COMPLIANCE REVIEW

Salt Lake County
PCI DATA SECURITY STANDARDS

MAY 2024

Chris Harding, CPA, CFE, CIA
County Auditor

Office of the Auditor
Salt Lake County

Audit Team

Audra Bylund, Audit Manager
Chris Scott, Internal Auditor

Audit Management

Chris Harding, CPA, CFE, CIA, County Auditor
Richard Jaussi, MBA, Chief Deputy Auditor
Roswell Rogers, Senior Advisor
Shawna Ahlborn, Audit Division Director

Audit Committee

Marty Van Wagoner, CPA, MBA

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

May 2024

I am pleased to present the results of our Payment Card Industry Data Security Standard ("PCI DSS") compliance review of Salt Lake County organizations for the period of October 1, 2022, to September 30, 2023. This compliance review was aimed at evaluating whether all county entities and outsourced contractors that accept payment cards met the PCI DSS compliance validation requirements during 2023, as required by Salt Lake County Countywide Policy 1400-7: Payment Card Industry Data Security Standard.

The compliance review we conducted revealed some county and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2023, submitted the Self-Assessment Questionnaire (SAQ) and/or Attestation of Compliance (AOC) form after the September 30th deadline, as required by Countywide Policy 1400-7. It highlighted how some county and non-county entities submitted SAQ and AOC forms with inconsistencies in responses or that had the absence of a wet or digital signature from an authorized employee. The report also noted that the county agency, Criminal Justice Services, no longer processes, stores, or receives payment card information, and is consequently no longer required to complete the forms annually.

We strongly recommend that management designate a primary and secondary employee responsible for completing and submitting the applicable SAQ and AOC forms by the annual September 30th deadline. We recommend that management implement a review process for completing the SAQ and AOC to ensure that the responses are consistent between forms, all questions and additional required forms are complete to the best of their knowledge, and a signature is present under Merchant Attestation by an authorized employee. Addressing these issues is crucial to safeguarding payment card information and remaining in compliance with PCI-DSS and Countywide Policy 1400-7.

This compliance review was authorized under Utah Code Title 17, Chapter 19a, "County Auditor", Part 2, "Powers and Duties." We conducted this review in accordance with generally accepted government auditing standards (GAGAS) for performing non-audit services. While designated as a compliance review, we followed the general principles of GAGAS in performing the procedures outlined. These procedures were designed to offer reasonable assurance regarding the reliability, completeness, and adherence to Countywide Policy 1400-7 of the information presented in the County's PCI DSS compliance documentation.

We appreciate the cooperation and assistance provided by the county and non-county entities and their staff during this process. For further information or clarification regarding this report, please feel free to contact me at 385-468-7200.

Chris Harding, CPA, CFE, CIA
Salt Lake County Auditor

Contents

RISK CLASSIFICATIONS 2

BACKGROUND 3

OBJECTIVES AND SCOPE 7

CRITERIA 7

METHODOLOGY 7

CONCLUSIONS 8

RESULTS 8

FINDING 1: AGENCIES SUBMITTED THE PCI DSS FORMS AFTER THE SEPTEMBER 30TH COUNTY DEADLINE 12

FINDING 2: INCONSISTENCIES BETWEEN SAQ AND AOC FORMS BY THREE AGENCIES 14

APPENDIX A 17

APPENDIX B 18

REPORT HIGHLIGHTS

PCI DATA SECURITY STANDARDS

MAY 2024

Objectives

Our overall compliance review objective was to determine whether all county entities and outsourced contractors that accept payment cards met the PCI DSS compliance validation requirements during 2023, as required by Countywide Policy 1400-7. The specific compliance review objectives were to:

- Determine if each County agency demonstrates PCI DSS compliance by submitting a completed SAQ and AOC for 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.
- Collect and review each agency's annual number of payment card transactions and dollar amount.

Agencies complied with County deadline, submitted forms prior to September 30th Deadline

15 of the 21 County and non-county entities that were required to demonstrate their compliance with the Payment Card Industry Data Security Standards ("PCI-DSS") in 2023, did so by the September 30th deadline.

Agencies Submitted the PCI DSS forms After the September 30th County Deadline

Six of the 21 County and non-county entities that were required to demonstrate their compliance with the Payment Card Industry Data Security Standards ("PCI-DSS") in 2023, submitted the forms after the September 30th deadline.

Inconsistencies between SAQ and AOC forms by Three Agencies

We found three agencies had either inconsistencies or absence of a wet or digital signature in the submitted SAQ and AOC forms. For example, one agency's response entered on the "Summary of Assessment" portion identified one requirement as not applicable, "N/A". However, the questionnaire responses were marked as "In Place" on the SAQ Form. Another agency submitted completed SAQ and AOC forms but did not sign the "Signature of Merchant Executive Officer" line.

One County agency stopped processing payment cards

Criminal Justice Services no longer processes, stores, or receives payment card information, and therefore is not required to complete SAQ and AOC forms annually for County PCI Compliance.

Chris Harding, CPA, CFE, CIA **Salt Lake County Auditor**

Finding Risk Classifications

Classification	Description
1 – Low Risk Finding	Low risk findings may have an effect on providing reasonable assurance that County entities and service contractors that process payment card revenue met PCI DSS compliance validation requirements per Salt Lake County Countywide Policy 1400-7. Recommendations may or may not be given to address the issues identified in the final compliance review report. If recommendations are given, management should try to implement the recommendations within one year of the final compliance review report date if possible. Follow-up compliance review 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 County entities and service contractors that process payment card revenue met PCI DSS compliance validation requirements per Salt Lake County Countywide Policy 1400-7. Recommendations will be given to address the issues identified in the final compliance review report. Management should implement the recommendations within one year of the final compliance review report date if possible. Follow-up compliance reviews will focus on the status of implementation.
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 County entities and service contractors that process payment card revenue met PCI DSS compliance validation requirements per Salt Lake County Countywide Policy 1400-7. Recommendations will include necessary corrective actions that address the significant risks identified in the final compliance report. Management should implement the recommendations within six months of the final compliance review report date if possible. Follow-up compliance reviews 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 County entities and service contractors that process payment card revenue met PCI DSS compliance validation requirements per Salt Lake County Countywide Policy 1400-7. Recommendations will include necessary corrective actions that address the critical risks identified in the final compliance review report. Management should implement the recommendations as soon as possible. Follow-up compliance reviews 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 2022, County agencies processed more than 1.2 million payment card transactions totaling over $102 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 over $102 million in payment card transactions during 2022, up from over $76 million in 2021.

Overall, 2022 payment card revenue increased by 33% from 2021. Community Services revenue increased 40% from 2021 revenue amounts. Public Works revenue increased 12% from 2021. When compared to the pre-pandemic revenue from 2019, revenue increased 26%.

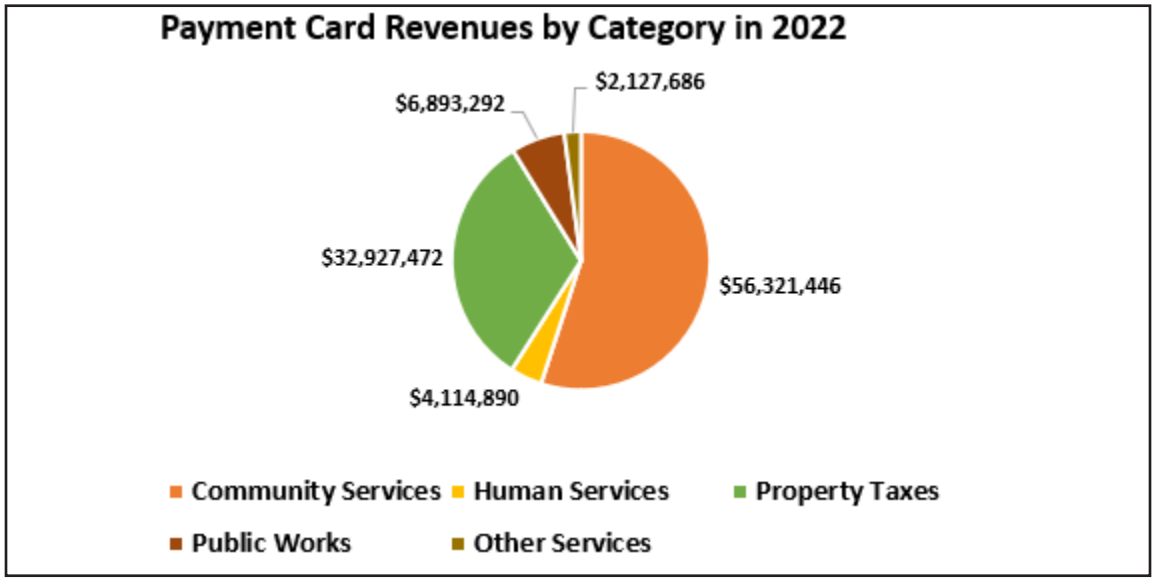
The County Treasurer sets up and manages merchant accounts for County agencies that accept payment cards. Payment card transactions are processed through a major payment card merchant bank. In some cases, payment card transactions are processed through a third-party vendor, on-behalf of County agencies, through an outsourcing agreement. Online property tax payments by credit or debit card are an example of outsourced payment card processing that is done on behalf of the County by a third-party processor through an online portal.

For the purposes of this compliance review, 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 2022, is shown in Figure 1.

Figure 1. County Payment Card Revenues by Category in 2022. Overall, there was a 33% increase in payment card revenue in 2022, indicating an increase of 26% of overall revenue from 2019 (Pre-Pandemic).



Source: Data compiled via payment card data requests from County agencies and data provided by payment card processors. County agency payment card processors include Chase Paymentech, Official Payments Corporation/ACI Worldwide, Square-up, and Heartland.

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. Note: v3.2.1 will retire March 2024 and v4.0 will be in effect.

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 records containing personally identifiable information (PII): financial, or medical account details, or other secret, confidential or proprietary data are potentially put at risk. These records can be in electronic or paper format."*

In 2023, Ponemon estimated the global per record cost of a data breach at $165, an increase from the 2022 estimate of $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 reveals confidential or proprietary corporate, governmental or financial data, or identifies an 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 PII, or a health record with the policyholder's name and payment information."*

1 Benchmark research sponsored by IBM Security, study conducted by Ponemon Institute, LLC, 2023 Cost of a Data Breach Report.

Some of the negative effects of a data breach involving cardholder data according to the PCI SSC[1] include:

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

The Ponemon study found that data breaches cost the public sector $2.6 million in 2023. The 2023 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 2023 on average was phishing at $4.76 million.

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 attack vectors from 2022 to 2023.*

Attack Vector	Percent of breaches	Average total Costs in millions	Ranking by percent 2023	Ranking by percent 2022
Compromised Credentials	15%	$4.62	3	1
Phishing	16%	$4.76	2	2
Cloud misconfiguration	11%	$4.00	4	3
Vulnerability in 3rd party software	17%	$8.62	1	4

Note: The 2023 Data Breach Report categorized software vulnerabilities into two categories: Known unpatched vulnerability and Unknown (zero-day vulnerability). In 2023, Known patched vulnerabilities total $4.17 million (6%) and Unknown patched vulnerabilities total $4.45 million (11%) for total vulnerability in 3rd party software of $8.62 million.

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.

1 https://east.pcisecuritystandards.org/pci_security/why_security_matters, website visited January 31, 2024

OBJECTIVES AND SCOPE

Our overall compliance review objective was to determine whether all county entities and outsourced contractors that accept payment cards met the PCI DSS compliance validation requirements during 2023, as required by Countywide Policy 1400-7. The specific compliance review objectives were to:

- Determine if each County agency demonstrates PCI DSS compliance by submitting a completed SAQ and AOC for 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.
- Collect and review each agency's annual number of payment card transactions and dollar amount.

The compliance review scope was October 1, 2022 – September 30, 2023.

CRITERIA

County agencies that accept payment cards must demonstrate compliance with the PCI DSS annually. Salt Lake County 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."

METHODOLOGY

To accomplish the compliance review objectives, we:

- Notified County agencies of procedures for annually validating PCI DSS compliance to the Auditor's Office and instructions for completing and submitting the forms.
- Reviewed all 2023 SAQs and AOCs submitted to the Auditor's Office 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.

CONCLUSION

We found that 15 out of 21 (71%) County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2023, did so by the September 30th deadline. However, six out of 21 (28%) County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2023, did not do so by the September 30th deadline. We noted that two agencies had inconsistencies in their responses between the SAQ and AOC submitted to the Auditor's Office. One agency submitted the forms without a wet or digital signature. The remaining 18 agencies submitted SAQs and AOCs that were complete, accurate, and signed by an appropriate level of organizational authority.

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 compliance review focused on validating completion of the 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 complete and accurate based on their understanding of their 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 notified all fiscal managers Countywide to submit their SAQ and AOC forms if they process payment card data. 18 County, and three non-county entities, submitted an annual SAQ and/or AOC to demonstrate their compliance with the PCI DSS in 2023. 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 2023. *The number of County agencies required to provide an annual SAQ and AOC to the Auditor's Office was 18 in 2023. Three non-county entities were required to provide only their annual AOC to comply with Countywide Policy 1400-7.*

Changes to PCI DSS Compliance Validation Requirements in 2023			
County Entity	Required Documentation 2023	Required Documentation 2022	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	N/A	SAQ & AOC	*No longer processes payment cards as of 1/1/2023*
District Attorney	SAQ & AOC	N/A	*Processed payment card transactions*
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*
ASM Global (Salt Palace, Mountain America Expo)	AOC	AOC	*No Change*
USU Extension Services	AOC	AOC	*No Change*

**ASM Global, formerly SMG, manages the two County owned venue properties.*

We found that 18 county entities did demonstrate their compliance with the PCI DSS. However, four out of 18 (22%) county entities submitted the required SAQ and AOC forms after the September 30th deadline. Additionally, two out of three (66%) outsourced contractors submitted the required AOC forms after the County deadline. Missing the County deadline does not impact PCI compliance but fails to meet the Countywide compliance deadline. We reviewed that each County agency's SAQ and AOC was completed correctly and accurately to the best of their knowledge and based on their understanding of their payment card processing environments.

Table 4. Entity – SAQ Type(s) – 2023 Completion Dates. . *All County and non-county entities that were required to demonstrate compliance with the PCI DSS, completed an SAQ and/ or AOC.*

Entity – SAQ Type(s) – 2023 Completion Dates		
County Agency	**2023 SAQ Type(s)**	**2023 Submission Date**
Aging and Adult Services	C	09/25/2023
Animal Services	C	09/07/2023
Archives	A	10/24/2023
Arts and Culture	C	09/23/2023
Assessor	A	09/26/2023
Clerk	B-IP	08/21/2023
Criminal Justice Services	N/A	No longer processes payment cards
District Attorney	A	09/28/2023
Engineering and Flood Control	C-VT	09/22/2023
Health Department	B-IP	09/29/2023
HealthyMe Clinic SL Gov. Center	D	09/27/2023
Justice Courts	C	10/12/2023
Library Services	B-IP	01/18/2024
Parks and Recreation – Golf	C	09/25/2023
Parks and Recreation Centers	C	09/25/2023
Planetarium	C	09/28/2023
Recorder	C	10/04/2023
ASM Global - 2 venues	C	10/05/2023
Solid Waste Management	C	09/29/2023
Surveyor	C-VT	08/14/2023
Treasurer	C-VT	09/27/2023
USU Extension Services	B-IP	10/11/2023

We found that all County agencies and two outsourced contractors remained the same SAQ types in 2023 as they were in 2022. The third outsourced contractor, USU Extension, changed their AOC type from D to B-IP in 2023. The District Attorney's Office was required to complete both SAQ and AOC forms for 2023 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 Contrac tors." (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 (electroni cally 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 compliance review, 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 Attestation of Compliance (AOC) form to the Auditor by September 30th.

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

- ASM Global, formerly Spectator Management Group ("SMG") provides professional management services for two County-owned facilities including: the Calvin L. Rampton Salt Palace Convention Center and the Mountain America Exposition Center.
- 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 compliance review demonstrated their compliance with the PCI DSS by completing and submitting an AOC form. Intermountain submitted their AOC before the September 30th deadline to the Auditor for review, and USU Extension and ASM Global submitted theirs after the deadline.

FINDING 1 AND RECOMMENDATIONS

Agencies Submitted the PCI DSS forms After the September 30th County Deadline

Risk Rating: Low Risk Finding

In 2023, the Auditor's Office adjusted the procedures for agencies and outsourced contractors to submit PCI DSS forms. An email notification was sent Countywide to fiscal managers in May, August, and September outlining the submission process and who to contact for questions.

We found that four out of 18 (22%) County agencies, and two out of three (66%) contractors submitted the forms after the County deadline of September 30th.

Table 5. List of County agencies and outsourced contractors that submitted PCI DSS form after the County deadline.

Agency	Submission Date
Archives	10/24/2023
Justice Court	10/12/2023
Library	01/18/2024
Recorder	10/04/2023
Outsourced Contractor	**Submission Date**
ASM	10/05/2023
USU Extension	10/11/2023

Countywide Policy on Information Technology Security 1400-7: Payment Card Industry Data Security Standard, Part 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."

Late submissions were attributed to a combination of management oversight and staff turnover.

County agencies are required to submit their PCI forms annually by the County deadline. Failure to submit the forms and demonstrate PCI compliance annually places an increased risk on the County for compromised payment card data, which negatively impacts both County operations and reputation.

1.1	RECOMMENDATION	Reporting Procedures

We recommend that management designate a primary and secondary employee responsible for completing and submitting PCI DSS forms and submitting the applicable SAQ and AOC forms by the annual September 30th deadline.

County Agencies included:

- Archives
- Justice Court
- Library
- Recorder

FINDING 2 AND RECOMMENDATIONS

Inconsistencies between SAQ and AOC forms by Three Agencies

Risk Rating: Low Risk Finding

After agencies submit their SAQ and AOC forms, we complete a review of the forms to ensure that all questions and additional forms are completed. We compare the SAQ and AOC forms for consistency in the responses as well as verify that a digital or wet signature is present by the appropriate authorizing individual. If there is a lack of consistency in the responses or an absence of a signature, we will notify the primary contact who submitted the forms to make the updates.

Three agencies had inconsistencies or absence of a wet or digital signature in their SAQ and AOC forms. We found that:

- Animal Services did not provide accurate corrections to the Executive Summary on the SAQ and AOC forms after being notified to update responses to maintain consistency between the two forms. For instance, responses in the Summary of Assessment section identified one requirement as not applicable, "N/A". However, the questionnaire responses were marked as "In Place" on the SAQ Form.
- Aging and Adult Services identified one requirement as "N/A", but did not enter the explanation of requirements noted as not applicable in Appendix C of the SAQ form.
- Justice Court submitted complete forms, but the individual who completed them only typed their name and title position without providing a wet or digital signature in the "Signature of Merchant Executive Officer" required under the Merchant Attestation on the SAQ and AOC forms.

PCI DSS V4.0 SAQ, Part 2: Executive Summary, Part 2.g: Summary of Assessment states: "Indicate below all responses that were selected for each PCI DSS Requirement"

PCI DSS V3.2.1, SAQ, Appendix C: Explanation of Requirements Noted as Not Applicable states: "This Appendix must be completed for each requirement where Not Applicable was selected."

PCI DSS V4.0 SAQ, Part 3b: Merchant Attestation, includes: "Signature of Merchant Executive Officer"

E-mail communication requesting updates was sent to the primary contacts of each agency; however, the Auditor's Office did not receive the requested corrections.

SAQ and AOC form responses that are not consistent may impact the validity and compliance with PCI DSS. Absence of required signatures on the forms reduces the validity.

2.1	RECOMMENDATION	Alternative Designee

We recommend that management implement a review process for completing SAQ and AOC forms to ensure that the forms are:

- Consistent in responses between the SAQ and AOC
- All questions and additional forms are complete to the best of their knowledge.
- A signature is present under Merchant Attestation by an authorized employee.

County Agencies included:

- Animal Services
- Aging and Adult Services
- Justice Court

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
2022 Payment Card Revenues

County Agencies - 2022 Payment Card Revenues & Transactions			
Agency	**Payment Card Revenue**	**Number of Payment Card Transactions**	**Category**
Aging and Adult Services	$116,280	4,439	Human Services
Animal Services	$493,691	15,441	Public Works
Archives	$1,845	49	Other Services
Arts & Culture	$27,658,126	122,127	Community Services
Assessor's Office	$2,773,429	6,619	Property Taxes
Clerk's Office	$870,833	19,018	Other Services
Criminal Justice Services	$68,124	1,624	Human Services
District Attorney	$11,769	93	Community Services
Engineering and Flood Control	$66,297	159	Public Works
Health Department	$3,930,487	32,926	Human Services
HealthyMe Clinic SL Gov. Center	$24,660	971	Other Services
Justice Courts	$866,488	6,271	Other Services
Library Services	$567,970	38,849	Community Services
Parks and Recreation Centers	$13,793,082	407,206	Community Services
Parks and Recreation Golf Courses	$10,362,523	218,027	Community Services
Planetarium	$2,306,300	95,561	Community Services
Recorder's Office	$184,893	3,096	Other Services
ASM - Mountain America Expo Center	$245,159	4,004	Community Services
ASM - Salt Palace Convention Center	$1,388,287	76,157	Community Services
Solid Waste Management	$6,333,304	178,951	Public Works
Surveyor's Office	$167,198	426	Other Services
Treasurer's Office	$30,154,043	9,291	Property Taxes
USU Extension Services	n/a	n/a	Other Services
Total 2022 Payment Card Revenues	**$ 102,384,787**	**1,241,305**	

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.

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

2. ASM Global is an outsourced contractor. AOC Form was required.

3. USU 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.