Washington County
Auditor's Office

Assessing Compliance with the Payment Card Industry Data Security Standard

Final Report
April 11, 2019

John Hutzler, CIA, CGAP, CCSA
County Auditor

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

ASSESSING COMPLIANCE WITH PCI-DSS

EXECUTIVE SUMMARY

Why we audited this

We conducted this 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?

What we found

- The county's contract with US Bank requires that the County comply with PCI-DSS.

- County locations authorized by Finance to process point of sale payments processed most card transactions.

- County policies and procedures do not address security requirements for card transactions.

- Because they process fewer than 6 million card transactions per year, Finance can self-assesses compliance with PCI-DSS for the County functions it has authorized to accept card payments.

- The self-assessment process employed by Finance is a pro-forma exercise that does not satisfy PCI-DSS requirements for self-assessment. It does not provide reasonable assurance of compliance with the security standard.

What we recommend

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

- The CAO should transfer responsibility for PCI-DSS Self-Assessment from Finance to ITS.

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

- 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.

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

- 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.

- 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.

John Hutzler, CIA, CGAP, CCSA
County Auditor

.

OVERVIEW

Washington County collects a variety of payments from residents and visitors. In 2017, the County received more than 105 thousand payments by credit cards or debit cards. Payment cards from major issuers American Express, Visa, MasterCard and Discover are used for an increasing number of payments to the County. These payments range from parking at a county park to probation supervision fees and property taxes.

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. The county's contract with a major bank for card processing requires that the County comply with this standard.

Payment card data breaches and fraud are on the rise, costing organizations millions of dollars. Failure to comply with 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 Finance Division (Finance) has self-assessed compliance with this international standard annually since 2013. Although Finance has consistently reported that the County is fully compliant, we found that the process for assessing PCI-DSS compliance is a pro-forma exercise that provides little assurance that the County is, in fact, compliant with the standard.

We recommend that:

- the County adopt a policy regarding payment card security;
- departments accepting card payments adopt appropriate procedures;
- responsibility for the PCI-DSS self-assessment be assigned to Information Technology Services (ITS);
- a qualified ITS employee be trained as an Internal Security Assessor (ISA);
- the ISA complete a single Self-Assessment Questionnaire (SAQ) covering all county card payment environments and perform all expected testing; and
- an executive officer of the County attest to compliance with PCI-DSS.

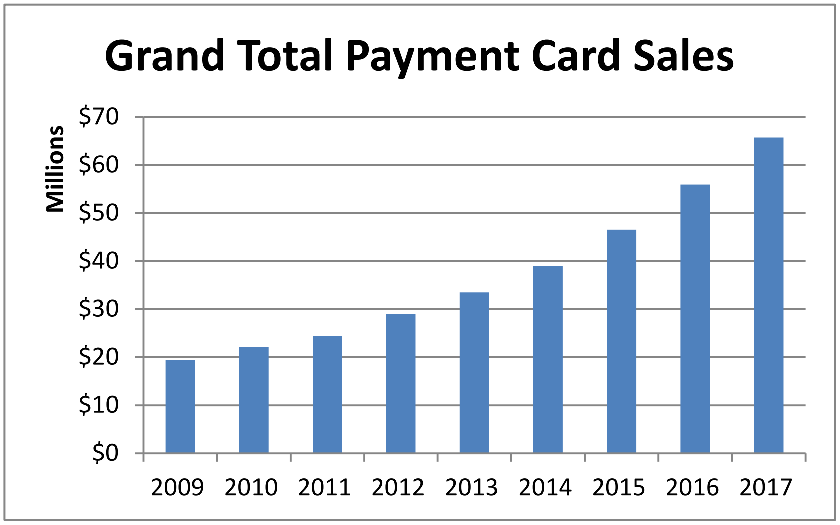
BACKGROUND

County departments, divisions or units must ask Finance to obtain a merchant identification number (MID) from US Bank to allow customers to make in person payments via credit or debit cards. To accept only online card payments, departments, divisions or units ask ITS to add them to its contract with FIS Global, the county's third-party online only payment processor.

As of May 2018, Washington County was accepting payment cards for payment of fees, fines and other obligations to the County at 23 locations or operations. Examples of such obligations include property taxes, building permits, traffic fines, and supervision fees. Eighteen of these locations have been assigned separate merchant ID numbers by US Bank. Five county operations accept payment only through FIS, the third-party payment processor.

The County selected US Bank as its primary payment-card service provider. In 2016 the County paid US Bank nearly $500,000 in payment processing fees. The County accepts American Express, VISA, MasterCard and Discover cards for payment transactions.

Revenues received through payment card transactions have risen steadily since the County began accepting such payments in 2009.



The County collected almost $66 million in net revenue on over 105,000 payment-card transactions in 2017. Eighty percent of the revenue from payment card transactions was processed by FIS. Although they accounted for only 20% of the revenue from payment card transactions, locations authorized by the Finance Division to accept point of sale payments processed most (63%) of the 105,000 card transactions.

Attacks on payment processes and breaches of merchant data have increased nationwide since 2008. The average cost per compromised record in the United States rose from $138 in 2006 to $225 in 2017. The average total cost to an organization of a data breach increased more than 36% between 2013 and 2017 to $7.35 million.

The major payment card brands (American Express, Discover, JCB International, MasterCard and Visa) established the Payment Card Industry (PCI) Security Standards Council in 2006. The Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. To protect the public's cardholder information and reduce the likelihood of fraud, the Council developed a comprehensive set of twelve international requirements known as the Payment Card Industry Data Security Standard (PCI-DSS).

Goals	***Requirements***
Build and maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Each requirement is divided into a number of sub-controls. Failing any of the sub- controls leads to non-compliance with the requirement and with the PCI standard. Although the 12 requirements have not changed since the inception of the standard, the sub-controls have been revised.

The standard is used to verify that merchants and service providers are appropriately protecting cardholder data. The PCI-DSS covers all forms of payment card (debit, credit, and merchant and company purchasing cards) and all merchants or entities that store, process or transmit cardholder data.

PCI-DSS requires organizations to maintain a secure network, implement internal controls and perform regular testing. These controls include encrypting stored data, conducting vulnerability assessments, configuring access controls and more. Compliance with the standard does not guarantee that payment systems breaches will never occur, but there is evidence that the standard is effective in lowering security risks.

The major credit card brands enforce compliance with PCI-DSS primarily through contractual agreements with banks and merchants. The County contracts with US Bank for card processing, and the Terms of Service for US Bank’s payment card processing firm, Elavon, require that the County comply with this standard. Merchants processing more than six million payment card transactions per year are required to hire an independent assessor to certify their compliance through onsite inspection. Because it processes fewer transactions, Finance completes Self-Assessment Questionnaires (SAQs) and files Attestations of Compliance (AoCs) with the bank for each of its merchant ID numbers. US Bank does not require the County to file AoCs for county functions accepting card payments only online through the third-party payment processor FIS.

FINDINGS & RECOMMENDATIONS

We found that the Finance Department's self-assessment process did not satisfy PCI-DSS requirements for self-assessment and does not provide reasonable assurance of compliance with PCI-DSS.

Expected Testing Not Performed

On its official website, PCI-DSS provides SAQ forms and detailed instructions for completing SAQs. Those instructions specify required testing for each applicable PCI requirement. The instructions direct the self-assessor to answer "Yes" to each question when "the expected testing has been performed, and all elements of the requirement have been met as stated."

Finance did not use the SAQ forms and instructions provided by PCI-DSS. Instead, a management analyst in Finance completed the self-assessment forms certifying compliance each year without performing any of the expected testing specified by PCI-DSS.

To accomplish this, Finance used TrustWave,[1] a software product of Elavon, Inc., the payment card-processing arm of US Bank. To set up a new merchant in TrustWave, the user must answer a series of questions regarding the merchant environment. The application uses this information to determine the appropriate SAQ for the merchant. TrustWave then leads the user through each of the questions for any PCI-DSS requirements for the appropriate SAQ, and the user responds with "Yes," "No," or "N/A." TrustWave makes no reference to the expected testing, nor does it instruct the user to answer "Yes" only when the expected testing has been performed. TrustWave produces an Attestation of Compliance (AoC) for the user and delivers a Certificate of Compliance (CoC) directly to Elavon and US Bank.

TrustWave provided an expedited process that allowed the user in subsequent years simply to indicate that nothing had changed in the past year. TrustWave would then produce the next AoC and CoC without requiring the user to answer any of the questions on the SAQ. The analyst completed all 18 self-assessments in a single day and performed none of the PCI-DSS expected testing.

For the various SAQs submitted for county merchants, expected testing that Finance did not perform before attesting to compliance included:

- Confirm that direct public access is prohibited between the internet and any system component in the cardholder data

[1] Although Finance now uses a different application, its functionality is similar to that of TrustWave.

environment by reviewing firewall and router configuration standards and examining those configurations.

- Ensure vendor-supplied defaults are always changed and unnecessary default accounts are removed before installing a system on the network by reviewing policies and procedures, examining vendor documentation, observing system configurations and account setting, and interviewing personnel.
- Confirm that configuration standards for all system components are consistent with industry-accepted hardening standards, are updated as new vulnerability issues are identified, and are applied when new systems are configured by reviewing system configuration standards, industry-accepted hardening standards, policies and procedures, and interviewing personnel.
- Ensure all system components and software are timely protected by reviewing policies and procedures, examining system components, and comparing the list of security patches installed to the recent vendor patch list.
- Verify that a firewall(s) is in place; examining system configurations, deletion processes and data sources to ensure stored cardholder data is protected by examining network configurations, reviewing the current network and dataflow diagrams, and observing network configurations.
- Ensure access to system components and cardholder data is limited to only those individuals whose jobs require such access by examining system configuration settings to verify password parameters, written access control policy, interviewing personnel and management, reviewing privileged user IDs, password procedures, access lists.
- Confirm transmission of cardholder data is encrypted across open, public networks by reviewing documented standards, policies and procedures, vendor documentation, wireless networks, and all locations where cardholder data is transmitted or received, observing inbound and outbound transmissions, examining system configurations, settings, keys and certificates.

- Ensure all systems are protected against malware and anti-virus software is regularly updated by examining system configurations, vendor documentation, policies and procedures, anti-virus configurations, system components, and log retention processes, interviewing personnel, and observing processes.
- Ensure physical access to cardholder data is properly restricted by observing physical access controls and personnel, interviewing personnel, including security personnel, examining media distribution, tracking logs, documentation, and storage container security, and reviewing policies and procedures for distribution and destruction of media.
- Confirm that security systems and processes are regularly tested by reviewing penetration testing methodology, examining segmentation controls, and interviewing responsible personnel.
- Ensure the county maintains a policy that addresses information security for all personnel, including contractors with access to the county’s cardholder data environment by reviewing the information security policy and procedures, usage policies, security awareness program, list of service providers, incident response plan and procedures, observing processes and interviewing responsible personnel.

We recommend that the County utilize official PCI-DSS SAQ forms and perform all expected testing before attesting to the county’s compliance.

Internal Security Assessor

The PCI Security Standards Council offers training to qualify an employee to become an Internal Security Assessor (ISA) for their organization. PCI-DSS requires that registrants for ISA training have significant relevant security audit and assessment experience (including but not limited to Network Security, Application Security and Consultancy, System Integration, and Auditing) and be sponsored by their employer. A minimum of five years of experience is recommended.

The analyst in Finance who conducted the county’s self-assessments had no formal training in how to conduct a PCI-DSS assessment and lacked the qualifications and experience to qualify for PCI training to become an ISA. County employees with the required knowledge and experience are most likely to be employed in Information Technology Services Division (ITS).

We recommend that responsibility for PCI-DSS Self-Assessment be transferred from Finance to ITS and that the County sponsor a qualified ITS employee to complete the ISA training and conduct the county's PCI-DSS self-assessment(s).

Attestation of Compliance

The PCI Security Standards Council requires that an executive officer of the organization execute the Attestation of Compliance. We found that only the analyst in Finance had signed the AoCs.

We recommend that an executive officer of the County, such as the County Administrator, Assistant County Administrator, Chief Information Officer or Chief Financial Officer, sign the AoCs.

County Policies and Procedures

Existing county financial policies and privacy policies do not address the security requirements of the PCI-DSS. Washington County adopted a Personal Information Protection Policy to implement the requirements of Oregon's recently enacted Consumer Theft Protection Act and provide guidance to county employees on how to protect and maintain files that contain personal information. In 2015 the County adopted a HIPAA Privacy policy to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 and Health Information for Economic and Clinical Health Act (HITECH). The definitions of personal information and protected health information in those policies do not encompass all cardholder data and sensitive access information that must be protected to comply with PCI-DSS.

TrustWave produced a "Security Policy" for each county merchant that addressed generically the PCI-DSS requirements applicable to the merchant environment. The Finance analyst printed and retained the security policy for each county merchant. However, those policies were not approved or adopted by anyone in Washington County. They had no standing in the County, and the analyst did not provide them to the merchant departments.

W***e recommend that the CAO either revise the Personal Information Protection Policy to encompass PCI-DSS or develop a separate policy addressing payment card security. The policy should require that county operations authorized to accept card payments have written procedures for processing card payments and ensuring the security of payment card information.***

Multiple Assessments

We found that every county operation processing payment card transactions through US Bank had a distinct MID and Finance completed a SAQ for each MID. The questionnaire and requirements vary depending on the merchant environment. For example, SAQ-A addresses PCI requirements applicable to merchants who completely outsource cardholder data functions to validated third parties. SAQ-B addresses PCI requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. SAQ-C addresses requirements applicable to merchants whose payment application systems are connected to the Internet. There are nine different SAQs that address various merchant environments.

Merchants who operate a variety of payment card environments may use SAQ-D, which covers all requirements. Washington County used five different SAQs forms to report the compliance of its 18 merchant locations. For most locations, the County used SAQ-B. We see no benefit to the County in completing a separate SAQ for each location.

We recommend the county ISA 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.

OBJECTIVES, SCOPE & METHODOLOGY

We conducted this audit to determine whether the Finance Division's self-assessment process for compliance with the Payment Card Industry Data Security Standard (PCI-DSS) provides reasonable assurance of county compliance with the standard.

To accomplish our audit objective, we reviewed county policies and procedures related to payment card processing. We reviewed the county's payment card environment and the annual reports of compliance with PCI-DSS. To gain an understanding of county payment card data security oversight and governance, we interviewed Finance and ITS management and staff, and observed self-assessment and attestation of compliance processes.

To identify PCI data security compliance requirements and best practices, we reviewed the Payment Card Industry Security Standards Council reports and guidance. We also reviewed the major bank card brand's requirements for payment card data. To gain an understanding of PCI data security compliance trends and data breaches across various industries, we reviewed research from national organizations and data security companies, and audits from other jurisdictions.

The scope of our review included the Finance Division's annual self-assessment processes for 2015 through 2018.

COMPLIANCE WITH AUDIT STANDARDS

United States Government Accountability Office

GAO

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision

GAO 90 YEARS

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we have not had an external peer review. 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 provides a reasonable basis for our findings and conclusions based on our audit objectives.

signed:

Audit Team: County Auditor: John Hutzler, CIA, CGAP, CCSA
Reviewer: Keith Shoop, CGAP

SUMMARY OF AUDIT 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 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).

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.

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.

WASHINGTON COUNTY
OREGON

Date: April 3, 2019

To: John Hutzler, County Auditor

From: Robert Davis, County Administrator
Don Bohn, Assistant County Administrator DB
Joel Bradach, Chief Information Officer
Jack Liang, Chief Finance Officer

Subject: Audit of Payment Card Industry Data Security Standard

Thank you for the opportunity to respond to the audit of payment card industry (PCI) data security standard dated March 22, 2019.

The County Administrative Office and Department of Support Services agrees with the recommendations and appreciates the thorough and thoughtful review of PCI compliance.

Below is a response to each of the seven recommendations:

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

   The County agrees and will develop a written plan detailing the process and procedures for testing and attesting compliance. The plan will be completed by October 1, 2019.

2. *The CAO should transfer responsibility for PCI-DSS Self-Assessment from Finance to ITS.*

   The County agrees and has documented this transfer in writing.

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

   The County agrees. In addition to sponsoring training for appropriate staff member(s); ITS will also assess the availability of duly trained contractors qualified to complete the self-assessment on the County's behalf. With either approach, ITS will take the lead on ensuring qualifications, documentation and follow-up.

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.*

   The County agrees. The Chief Information Officer and Chief Finance Officer will be co-signatories on the compliance documents.

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.*

   The County agrees. The County will update the Protection of Personal Information Policy to include payment card security. This policy update will be completed by October 1, 2019.

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.*

   The County agrees. All County operations authorized to accept card payments will have documented written procedures by October 1, 2019.

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.*

   The County agrees and will pursue a single PCI-DSS SAQ-D to achieve enterprise-wide compliance upon validating this approach is acceptable under the PCI-DSS guidelines. This approach will be pursued as part of the next PCI compliance process.

Recognizing the interface of PCI compliance between ITS and Finance, the two divisions will continue to work closely to develop written procedures, train staff and complete appropriate testing as part of the attestation process. Protecting confidential and sensitive information is a priority for the County.

We look forward to working with you and your staff in the future.