Washington County
Auditor's Office

Final Follow-Up Report

Assessing Compliance with the

Payment Card Industry Data Security Standard

December 13, 2022

County Auditor John Hutzler, CIA, CGAP, CCSA

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.

In our first follow-up report in February 2020, we found that implementation of all seven of the audit recommendations remained In Process four months beyond originally targeted dates for completion.

In our second follow-up review in March 2021. We found that management had Fully Implemented four of the recommendation. Three recommendations remained In Process.

In this final follow-up report, we find that management has partially implemented two of the remaining recommendations and had not implemented the other two

In summary, of the seven recommendations, management fully implemented four, partially implemented two and did not implement one.

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. Status of Recommendations

1. The County should use official PCI DSS SAQ forms and perform all expected testing before attesting to the county's compliance.
   Final Status – Partially Implemented. In its first attestation in 2020, ITS reported that the County was Not In Compliance for which the County incurred fines of more than $11,000. The County requested an extension, reported in 2021 that it was In Compliance, and received a refund of the fines imposed. We did not review the 2021 attestation.

ITS reports that it has fully implemented this recommendation, and it is clear from the material submitted that the County made considerable progress toward CIS DsS compliance. However, ITS could not provide evidence that it had performed all required testing for its 2022 attestation, that documented all policies and procedures that should have been reviewed had been adopted, or that it had performed a comprehensive risk assessment. We concluded that, while the County used the official PCI DSS SAQ form, it did not perform all required testing before attesting to the County's compliance.

Submitting a false attestation of PCI DSS compliance can also result in fines and penalties. We urge the Chief Information Officer, or any County official asked to execute a PCI DSS attestation, to seek the advice of legal counsel on whether executing a false attestation may constitute fraud.

2. The CAO should transfer responsibility for PCI DSS Self-Assessment from Finance to Information Technology Services (ITS).
   Final Status – Fully Implemented. In January 2020, the County Administrator transferred responsibility for completing the PCI DSS Self-Assessment from Finance to ITS.

3. The County should sponsor a qualified ITS employee to complete the ISA training and conduct the county's PCI DSS self-assessment(s).
   Final Status – Fully Implemented. Two ITS employees completed the ISA training and conducted the county's 2020 PCI DSS Self-Assessment.
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.
   Final Status – Fully Implemented. The Chief Information Officer signed the 2020 PCI DSS 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.
   Final Status – Partially Implemented. In June 2020 the County amended its Protection of Personal Information Policy (PIP), but it does not encompass PCI DSS requirements and there are no procedures implementing the policy. County plans to amend the Fiscal Policy to encompass PCI DSS requirements appear to have been abandoned.

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.
   Final Status – Partially Implemented. The County has adopted a policy .

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.
   Final Status – Fully Implemented. in June 2020 ITS completed a single PCI DSS SAQ-D covering all county payment card operations.

IV. About this Review

In September 2022 we initiated our third and final 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,

signed:

John Hutzler, CIA, CGAP, CCSA
Washington County Auditor

WASHINGTON COUNTY
OREGON

Memorandum

To: John Hutzler, County Auditor

From: Tanya Ange, County Administrator Tanya Ange

cc: Board of County Commissioners

Date: December 12, 2022

Subject: Response to follow-up and new audits submitted for Dec. 13

In your elected role as County Auditor, you have provided seven follow-up audits as part of your presentation to the Washington County Board of Commissioners meeting packet for December 13, 2022. I commend staff for their work especially over the last two weeks to prioritize responding to your requests for the community that we both serve. This demonstrates a respect for your elected role and the shared value that employees place on effective and efficient local government employees.

It is my understanding that follow-up audits do not require a management response as they are based on the scope of the original audit. After an initial review of your audits, it appears that there are three audits that I need to respond to as management does not agree with your position and/or the follow-up has gone beyond the scope of the original audit. I am sending this memo to you and will be adding this memo to the Board's agenda packet for public transparency. I should note that you have not requested a management response for any of the seven follow-up audits included in the packet for December 13, 2022.

Auditor's Response: Thank you for your response to the Emergency Ambulance Franchise follow-up report. You are correct that a management response is not required. However, since you have submitted your response, I will include it, along with my response when I publish my report. Had you chosen to respond during last night's Board meeting, I would have addressed your concerns at that time. My responses to the points you raise follow.

3. Payment Card Industry Data Security Standards (PCI DSS)

Selected Sample Questions

On November 30, 2022, the Auditor submitted an urgent request for Information Technology Services to provide evidence of required testing on selected sample of questions marked as "Yes" on the PCI-DSS Self-Assessment Questionnaire D (SAQ D) report. SAQ D is used to verify compliance with PCI-DSS requirements. Although the Internal Security Assessor (ISA) who performed the testing is no longer with the County, a thorough due diligence was undertaken to discover the documentation that demonstrates how the County complies with these requirements. Within the short timeframe requested by the Auditor, we have provided the Auditor with copies of policies and procedures that were reviewed by the County staff. We have also provided evidence that the required tests were performed on the selected sample of questions.

<u>Auditor's Response</u>: I appreciate the efforts of ITS to provide evidence of its implementation of audit recommendations. I alerted them before the ISA left the County that I would need to assess his testing records, but they were apparently not available when requested. My assessment was that the evidence they were able to provide did not demonstrate full compliance.

Recommendations from 2019 PCI-DSS Audit

On December 6, 2022, the Auditor also requested status of Recommendations 5 and 6 with supporting evidence. Staff response is as follows on the two recommendations in question:

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.	A response to the County Auditor's follow-up from the 2019 PCI-DSS Audit was provided on July 20, 2021.. The 406 Comprehensive Financial Management Policy, together with 506 Personal Information Protection Policy (PIPP), addressed both of these requirements. NOTE: Policy 406 was revised and adopted by the Board of Commissioners on July 20, 2021. Policy 506 was revised and adopted by the Board of Commissioners on June 23, 2020.
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.	

We have consulted with legal counsel and are confident that the three SAQ D attestations were accurate when submitted.

<u>Auditor's Response</u>: County Counsel is entitled to his opinion regarding the accuracy of the County's most recent attestations, but this is not a legal question. (County Counsel has not addressed the legal question whether executing a false attestation might constitute fraud.)
My responsibility is to express my opinion based upon the evidence. The evidence in the original audit and three follow-ups indicates that the only accurate attestation submitted by the County in the past 10 years is the 2020 attestation that the County is not PCI DSS compliant.

Thank you again for your responses. I recognize that most of the issues described in these reports, as well as most County action to address them, occurred before you were hired as County Administrator, and I appreciate your commitment to addressing them.