AUDIT REPORT

Salt Lake County

PCI DATA SECURITY STANDARDS

JANUARY 2023

Chris Harding, CPA, CFE, CIA
County Auditor

Office of the Auditor
Salt Lake County

Audit Team

Matt Cullinen, Internal Auditor
Tammy Brakey, Internal Auditor
Audra Bylund, Audit Manager
Brenda Nelson, CISA, Audit Manager

Audit Management

Chris Harding, CPA, CFE, CIA, Auditor
Richard Jaussi, MBA, Chief Deputy Auditor
Shawna Ahlborn, Audit Division Director

Office of the Auditor
Salt Lake County
2001 S State Street, Ste N3-300
Salt Lake City, UT 84190-1100
Phone: (385) 468-7200

www.slco.org/auditor

Salt Lake County Auditor

Chris Harding, CPA, CFE, CIA
County Auditor

2001 S State Street, Ste N3-300, Salt Lake City, UT 84190
Phone: (385) 468-7200 www.slco.org/auditor

AUDITOR'S LETTER

We conducted a PCI audit of all 19 County agencies and three non-county entities that accept payment cards to ensure they are in compliance with Countywide policy 1400-7, Payment Card Industry Data Security Standard Policy. We determined that each was using the correct self-assessment questionnaires and/or attestation of compliance forms. We had a single moderate-risk finding in which we noted a contract was not in compliance with the above policy by the stated deadline of September 30, 2022, but the issue was resolved the following week.

This audit is authorized pursuant to Utah Code Ann. 17-19a-204 "Auditing Services." We conducted this audit in accordance with generally accepted government auditing standards (GAGAS), except for the requirement in GAGAS 3.18, which states, "In all matters relating to the GAGAS engagement, auditors and audit organizations must be independent from an audited entity." GAGAS states in 3.21, "Independence comprises the following:

> a. Independence of mind: The state of mind that permits the conduct of an engagement without being affected by influences that compromise
> professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.
> b. Independence in appearance: The absence of circumstances that would cause a reasonable and informed third party to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the engagement team had been compromised.

Our state statute, 17-19a-206 Performance audit services, reads:

> (1) A county auditor shall, under the direction and supervision of the county legislative body or county executive and subject to Subsections (1)(b) and (2), provide performance audit services for a county office, department, division, or other county entity. A county auditor may not conduct a performance audit of the auditor's own office.
> (2) The county legislative body or county executive shall establish the goals and nature of a performance audit and related services.

Although this audit is not a performance audit, GAGAS 3.19 states: "auditors and audit organizations should avoid situations that could lead reasonable and informed third parties to conclude that the auditors and audit organizations are not independent and thus are not capable of exercising objective and impartial judgment on all issues associated with conducting the engagement and reporting on the work."

A reasonable and informed third party is defined by GAGAS: "As evaluated by a hypothetical person, a person who possesses skills, knowledge, and experience to objectively evaluate the appropriateness of the auditor's judgments and conclusions. This evaluation entails weighing all the relevant facts and

circumstances, including any safeguards applied, that the auditor knows, or could reasonably be expected to know, at the time that the evaluation is made."

Although we are working with the State Legislature, County Council and Mayor, Utah Association of Counties, Utah Association of CPAs, to change this statute, we currently have no control or ability to change this statute. As such there is a risk that readers of our report would conclude that we are not capable of exercising objective and impartial judgment on the audit subject matter.

GAGAS standards require that we plan and perform the audit to obtain suffcient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Except for the independence issues above, we believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives."

We appreciate the leaders and team members at the various agencies and departments who shared their time and knowledge with us during the audit.

Please contact me at 385-468-7200 with any questions.

Chris Harding, CPA, CFE, CIA
Auditor

Contents

REPORT HIGHLIGHTS

PCI DATA COMPLIANCE

JANUARY 2023

Objectives

To accomplish the audit objectives, we:

- Identified all County agencies that accept payment cards, and therefore are required to validate their compliance with the PCI DSS annually.
- Evaluated the cardholder data environment for each agency to determine if the correct SAQ type was completed.
- Reviewed all 2022 SAQs and AOCs to determine if all sections were completed and answered accurately and completely.
- Reviewed contract agreements with outsourced contractors to verify that the agreements included requirements that outsourced contractors comply with the PCI DSS and Countywide Policy 1400-7.

All 22 of the County and non-county entities that were required to demonstrate their compliance with the Payment Card Industry Data Security Standards ("PCI-DSS") in 2022, did so by the September 30th deadline.

Countywide Policy 1400-7 states that agencies that collect payment card revenue on behalf of the County will demonstrate their compliance with PCI-DSS annually to the County Auditor by September 30th. We identified 19 County, and three non-county entities, that were required to submit an annual Self-Assessment Questionnaire ("SAQ") and/or Attestation of Compliance ("AOC") to demonstrate their compliance with the PCI DSS in 2022. All SAQs and AOCs were submitted by the deadline to the Auditor for verification and review. Each were found to be complete, accurate, and signed by an appropriate level of organizational authority. We verified that each County agency's SAQ and AOC was completed correctly and accurately to the best of their knowledge and based on our understanding of their payment card processing environments.

Outsourced Contractors Demonstrated PCI DSS Compliance.

Countywide Policy 1400-7 includes in its scope County agencies and a list of other entities that "accept, store, process, or transmit cardholder data (electronically or on paper), their employees, volunteers, and anyone else who has access to the Salt Lake County cardholder data environment, including contractors, consultants, and others with a business association with Salt Lake County…Outsourced Contractors." During the audit, we identified three non-county entities that met the definition of an "Outsourced Contractor," under County Policy 1400-7. We found that all three of the outsourced contractors identified during the audit demonstrated their compliance with the PCI DSS by completing and submitting an AOC form (as required by County Policy 1400-7) before the September 30th deadline to the Auditor for review.

An addendum to an Intermountain Contract was not signed by the September 30th deadline.

Countywide Policy 1400-7 states that County agencies ensure that written agreements with outsourced contractors include in them the requirements for compliance with Countywide Policy 1400-7 and with PCI-DSS standards 3.3.2. We found that the contract with Intermountain Medical Group ("IMG"), which manages the HealthyMe Clinic, did not include language regarding compliance with Countywide Policy 1400-7 and PCI DSS. An updated addendum was sent to IMG for signatures on September 12, 2022. Unfortunately, they were unable to have the necessary parties sign the addendum by the Countywide PCI compliance deadline of September 30. This finding did not have an impact on IMG providing the necessary AOC form by the September 30th deadline. Management provided the signed addendum of both parties on October 4, 2022.

Finding Risk Classifications

Classification	Description
1 – Low Risk Finding	Low risk findings may not have an effect on providing reasonable assurance that: (1) Cash receipts and receivables are recorded and reported accurately, completely and free from significant error (2) Processes and procedures for cash receipts and receivables are in accordance with County policies and standards or (3) Management provides adequate fiscal oversight to properly safeguard against loss, theft, waste or abuse. Recommendations may or may not be given to address the issues identified in the final audit report. If recommendations are given, management should try to implement the recommendations within one year of the final audit report date if possible. Follow-up audits may or may not focus on the status of implementation.
2 – Moderate Risk Finding	Moderate risk findings may have an effect on whether there is reasonable assurance that: (1) Cash receipts and receivables are recorded and reported accurately, completely, and free from significant error (2) Processes and procedures for cash receipts and receivables are in accordance with County policies and standards or (3) Management provides adequate fiscal oversight to properly safeguard against loss, theft, waste or abuse. Recommendations will be given to address the issues identified in the final audit report. Management should implement the recommendations within one year of the final audit report date if possible. Follow-up audits will focus on the status of implementation.

Finding Risk Classifications	
3 – Significant Risk Finding	Significant risks are the result of one or more findings that may have an effect on whether there is reasonable assurance that: (1) Cash receipts and receivables are recorded and reported accurately, completely, and free from significant error (2) Processes and procedures for cash receipts and receivables are in accordance with County policies and standards or (3) Management provides adequate fiscal oversight to properly safeguard against loss, theft, waste or abuse. Recommendations will include necessary corrective actions that address the significant risks identified in the final audit report. Management should implement the recommendations within six months of the final audit report date if possible. Follow-up audits will focus on the status of implementation.
4 – Critical Risk Finding	Critical risks are the result of one or more findings that would have an effect on whether there is reasonable assurance that: (1) Cash receipts and receivables are recorded and reported accurately, completely, and free from significant error, (2) Processes and procedures for cash receipts and receivables are in accordance with County policies and standards, or (3) Management provides adequate fiscal oversight to properly safeguard against loss, theft, waste or abuse. Recommendations will include necessary corrective actions that address the critical risks identified in the final audit report. Management should implement the recommendations as soon as possible. Follow-up audits will focus on the status of implementation.

BACKGROUND

Salt Lake County organizations accept credit and debit cards ("payment cards") as a form of payment for a wide variety of goods and services provided to County residents and customers. In 2021, County agencies processed more than one million payment card transactions totaling $76.8 million in revenue. County residents and customers can use payment cards to pay for many types of County services and programs such as fitness and recreation center passes, theater tickets, youth sports registrations, library fines and fees, document recording fees, pet licenses, donations, and property taxes. County organizations benefit from accepting payment cards by receiving payment more quickly, and County residents and customers enjoy the convenience of being able to use payment cards to pay for goods and services offered by the County.

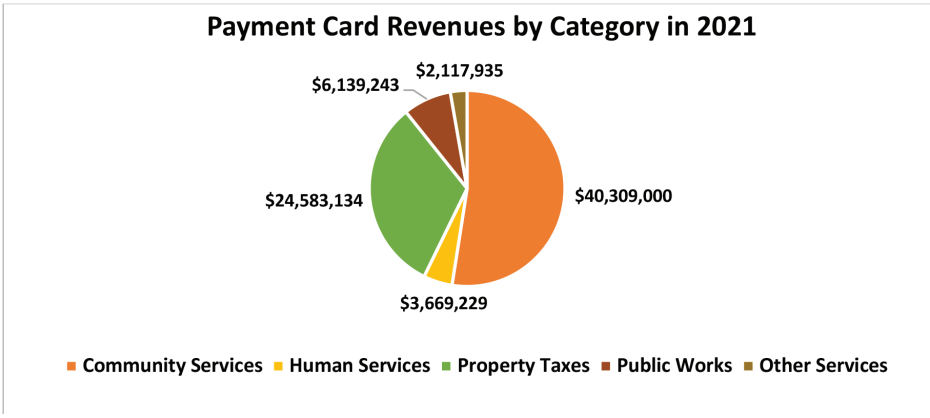
County agencies processed $76.8 million in payment card transactions during 2021, up from $49.8 million in 2020.

Overall, 2021 payment card revenue increased 54% from 2020, indicating a recovery within 6% of payment card revenue prior to the pandemic in 2019. Property Taxes accounted for 28% of the increase in payment card revenue from 2019 to 2021. Community Services credit card revenue increased 139% from 2020. However, the department still had fewer transactions than prior to the pandemic, with 14% less in payment card revenue in 2021 than in 2019. Community Services includes agencies such as Parks and Recreation, Library Services, and the Clark Planetarium, which were shut down during portions of 2020 and 2021.

For the purposes of this audit, we categorized County payment card revenues into five major categories:

- Human Services
- Community Services
- Public Works
- Property Tax Payments
- Other Services

The total dollar amount of payment card transactions in each of the five categories during 2021, is shown in Figure 1.



The Payment Card Industry Data Security Standard

The Payment Card Industry ("PCI") Data Security Standard ("Standard" or "DSS") is a set of 12 requirements, created and maintained by the PCI Security Standard Council ("Security Council" or "PCI SSC"). The Security Council is a private sector body, made up of all the major payment card brands, including American Express, Discover, MasterCard, Visa, and JCB International. The goal of the PCI DSS is to protect the public's cardholder data and to decrease the likelihood of payment card fraud.

Compliance with the PCI DSS is mandatory for any entity, public or private, that stores, processes, or transmits cardholder data. The PCI DSS requires organizations to build and maintain a secure network; encrypt and protect stored cardholder data; maintain a vulnerability management program; implement a strong user access control environment; monitor and test networks regularly; and maintain an information security policy. Table 1 lists the goals and specific requirements of the PCI DSS.

Table 1. PCI DSS Goals and Requirements. The primary goal of the PCI DSS is to protect cardholder data and decrease the likelihood of payment card fraud. The requirements apply to any entity that stores, processes, or transmits cardholder data.

PCI DSS Goals and Requirements	
Goals	**PCI DSS 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.

Source: Payment Card Industry (PCI) Data Security Standard, v3.2.1.

Securing cardholder data is a challenge facing all merchants that process payment cards. Complying with the PCI DSS is a way to help prevent a data breach of payment card data. In a recent study[1] conducted by the Ponemon Institute, LLC, a data breach is defined as:

"An event in which an individual's name and a medical record, a financial record or both, or debit card are potentially put at risk. These records can be in electronic or paper format."

In 2021, Ponemon estimated the global per record cost of a data breach at $161. In the 2022 report, Ponemon increased this estimate to $164 for the average per record cost of a data breach. The study examined breaches sized between 2,200 and 102,000 records. The Ponemon study defines a compromised record as:

"A record is information that identifies the natural person or individual whose information has been lost or stolen in a data breach. Examples include a database with an individual's name, credit card information and other personally identifiable information (PII) or a health record with the policyholder's name and payment information."

Measured in USD (Source: IBM Security, Cost of a Data Breach Report 2022)

Some of the negative effects of a data breach involving cardholder data according to the PCI SSC[2] include:

- Loss of confidence by cardholders and customers, resulting in decreased revenues.
- Costs of reissuing new payment cards to replace compromised cards.
- Legal costs, settlements, and judgments.
- Regulatory fines and penalties.
- Termination of ability to accept payment cards.

The Ponemon study found that eighty-three percent of the organizations they studied experienced more than one data breach. Seventeen percent claimed it was their first data breach. Eleven percent of the breaches were from ransomware attacks, which was an increase of 41% from 2021.

The 2021 report saw the same order of the top four initial attack vectors (see table 2 below). While second in percentage of breaches, the costliest initial attack vector in 2022 on average was phishing at $4.91 million

1 Benchmark research sponsored by IBM Security, study conducted by Ponemon Institute, LLC, 2022 Cost of a Data Breach Report.

2 https://www.pcisecuritystandards.org/pci_security/why_security_matters, September 8, 2021

Table 2. Average total cost and frequency of data breaches of the top four attack vectors. There was consistency in the type and percentage of consistency of attack vectors from 2021 to 2022.

Attack Vector	Percent of breaches	Average total Costs in millions	Ranking by percent 2022	Ranking by percent 2021
Compromised Credentials	19%	$4.50	1	1
Phishing	16%	$4.91	2	2
Cloud misconfiguration	15%	$4.14	3	3
Vulnerability in 3rd party software	13%	$4.55	4	4

The PCI DSS Compliance Validation Process

The Standard Security Council requires that all payment card merchants validate that they comply with the PCI DSS at least annually. Depending on the merchant's annual volume of payment card transactions, and their payment card processing environment, some smaller merchants can validate their compliance through a self-assessment process.

In the self-assessment compliance validation process, merchants are required to complete a Self-Assessment Questionnaire ("SAQ") and attest to their compliance with the PCI DSS through an Attestation of Compliance ("AOC") form. Copies of completed SAQs and AOCs must be sent to the merchant's bank once a year as well. Detailed descriptions of each SAQ type are provided for reference in Appendix A.

When a merchant uses a third-party vendor to process payment card transactions on their behalf, then the PCI DSS states that the merchant is responsible for ensuring that the third-party vendor demonstrates their compliance with the PCI DSS at least annually and maintaining records of the compliance validation process.

OBJECTIVES AND SCOPE

Our overall audit objective was to determine whether all county entities and outsourced contractors that accept payment cards met the PCI DSS compliance validation requirements during 2022, as required by Countywide Policy 1400-7. The specific audit objectives were to:

- Determine if each County agency completed the appropriate level of SAQ, based on their annual number of payment card transactions and their unique payment card processing environment.
- Determine if outsourced contractors that process payment card transactions on behalf of the County satisfied the PCI DSS compliance validation requirements consistent with Countywide Policy 1400-7.
- Continue to monitor the impact of the Coronavirus (COVID-19) pandemic on the County's payment card processing environment and determine any impact on the County agency's PCI DSS compliance validation requirements.

To accomplish the audit objectives, we:

- Identified all County agencies that accept payment cards, and therefore are required to validate their compliance with the PCI DSS annually.
- Evaluated the cardholder data environment for each agency to determine if the correct SAQ type was completed.
- Reviewed all 2022 SAQs and AOCs to determine if all sections were completed and answered accurately and completely.
- Reviewed contract agreements with outsourced contractors to verify that the agreements included requirements that outsourced contractors comply with the PCI DSS and Countywide Policy 1400-7.

AUDIT CRITERIA

County agencies that accept payment cards must demonstrate compliance with the PCI DSS annually. Countywide Policy 1400-7, "Information Technology Security-Payment Card Industry Data Security Standard Policy," Section 5.0, Enforcement, states: "County agencies that collect payment card revenue on behalf of the County will demonstrate their compliance with PCI-DSS annually to the County Auditor by September 30th. County agencies found to be non-compliant will have a 6-month grace period to become compliant. County agencies that are deemed non-compliant after the 6-month grace period shall cease accepting, processing, transmitting, or storing cardholder data until such time that they are deemed compliant by the County Auditor." (Countywide Policy 1400-7, 3.0, p. 3)

AUDIT RESULTS

County Agencies Successfully Completed PCI DSS Compliance Validation Requirements

County agencies that accept payment cards must demonstrate compliance with the PCI DSS annually. Countywide Policy 1400-7, "Information Technology Security-Payment Card Industry Data Security Standard Policy," Section 5.0, Enforcement, states: "County agencies that collect payment card revenue on behalf of the County will demonstrate their compliance with PCI-DSS annually to the County Auditor by September 30th. County agencies found to be non-compliant will have a 6-month grace period to become compliant. County agencies that are deemed non-compliant after the 6-month grace period shall cease accepting, processing, transmitting, or storing cardholder data until such time that they are deemed compliant by the County Auditor." (Countywide Policy 1400-7, 5.0, p. 4)

Our audit focused on determining the correct merchant level and

SAQ-type for each County or non-county entity that was required to demonstrate PCI DSS compliance. We evaluated each SAQ as the entities submitted them to the Auditor to determine if the forms were completed correctly based on our understanding of each entity's payment card processing environment. If any deficiencies were identified, we contacted the agency to correct the error(s) in the forms and have them resubmitted for our review. This process sometimes took several contacts with the agency before we were able to determine if all areas of the forms were completed correctly.

We identified 19 County, and three non-county entities, that were required to submit an annual SAQ and/or AOC to demonstrate their compliance with the PCI DSS in 2022. The audit scope was expanded in 2022 to include an additional agency, the District Attorney's Office, due to the office beginning collection of payment cards. All identified County and non-county entities and their total payment card revenues and total number of payment card transactions are listed in Appendix B.

Table 3. PCI DSS Compliance Validation Requirements in 2022. The number of County agencies required to provide an annual SAQ and AOC to the Auditor's Office was 19 in 2022. Three non-county entities were required to provide only their annual AOC to comply with changes to Countywide Policy 1400-7.

Changes to PCI DSS Compliance Validation Requirements in 2022			
	Required Documentation		
County Entity	2022	2021	Explanation
County Agencies Required to Submit an SAQ & AOC			
Aging and Adult Services	SAQ & AOC	SAQ & AOC	*No Change*
Animal Services	SAQ & AOC	SAQ & AOC	*No Change*
Archives	SAQ & AOC	SAQ & AOC	*No Change*
Arts & Culture	SAQ & AOC	SAQ & AOC	*No Change*
Assessor's Office	SAQ & AOC	SAQ & AOC	*No Change*
Clerk's Office	SAQ & AOC	SAQ & AOC	*No Change*
Criminal Justice Services	SAQ & AOC	SAQ & AOC	*No Change*
District Attorney	SAQ & AOC	N/A	*Collected payments in 2022, not 2021*
Engineering and Flood Control	SAQ & AOC	SAQ & AOC	*No Change*
Health Department	SAQ & AOC	SAQ & AOC	*No Change*
Justice Court	SAQ & AOC	SAQ & AOC	*No Change*
Library Services	SAQ & AOC	SAQ & AOC	*No Change*
Parks and Recreation – Rec. Centers	SAQ & AOC	SAQ & AOC	*No Change*
Parks and Recreation – Golf Courses	SAQ & AOC	SAQ & AOC	*No Change*
Planetarium	SAQ & AOC	SAQ & AOC	*No Change*
Recorder's Office	SAQ & AOC	SAQ & AOC	*No Change*
Solid Waste Management	SAQ & AOC	SAQ & AOC	*No Change*
Surveyor's Office	SAQ & AOC	SAQ & AOC	*No Change*
Treasurer's Office	SAQ & AOC	SAQ & AOC	*No Change*
Outsourced Contractors (Non-County Entities) Required to Submit an AOC			
Healthy-Me Clinic	AOC	AOC	*No Change*
SMG (Salt Palace, MA Expo, Equestrian Park*)	AOC	AOC	*No Change*
USU Extension Services	AOC	AOC	*No Change*

**Equestrian Park was sold to Utah State University in 2021 and no longer in scope for compliance or payment card transactions.*

We found that all 22 County and non-county entities required to demonstrate their compliance with the PCI DSS in 2022, did so by the September 30, 2022, deadline. However, one outsourced contractor did miss the deadline for an updated signed contract addendum to include compliance with CWP 1400-7 and PCI DSS. We verified that each County agency's SAQ and AOC was completed correctly and accurately to the best of their knowledge and based on our understanding of their payment card processing environments.

Table 4. Entity – SAQ Type(s) – 2022 Completion Dates. All County and non-county entities that were required to demonstrate compliance with the PCI DSS, completed an SAQ and/ or AOC by the annual September 30 deadline.

Entity – SAQ Type(s) – 2022 Completion Dates		
County Agency	**2022 SAQ Type(s)**	**2022 Completion Date**
Aging and Adult Services	C	6/24/2022
Animal Services	C	5/9/2022
Archives	A	6/23/2022
Arts and Culture	C	7/1/2022
Assessor	A	5/25/2022
Clerk	B-IP	9/12/2022
Criminal Justice Services	B-IP	4/27/2022
District Attorney	A	6/14/2022
Engineering and Flood Control	C-VT	6/23/2022
Health Department	B-IP	6/14/2022
HealthyMe Clinic SL Gov. Center	D	04/01/2022
Justice Courts	C	08/10/2022
Library Services	B-IP	09/28/2022
Parks and Recreation – Golf	C	08/09/2022
Parks and Recreation Centers	C	08/15/2022
Planetarium	C	05/03/2022
Recorder	C	07/19/2022
SMG - 2 venues	C	01/18/2022
Solid Waste Management	C	04/06/2022
Surveyor	C-VT	3/17/2022
Treasurer	C-VT	7/27/2021
USU Extension Services	D	7/1/2021

We found that all County agencies and two outsourced contractors remained the same SAQ types in 2022 as they were in 2021. The third outsourced contractor, USU Extension, changed their AOC type from B-IP to D in 2022. The District Attorney's Office was required to complete both SAQ and AOC forms for 2022 as they received payments for a camp and a conference in the year.

Outsourced Contractors Demonstrated PCI DSS Compliance

Countywide Policy 1400-7, "Information Technology: Payment Card

Industry Data Security Standard Policy," Section 1.0, Scope, states: "The scope of this policy includes County agencies and other entities listed below that accept, store, process, or transmit cardholder data (electronically or on paper), their employees, volunteers, and anyone else who has access to the Salt Lake County cardholder data environment, including contractors, consultants, and others with a business association with Salt Lake County…Outsourced Contractors." (CWP 1400-7, 1.0, p. 1)

The definition of an "Outsourced Contractor," states: "Non-County entities that accept, store, process, or transmit cardholder data (electronically or on paper) on behalf of the County, using either the County's IT systems or resources or an independent IT system." (CWP 1400-7, 2.0, p.3)

During the audit, we identified three non-county entities that met the definition of an "Outsourced Contractor," under Countywide Policy 1400-7. According to the policy, any entity meeting the definition of an outsourced contractor is required to demonstrate their compliance with the PCI DSS by providing an annual AOC form to the Auditor by September 30th.

The non-county entities that we identified as outsourced contractors according to the policy were:

- Spectator Management Group ("SMG") that provides professional management services for two County-owned facilities including: the Calvin L. Rampton Salt Palace Convention Center and the Mountain America Exposition Center. SMG is now ASM Global. This change had no impact on PCI DSS Compliance.
- Healthy-Me Clinic managed by Intermountain Medical Group.
- USU Extension Services managed by Utah State University and located in the Salt Lake County Government Center.

We found that all three of the outsourced contractors identified during the audit demonstrated their compliance with the PCI DSS by completing and submitting an Attestation of Compliance form before the September 30th deadline to the Auditor for review.

The Coronavirus (COVID-19) Pandemic Continues to have Minimal Impact on PCI DSS Compliance Validation Requirements

Due to the Coronavirus pandemic, declared on March 13, 2020, payment card processing procedures throughout County facilities were modified to ensure continuity of operations where possible, while adhering to state and local public health orders. These modifications included contactless payment procedures, such as customer-only contact with payment card readers, and over-the-phone or online payment options.
Through our preliminary survey, email correspondence, and phone calls with County agencies, we found that agencies continued to implement

these contactless payment procedures in 2022. These changes did not significantly affect agency's SAQ types or substantially change their PCI DSS compliance validation requirements. County employees should be commended for their continuing efforts to ensure the safety and security of cardholder data and compliance with the PCI DSS in their organizations.

CONCLUSION

We found that all 22 of the County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2022, did so by the September 30th deadline. All SAQs and AOCs submitted to the Auditor for verification and review, were found to be complete, accurate, and signed by an appropriate level of organizational authority. The one finding related to the contract addendum with Intermountain Medical Group was resolved four days after the September 30th deadline.

FINDING 1 AND RECOMMENDATION

Addendum to Intermountain Contract not signed by September 30th deadline

Risk Rating: Moderate Risk Finding

The contract between the County and Intermountain Medical Group (IMG), which manages the HealthyMe Clinic, did not include provisions regarding compliance with Countywide Policy 1400-7, "Payment Card Industry Data Security Standard Policy" and the PCI-DSS by the September 30th compliance deadline.

Countywide Policy 1400-7, "Payment Card Industry Data Security Standard Policy," Section 3.3, states,

"3.3.1 County agencies that establish agreements with outsourced contractors will ensure that written agreements include requirements for compliance with this policy and with PCI-DSS standards." 3.3.2 "County agencies that establish agreements with onsite contractors will ensure that written agreements include requirements for PCI-DSS compliance."

Additionally, Section 5.0., states:

"County agencies that collect payment card revenue on behalf of the County will demonstrate their compliance with PCI-DSS annually to the County Auditor by September 30th. County agencies found to be non-compliant will have a 6-month grace period to become compliant."

We found that the contract with Intermountain Medical Group, which manages the HealthyMe Clinic, did not include language regarding compliance with Countywide Policy 1400-7 and Payment Card Industry Data Security Standards. We communicated with the District Attorney's office and the Director of the Human Resources Division on March 16, 2022, that an addendum should be drafted to include the language required in Countywide Policy 1400-7. Regular communication on addendum updates were made throughout the audit period.

The updated addendum was sent to IMG for signatures on September 12, 2022. Unfortunately, they were unable to have the necessary parties sign the addendum by the Countywide PCI compliance deadline of September 30.

We want to emphasize that this finding did not have an impact on IMG providing the necessary AOC form by the September 30th deadline, which they complied with.

There is an increased risk that outsourced and onsite contractors are not aware of, and adhere to, Countywide Policy 1400-7 and PCI DSS unless there is a written agreement established between the two parties. The

County could be placed at an increased risk of litigation if there were to be a breach in payment card security.

IMG was unable to have the necessary parties sign the addendum by the Countywide PCI compliance deadline of September 30 due to the primary signatory being out of the office.

1.1	RECOMMENDATION	Contract Dates

We recommend an addendum be drafted for the contract between Intermountain Medical Group and the County. The addendum should include compliance with Countywide Policy 1400-7 and Payment Card Industry Data Security Standards.

AGENCY RESPONSE:

Management resolved this finding by providing the signed addendum of both parties on October 4, 2022.

APPENDIX A: PCI DSS SAQ Types and Descriptions

PCI DSS Self-Assessment Questionnaire Types and Descriptions	
SAQ Type	**Description**
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. ***Not applicable to face-to-face channels.***
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data, but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises. ***Applicable only to e-commerce channels.***
B	Merchants using only imprint machines with no electronic cardholder data storage, and/or standalone, dial-out terminals with no electronic cardholder data storage. ***Not applicable to e-commerce channels.***
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. ***Not applicable to e-commerce channels.***
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. ***Not applicable to e-commerce channels.***
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. ***Not applicable to e-commerce channels.***
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed Point-to-Point Encryption (P2PE) solution, with no electronic cardholder data storage. ***Not applicable to e-commerce merchants.***
D	All merchants not included in descriptions for the above SAQ types.

Source: PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard, version 3.2.1.

APPENDIX B: County Agencies – 2021 Payment Card Revenues

County Agencies - 2021 Payment Card Revenues & Transactions			
Agency	**Payment Card Revenue**	**Number of Payment Card Transactions**	**Category**
Aging and Adult Services	$129,134	2,608	Human Services
Animal Services	$690,691	16,164	Public Works
Archives	$1,609	80	Other Services
Arts & Culture	$17,817,001	68,423	Community Services
Assessor's Office	$2,166,947	6,714	Property Taxes
Clerk's Office	$797,704	18,838	Other Services
Criminal Justice Services	$89,704	1,940	Human Services
District Attorney ①	N/A	N/A	Community Services
Engineering and Flood Control	$28,782	131	Public Works
Health Department	$3,450,392	30,753	Human Services
HealthyMe Clinic SL Gov. Center	$24,530	976	Other Services
Justice Courts	$1,009,169	6,909	Other Services
Library Services	$480,938	55,239	Community Services
Parks and Recreation Centers	$10,233,935	332,808	Community Services
Parks and Recreation Golf Courses	$9,281,749	198,114	Community Services
Planetarium	$1,666,650	66,133	Community Services
Recorder's Office	$165,261	2,702	Other Services
SMG - Equestrian Park ②	N/A	N/A	Community Services
SMG - Mountain America Expo Center ②	$286,634	8,440	Community Services
SMG - Salt Palace Convention Center ②	$542,093	17,922	Community Services
Solid Waste Management	$5,419,770	165,182	Public Works
Surveyor's Office	$119,662	465	Other Services
Treasurer's Office	$22,416,187	8,096	Property Taxes
USU Extension Services ③	N/A	N/A	Other Services
Total 2021 Payment Card Revenues ④	**$76,818,541**	**1,008,637**	

Source: Data compiled through surveys of County Agencies' and data provided by payment processors. County agency payment processors include Chase Paymentech, Official Payments Corporation/ACI Worldwide, Square-up, Heartland, and PayPal.

①District Attorney did not collect payments in 2021 but did collect payment card revenue in 2022.

②SMG is an outsourced contractor. AOC Form was required. The Equestrian Park is no longer part of the County due to sale to Utah State University in 2021.

③USU Extension services does not collect payment card revenue on behalf of the County but is located within the County Government Center and has access to the County network, required to provide AOC form.