MAYOR LINDA GORTON

LEXINGTON

BRUCE SAHLI
DIRECTOR
OFFICE OF INTERNAL AUDIT

INTERNAL AUDIT ATTESTATION

DATE: March 27, 2020

TO: Linda Gorton, Mayor

CC: Sally Hamilton, Chief Administrative Officer
Glenn Brown, Deputy Chief Administrative Officer
Aldona Valicenti, Chief Information Officer
William O'Mara, Commissioner of Finance & Administration
Monica Conrad, Acting Commissioner of General Services
Phyllis Cooper, Director of Accounting
Jeff Lewis, Acting Director of Revenue
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 Review

Background

According to the Payment Card Industry Security Standards Council, the Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. This applies to essentially any merchant that has a Merchant ID (MID).

The Payment Card Industry Security Standards Council (PCI SSC) was formed on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI)

security standards, with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB).

It is important to note that the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

PCI applies to any organization or merchant, regardless of size or number of transactions, that accepts, transmits, or stores any cardholder data. In addition, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

PCI is not, in and of itself, a law. The standard was created by the major card brands Visa, MasterCard, Discover, AMEX and JCB. At their acquirers'/service providers' discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, and brand damage, etc., should a breach occur.

The payment card brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine along to the merchant who committed the violation. Furthermore, the bank will also most likely either terminate its relationship with the violating merchant or increase transaction fees. Penalties are not openly discussed nor widely publicized, but the fine amounts listed above can be catastrophic to a small business.

According to the Payment Card Industry Security Standards Council, over 38 states have data breach notifications laws in place for accepted parties.

LFUCG Parks & Recreation Enterprise Program and the Division of Revenue are merchants who accept the payment card brands listed above. In calendar year 2019, those two Divisions processed credit card transactions through US Bank using point of sale equipment which transmits encrypted credit card data. In order to be Payment Card Industry Data Security Standard (PCI DSS) compliant, LFUCG must complete Self-Assessment Questionnaires (SAQ-A, B, & D) and Attestation of Compliance.

Scope and Objectives

The objectives for the engagement were to:

- Perform all necessary SAQ's for US Bank
- Perform Attestation of Compliance PCI DSS for US Bank

The scope of the SAQ – A, B, & D covers Parks & Recreation Enterprise Program and Revenue credit card transactions that are processed through US Bank.

Statement of Auditing Standards

We conducted our review in accordance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the review to afford a reasonable basis for our judgments and conclusions. We believe that our review provides a reasonable basis for our conclusions.

Review Opinion

In our opinion, the LFUCG was compliant with PCI DSS for US Bank during calendar 2019.