Bank credit card processing.

Effect:
An incident response plan is necessary to be PCI compliant.

Recommendation:
Develop a formal plan on how to respond to an incident, including notification of appropriate law enforcement agencies, merchant bank, and various payment card associations. Once the plan is developed, contact the merchant bank customer service department to determine all their incident response requirements are addressed in the plan.

Director of Revenue Response:
Revenue concurs with the recommendation of a formal incident response plan. This plan should be maintained centrally in Finance so that if an issue happens, the areas affected would know who to contact immediately and begin the response plan. Finance works directly with US Bank on credit card processing and would be the first contact concerning any credit card issue. Revenue would want to be a part of any project to develop an incident response plan.

Commissioner of Finance & Administration Response:
We appreciate Internal Audit's review and education of best practices in this area. An Incident Response Plan has been created and is effective immediately; however, Finance will also work to have this and the PCI Compliance Policy become CAO Policy.

Director of Parks & Recreation Response:
Parks and Recreation has drafted an incident response plan outlining Parks and Recreation's initial responses to cardholder data breaches. Parks' plan will take deference to the LFUCG data breach incident response plan currently being drafted.

Commissioner of General Services Response:
I concur with the Director's response.

Follow-Up Detail Results:
A Finance & Investment Analyst provided the Incident Response Plan for the Department of Finance & Administration. The Incident Response Plan for the Division of Parks & Recreation was provided by an Information Systems Specialist. Both plans contain comprehensive steps to be taken if an incident occurs. If the CIO develops a government-wide Incident Response Plan, it will replace these two Plans.

This finding has been resolved. No management response required.

Original Finding #3: Lack of Annual Security Training for Employees
Priority Rating: High

Condition:
An annual security training program does not exist for LFUCG employees involved in processing credit card payments.

Effect:
An annual security training program is required in order to be PCI DSS compliant.

Recommendation:
A formal training program for all relevant employees that teaches them about security as it relates to credit cards, paper with credit card numbers on them, to never send credit card information by end-user messaging technologies (e.g. e-mail, instant messaging, SMS/text, chat, etc.) should be developed.

The training should also cover attempted tampering or replacement of devices. Training on this subject should include the following:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (e.g. attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g. supervisor, manager, or director).

Director of Revenue Response:
Revenue agrees that a formal training program should be developed by LFUCG and that the Division would assist in any training program being developed.

Commissioner of Finance & Administration Response:
We appreciate Internal Audit's review and education of best practices in this area. Finance will provide training by calendar year end 2017 for all relevant users and training will be completed on an annual basis from that point going forward. Training will come from the Incident Response Plan and the PCI Compliance Policy.

Director of Parks & Recreation Response:
Parks is in agreement and will implement a training program focusing on cardholder data and terminal security effective Sept 2017.

Commissioner of General Services Response:
I concur with the Director's response.

Follow-Up Detail Results:
A Finance & Investment Analyst provided the Training Policy for the Department of Finance & Administration. A copy of the training log demonstrating that annual training has occurred in the Division of Revenue was also provided. The Training Policy for the Division of Parks & Recreation and a log demonstrating that annual training has occurred there was provided by an Information Systems Specialist.

This finding has been resolved. No management response required.

Original Finding #4: SAQ – B & D Need to be Completed
Priority Rating: High

Condition:
SAQ – B & D need to be completed. Eight merchant ID's are under SAQ B and one merchant ID is under SAQ – D.

Effect:
Completing the proper SAQ's and relevant Attestation of Compliance is required to be PCI DSS compliant.

Recommendation:
Once all the questions in the SAQ – B and D can be answered yes or N/A, complete the relevant attestation of compliance for each. One may be compliant and completed before the other one.

Director of Revenue Response:
Revenue agrees that the SAQ – B&D needs to be completed. The Division attempted to get this completed previously; however, due to changeover in employee staffing in the area we needed assistance in it was put aside. The Division would provide any assistance to ensure proper completion of the document.

Commissioner of Finance & Administration Response:
We appreciate Internal Audit's review and education of best practices in this area. When Findings 1-3 are mitigated, Internal Audit will be notified and SAQ B will be completed.

Director of Parks & Recreation Response:
Parks and Recreation is researching more secure methods of taking credit card transactions, including EMV-certified devices.

Commissioner of General Services Response:
I concur with the Director's response.

Follow-Up Detail Results:
The Deputy Director of Internal Audit completed SAQ-A with attestation of compliance and SAQ-B with attestation of compliance on January 19, 2018 and October 31, 2017, respectively. Observation proof of a redirect from the Parks & Recreation website to Plug N Pay allowed LFUCG to fill out an SAQ-A as recommended by SYSNET. SYSNET is the new third party vendor in charge of PCI-DSS compliance for Elavon. This redirect is where all of the credit card information is entered. LFUCG does not store any of the credit card data.

This finding has been resolved. No management response required.