# Office of
# Multnomah County Auditor

Steve March
County Auditor

501 SE Hawthorne Room 601
Portland, Oregon 97214
Phone: 503-988-3320

Fran Davison
Nicole Dewees
Craig Hunt
Jennifer McGuirk
Annamarie McNiel
Marc Rose
Mark Ulanowicz
Caroline Zavitkovski

Date: August 6, 2018

To: Chair Kafoury; Commissioners Meieran, Smith, Vega Pederson, and Stegmann; COO Madrigal; CFO Campbell

From: Steve March, County Auditor

Re: Letter to Management – PCI Security Compliance

Every organization is governed by rules and regulations. When Multnomah County receives federal money, it complies with federal guidelines. When the County receives money from individuals or businesses, it follows other rules, including some that most businesses must follow. Like most businesses, the County must follow the Payment Card Industry's (PCI) Data Security Standards (Standards) when we accept credit and debit cards for payment.

The Standards are a set of requirements designed to help ensure that all organizations that accept credit or debit cards maintain a secure environment to protect cardholder information. For example, organizations that accept payment cards are prohibited from storing debit card personal identification numbers (PIN). Multnomah County accepts payment cards in several operations, ranging from property tax payments to the sale of pet supplies.

We first examined the County's compliance with the PCI Standards in our 2009 audit: County's Receivables and Cash Handling. During the 2009 audit, we initially found that the County was out of compliance with the Standards, but achieved compliance by the time the audit was issued. The objective of this latest audit was to determine if Multnomah County was still in compliance with the PCI standards and if the organization had a structure in place to facilitate continued compliance with the Standards.

## What We Found

We found the County's payment card processes were in compliance with the PCI Standards. Moreover, we believe that the County's Treasury unit has developed a process to help the County remain in compliance as operations and the associated risks evolve.

The Treasury unit of the Department of County Management coordinates the County's PCI compliance process. In developing a sustainable process, Treasury implemented a strategy of simplifying the County's in-person payment operations and outsourcing the risks associated with e-commerce (online) and automated telephone transactions.

Simplifying in-person payment operations, like payments for marriage licenses, meant changing from PC-based card-swipe devices connected to the County's network to stand alone PCI compliant card reading devices and terminals that use either mobile phone technology or analog phone lines to directly connect to the bank. Outsourcing e-commerce risk meant taking potential customers out of the County's network via a hyperlink to a PCI compliant third-party payment processor for online payments and via a third-party telephone payment vendor for most transactions occurring over the phone.

The County does not store any sensitive payment card data or allow these data to pass through the network. This means Treasury was able to satisfy PCI requirements by conducting relatively simple self-assessments, reviewed by a PCI approved assessment consultant. While the County's systems meet the technical requirements for safeguarding cardholder data, it does not appear that changes in County procedures have kept pace with the changes in technology, as some procedures need to be updated. For example, procedures should reflect the risk of accepting card payments using County telephone lines that operate over the County's computer network.

## What We Recommend

To better facilitate keeping the County in compliance with PCI requirements, the Department of County Management should update County cash handling and payment card technology procedures to more closely align with current practices. And, Treasury should continue to review its PCI compliance at least annually, or as technology and business needs change.

## Scope and Methodology

We reviewed PCI Data Security Standards and the work done by Treasury to follow the steps to compliance outlined by the Payment Card Industry Security Standards Council. We reviewed the fiscal year 2016 needs assessment and PCI Self-Assessment Questionnaire overseen by the County's PCI Qualified Assessor. We visited seven County work units to confirm that the PCI compliant solutions were in fact in place and that these business units were not accessing sensitive card data in their routine reconciliations of payments.

Mark Ulanowicz performed the audit work for this letter. 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 findings and conclusions based on our audit objectives.

Department of County Management
Finance & Risk Management Division

Multnomah County

## MEMORANDUM

Date: August 6, 2018

To: Steve March, Auditor

From: Mark Campbell, Chief Financial Officer

Re: PCI Compliance Report

Thanks to you and your staff for undertaking a review of the County's Payment Card Industry – Data Security Standards (PCI DSS) procedures and practices. On behalf of the Treasury team, I appreciate that your review highlighted and acknowledged the excellent job we are doing to ensure the security of cardholder information.

Compliance with PCI DSS has been a top priority for my Division since you conducted your initial audit. Treasury manages the compliance process for the County through collaboration with departments who accept credit card payments, IT security, Bank of America Merchant Services (the County's primary credit card processor) and other business partners that process credit card payments. We have established a centralized process whereby Treasury collects, maintains, and manages the information necessary to perform compliance functions. I feel this process has worked well and serves as an important control in the sense that there is one point of contact for all PCI DSS related activities.

We agree with your recommendation that our cash handling and credit card procedures be updated. In fact, the procedures are currently being updated and we will share them with your office when completed. Generally speaking, however, Treasury updates the County's Cash Handling manual as needed (i.e., when new payment methods are made available) and also conducts periodic training with departments as requested. I see compliance with PCI DSS as a continuous improvement process and the Treasury team, along with IT Security, is regularly on the lookout for solutions that will enhance the security of our credit card processing environment.