Washington County
Auditor's Office

Follow-Up Report

Assessing Compliance with the Payment Card Industry Data Security Standard

Final Report
March 9, 2020

Audit Team: County Auditor: John Hutzler, CIA, CGAP, CCSA
Reviewer: Sherry Kurk, CISA

I. Background and Summary

Washington County collects a variety of payments from residents and visitors. Payment cards from major issuers American Express, Visa, MasterCard and Discover are used for an increasing number of payments to the County. These transactions range from parking at a county park to probation supervision fees and property taxes.

Payment card data breaches and fraud are on the rise, costing organizations millions of dollars. The Payment Card Industry Data Security Standard (PCI-DSS) is an international standard that applies to merchants, like the County, that accept payment cards. The standard is important to help protect both merchants and customers from data breaches and from fraud.

Failure to follow the international payment card standard increases an organization's risk for fraud and data breaches, potentially exposing customers' payment card data and violating the public's trust. The county's contract with a major bank for card processing requires that the County follow this standard.

Because the County processes less than six million payment card transactions per year, it is not required to hire an independent assessor to certify its compliance. The county's Finance Division (Finance) has conducted self-assessments of compliance with this international standard annually since 2013.

In April 2019, the Washington County Auditor released the report titled "Assessing Compliance with the Payment Card Industry Data Security Standard" together with the response of the County Administrator. We found that, although Finance has consistently reported that the County is fully compliant, the process for assessing PCI-DSS compliance was a pro-forma exercise that provided little assurance that the County was, in fact, compliant with the standard. The Auditor made seven recommendations for action. The County Administrator agreed with the Auditor's recommendations and planned to implement most of them by October 1, 2019.

We scheduled this follow-up review to determine the extent to which the County had implemented the audit recommendations. Our review covers implementation action through January 2020.

We found that implementation of all seven of the audit recommendations remained In Process four months beyond originally targeted dates for completion. Failure to implement applicable PCI-DSS requirements and complete all required testing could jeopardize the County's ability to continue to accept card payments. Losing the ability to accept card payments could disrupt incoming revenue to the County and inconvenience county residents wishing to make card payments.

This report summarizes findings and recommendations from the original audit and describes the results of our follow-up review. The acting County Administrator chose not to file a written response.

II. Overview of the Original Audit

Audit Objective

The Auditor's Office initiated the audit to address the following question:

> Does the Finance Division's self-assessment process for compliance with the Payment Card Industry Data Security Standard (PCI-DSS) provide reasonable assurance of compliance with the standard?

Audit Recommendations

The original audit determined that the process for assessing PCI-DSS compliance was a pro-forma exercise that provided little assurance that the County was, in fact, compliant with the standard. To improve the effectiveness of the county's self-assessment process, the auditor made the following recommendations:

1. The County should use official PCI-DSS SAQ forms and perform all expected testing before attesting to the county's compliance.

2. The CAO should transfer responsibility for PCI-DSS Self-Assessment from Finance to Information Technology Services (ITS).

3. The County should sponsor a qualified ITS employee to complete the Internal Security Assessor (ISA) training and conduct the county's PCI-DSS self-assessment(s).

4. An executive officer of the County, such as the County Administrator, Assistant County Administrator, Chief Information Officer (CIO) or Chief Financial Officer (CFO) should sign the Assessment of Compliance.

5. The CAO should either revise the Protection of Personal Information Policy to encompass PCI-DSS or develop a separate policy addressing payment card security.

6. County policy should require that county operations authorized to accept payment card payments have written procedures for processing card payments and ensuring the security of payment card information.

7. The county's Internal Security Assessor should complete a single PCI-DSS SAQ-D to assess the compliance of all county payment card operations, including those utilizing the third-party online payment processor.

III. Follow-Up Findings

We found that all seven recommendations remained In Process.

1. The County should use official PCI-DSS SAQ forms and perform all expected testing before attesting to the county's compliance.
   Current Status – In Process. Revised implementation date: June 2020.
   Although the CAO responded that, "The County agrees and will develop a written plan detailing the process and procedures for testing and attesting to compliance … by October 1, 2019, we found that such a plan had not yet been developed. The County did not use official PCI-DSS-SAQ forms or perform expected testing in its 2019 PCI-DSS self-assessment process.
   ITS reports that it intends to use official forms and perform all expected testing as part of the 2020 self-assessment. The acting CIO has indicated that assessment will identify any PCI compliance gaps and subsequent remediation plans.

2. The CAO should transfer responsibility for PCI-DSS Self-Assessment from Finance to Information Technology Services (ITS).
   Current Status – In Process. Revised implementation date: June 2020.
   On April 1, 2019 before the audit report was issued, the former Director of Support Services directed that responsibility for PCI-DSS testing and attestation be transferred from Finance to ITS. Although the CIO and the CFO acknowledged the transfer of responsibility, ITS did not perform the testing or attest to PCI-DSS compliance for FY 2019. The PCI-DSS attestation submitted in June 2019 was completed by Finance without the required testing. The acting CIO has indicated that ITS will assume responsibility for the FY 2020 PCI-DSS testing and attestation.

3. The County should sponsor a qualified ITS employee to complete the ISA training and conduct the county's PCI-DSS self-assessment(s).
   Current Status – In Process. Revised implementation date: April 2020.
   The acting CIO reports that a qualified ITS employee has completed the ISA curriculum and will take the ISA qualification exam in April. That employee will conduct the county's PCI-DSS self-assessment for FY2020.

4. An executive officer of the County, such as the County Administrator, Assistant County Administrator, Chief Information Officer or Chief Financial Officer should sign the Assessment of Compliance.
   Current Status – In Process. Revised implementation date: June 2020.
   Neither the CIO nor the CFO signed the FY2019 Attestation of Compliance. In fact, no County official signed the attestation. The acting CIO has indicated that the FY2020 Attestation of Compliance will include signatures.

5. The CAO should either revise the Protection of Personal Information Policy to encompass PCI-DSS or develop a separate policy addressing payment card security.
   Current Status – In Process. Revised implementation date: June 30, 2020.
   The acting CIO reports that ITS is actively working with County Counsel to revise the Personal Information Protection Policy to address payment card security.

6. County policy should require that county operations authorized to accept payment card payments have written procedures for processing card payments and ensuring the security of payment card information.

Current Status – In Process. Revised Implementation date: June 30, 2020.
The acting CIO reports that ITS is actively working with County Counsel to revise the Personal Information Protection Policy to include this requirement.

7. The county's Internal Security Assessor should complete a single PCI-DSS SAQ-D to assess the compliance of all county payment card operations, including those utilizing the third-party online payment processor.
   Current Status – In Process. Revised implementation date: June 2020.
   The County has not yet qualified an ITS employee as an Internal Security Assessor. The FY 2019 self-assessment by Finance resulted in multiple SAQ-Ds. The acting CIO indicated that ITS intends to implement this recommendation with the FY2020 self-assessment.

IV. About this Review

In January 2020 we initiated a follow-up review to determine whether the County had implemented the recommendations of our April 2019 Audit of the PCI-DSS self-assessment process. We asked the County Administrator and the responsible department(s) to describe any actions taken to implement the Auditor's recommendations, and to provide documentation that would support the actions taken. We reviewed the response to our request, reviewed the documentation submitted, and collected additional information as necessary to provide sufficient, appropriate evidence to conclude whether each recommendation was fully implemented.

We concluded that a recommendation was:

- **Fully Implemented** if we found that the recommended actions had been completed or that the County had adequately addressed the issues identified by the Auditor by alternative means,
- **Partially Implemented** if we found that the County had completed some, but not all, actions and planned to take no further action on the recommendation,
- **Not Implemented** if we found that the County had taken no action to implement the recommendation and did not plan to take action,
- **In Process** if the County planned to take further action to implement a recommendation.

We conducted this follow-up audit in accordance with generally accepted government auditing standards, except that our office has not had an external peer review performed by reviewers independent of the audit organization. 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.

signed:

_jlh_____
John Hutzler, CIA, CGAP, CCSA
Washington County Auditor