A Report to the
Citizens of Salt Lake County
The County Mayor and the
County Council

An Audit of Salt Lake County's Compliance with the Payment Card Industry Data Security Standard

**Office of the
Salt Lake County
Auditor**

**Scott Tingley
County Auditor**

October 2021

An Audit of Salt Lake County's Compliance with the Payment Card Industry Data Security Standard

October 2021

Scott Tingley, CIA, CGAP
SALT LAKE COUNTY AUDITOR

Cherylann Johnson, MBA, CIA, CFE, CRMA
CHIEF DEPUTY AUDITOR

Shawna Ahlborn
AUDIT SERVICES DIVISION ADMINISTRATOR

AUDIT MANAGER
Brenda Nelson, CISA, PCIP

AUDIT STAFF
Audra Byland
Tammy Keller

OFFICE OF THE SALT LAKE COUNTY AUDITOR
AUDIT SERVICES DIVISION

OUR MISSION

To foster informed decision making, strengthen the internal control environment, and improve operational efficiency and effectiveness for Salt Lake County, through independent and objective audits, analysis, communication, and training.

SCOTT TINGLEY
CIA, CGAP
Salt Lake County Auditor
STingley@slco.org

CHERYLANN JOHNSON
MBA, CIA, CFE
Chief Deputy Auditor
CAJohnson@slco.org

ROSWELL ROGERS
Senior Advisor
RRogers@slco.org

STUART TSAI
JD, MPA
Property Tax
Division Administrator
STsai@slco.org

SHAWNA AHLBORN
Audit Services
Division Administrator
SAhlborn@slco.org

OFFICE OF THE
SALT LAKE COUNTY
AUDITOR
2001 S State Street, N3-300
PO Box 144575
Salt Lake City, UT 84114-4575

(385) 468-7200; TTY 711
1-866-498-4955 / fax

October 6, 2021

Honorable Members of the Salt Lake County Council,
Honorable Salt Lake County Mayor, and
The Citizens of Salt Lake County

Re: An Audit of Salt Lake County's Compliance with the Payment Card Industry Data Security Standard

The Salt Lake County Auditor's Office has completed an audit of Salt Lake County's compliance with the Payment Card Industry Data Security Standard. The overall objectve of the audit was to determine whether all County agencies that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2021.

The PCI DSS is a set of 12 requirements, created and maintained by the PCI Security Standard Council. The goal of the Standard and the requirements is to protect the public's cardholder data and to help decrease the likelihood of payment card fraud. Compliance with the standard is mandatory for any entity, public or private, that stores, processes, or transmits cardholder. In the event of a data breach, non-compliance with the DSS could lead to significant fines, fees, and legal liabilities for the County.

We truly appreciate the time and efforts of the employees of Salt Lake County and the Information Technology Division throughout the audit. Our work was made possible by their cooperation, assistance, and prompt attention given to our requests.

We will be happy to meet with any appropriate committees, council members, management, or advisors to discuss any item contained in the report for clarification or to better facilitate the implementation of the recommendations.

Respectfully submitted,

Scott Tingley

Scott Tingley, CIA, CGAP
Salt Lake County Auditor

Cc: K. Wayne Cushing, Salt Lake County Treasurer
Zachary Posner, Chief Information Officer, Salt Lake County
Mark Evans, Associate Director of Information Security, IT Division
Jon Daich, Director of Finance, SMG Property Management, Inc.

SALT LAKE
COUNTY

Audit Summary

Background and Purpose

Salt Lake County organizations accept credit and debit cards as a form of payment for a wide variety of goods and services provided to County residents and customers. In 2020, County agencies processed almost 750,000 payment card transactions totaling $49.8 million in revenue. County residents and customers can use payment cards to pay for many types of County fees and services including fitness and recreation center passes, theater tickets, youth sports registrations, library fines and fees, document recording fees, pet adoptions and licenses, 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.

The Payment Card Industry Data Security Standard is a set of 12 requirements, created and maintained by the PCI Security Standard Council. Compliance with the Standard and the requirements is mandatory for any entity, public or private, that stores, processes, or transmits cardholder data. The Standard requires organizations to build and maintain a secure network; encrypt and protect any 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 for the organization.

The purpose of the audit was to determine whether all County entities that accept payment cards and any outsourced contractors that process payment card transactions on behalf of the County, met the PCI DSS compliance validation requirements for 2021, as required by Countywide Policy 1400-7 Information Technology Security: Payment Card Industry Data Security Standard Policy.

What We Found

County Agencies Successfully Completed PCI DSS Compliance Validation Requirements

Our audit focused on determining the correct merchant level and Self-Assessment Questionnaire (SAQ) type for each County or non-county entity that was required to demonstrate their compliance with the PCI DSS. 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.

We found that all 18 County, and the 3 non-county entities that were required to demonstrate their compliance with the PCI DSS in 2021, did so by the September 30th deadline. We also verified that each County agency's SAQ and Attestation of Compliance form 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

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 Attestation of Compliance (AOC) form to the Auditor by September 30th each year.

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 three County-owned facilities including: the Calvin L. Rampton Salt Palace Convention. Center, the Mountain America Exposition Center, and the Salt Lake County Equestrian Park
- Healthy-Me Clinic managed by Intermountain Medical Group.
- USU Extension Services at 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 state of emergency, 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 2021. We found that these changes did not significantly affect any agency’s SAQ type or substantially change their PCI DSS compliance validation requirements.

Conclusion

We found that all 21 of the County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2021, 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. In addition, despite the ongoing Coronavirus pandemic in 2021, the County’s compliance validation efforts were timely, effective, and completed in accordance with Countywide policy and PCI DSS requirements.

Table of Contents

Background 1

Objectives 5

Scope and Methodology 5

Audit Results 5

County Agencies Successfully Completed PCI DSS Compliance Validation Requirements........ 5

Outsourced Contractors Demonstrated PCI DSS Compliance 7

The Coronavirus (COVID-19) Pandemic Continues to have Minimal Impact on PCI DSS Compliance Validation Requirements 8

Conclusion........ 9

Appendix A: PCI DSS SAQ Types and Descriptions........ 10

Appendix B: County Agencies – 2020 Payment Card Revenues 11

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 2020, County agencies processed almost 750,000 payment card transactions totaling $49.8 million in revenue. County residents and customers can use payment cards to pay for many types of County fees and services such as fitness and recreation center passes, theater tickets, youth sports registrations, library fines and fees, document recording fees, pet licenses, charitable 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.

Overall, there was a 39% decrease in payment card revenue during 2020, because of the closure of several County facilities and venues due to the ongoing COVID-19 pandemic. County payment card revenue shrunk from $81.5 million in 2019 to $49.8 million in 2020, a decrease of $31.7 million. The Department of Community Services was hit the hardest because of the closures and made up 95% ($30.1 million) of the revenue decrease. Community Services includes agencies such as Parks and Recreation, Library Services, and the Clark Planetarium, which were all shut down during portions of 2020.

County agencies processed $49.8 million in payment card transactions during 2020, down from $81.5 million in 2019.

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 web portal.

County agencies that accept payment cards must demonstrate compliance with the Payment Card Industry (PCI) Data Security Standard (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)*

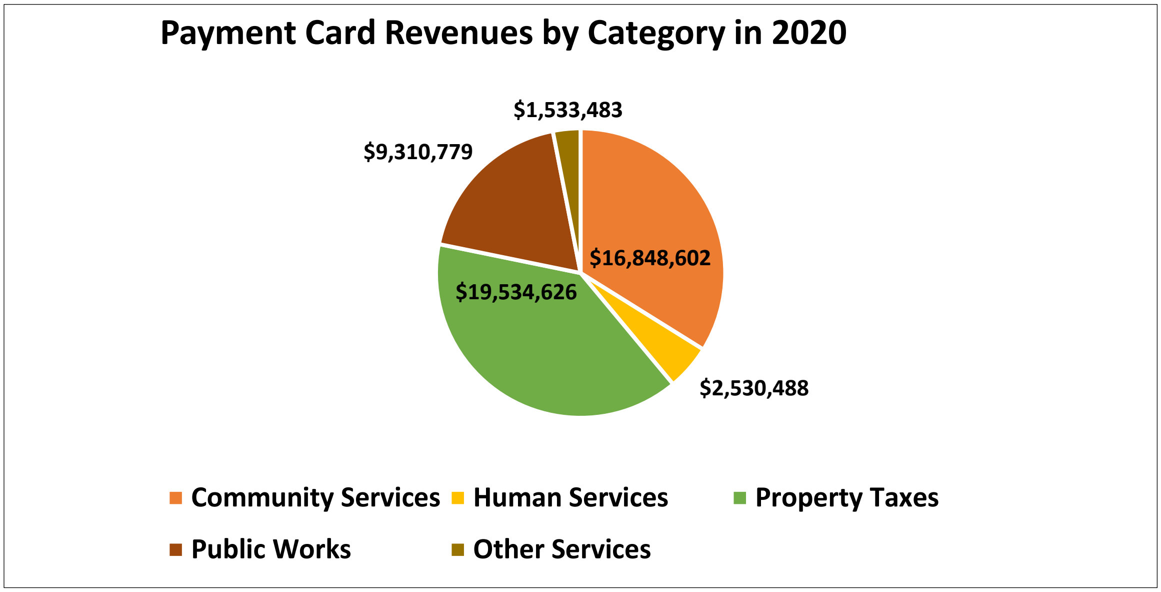
For the purposes of this audit, we categorized County payment card revenues into five major categories:

- 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 2020, is shown in Figure 1.

Figure 1. County Payment Card Revenues by Category in 2020. *Overall, there was a 39% decrease in payment card revenue in 2020 due to the Coronavirus pandemic. Unlike prior years, property tax was the largest payment card revenue source at $19.5 million (39%) followed by Community Services at $16.8 million (34%).*



Source: Data compiled through surveys of 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 Data Security Standard is a set of 12 requirements, created and maintained by the PCI Security Standard Council (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 help 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 and/or a financial record or debit card is potentially put at risk — either in electronic or paper format."*

In 2020, Ponemon estimated the cost of data breaches at $150 per record containing personally identifiable information (PII), which includes payment card data. In the 2021 report, Ponemon increased this estimate to $180 per record containing PII, a 20% increase over the prior year. The study concluded that data breach costs can be higher depending on the severity of the data breach, and the type of data that was compromised. The Ponemon study defines a compromised record as:

> *"Information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples include a database with an individual's name, credit card*

[1] *Benchmark research sponsored by IBM Security, study conducted by Ponemon Institute, LLC, 2021 Cost of a Data Breach Report.*

> *information and other personally identifiable information (PII) or a health record with the policyholder's name and payment information."*

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 further noted that:

> *"In 2021, the most frequent initial attack vectors were (1) compromised credentials, 20% of breaches (2) phishing, 17% (3) cloud misconfiguration, 15%. Business email compromise was responsible for only 4% of breaches but had the highest average total cost at $5.01 million. The second costliest initial attack vector was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million)."*

Table 2. Average total cost and frequency of data breaches of the top four attack vectors. *The top four types of successful attack vectors remained the same from 2020 to 2021. However, Phishing attacks moved up in ranking to the second highest type of successful data breach attack in 2021.*

Data Breach Attack Vector	Percent of Breaches	Average Total Cost (in millions)	Ranking 2021	Ranking 2020
Compromised Credentials	20%	$4.37	1	1
Phishing	17%	$4.65	2	4
Cloud Misconfiguration	15%	$3.86	3	2
Third Party Software Vulnerabilities	14%	$4.33	4	3

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

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

demonstrates their compliance with the PCI DSS at least annually and maintaining records of the compliance validation process.

Objectives

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 2021, 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 in 2021.

Scope and Methodology

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 2021 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 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 18 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 2021.

Table 3. PCI DSS Compliance Validation Requirements in 2021. *A total of 18 County agencies and 3 non-county entities that accept payment cards on behalf of the County were required to demonstrate their compliance with the PCI DSS in 2021.*

Changes to PCI DSS Compliance Validation Requirements in 2021			
	Required Documentation		
County Entity	2021	2020	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*
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	SAQ & AOC	*Clinic is managed by Intermountain Medical Group.*
SMG (Salt Palace, MA Expo, Equestrian Park)	AOC	AOC	*No Change*
USU Extension Services	AOC	AOC	*No Change*

We found that all 21 County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2021, did so by the September 30, 2021, deadline. We also 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) – 2021 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 September 30, 2021 deadline.*

Entity – SAQ Type(s) – 2021 Completion Dates		
County Agency	**2021 SAQ Type(s)**	**2021 Completion Date**
Aging and Adult Services	C	4/20/2021
Animal Services	C	5/20/2021
Archives	A	3/31/2021
Arts and Culture	C	8/20/2021
Assessor	A	5/25/2021
Clerk	B-IP	4/7/2021
Criminal Justice Services	B-IP	7/19/2021
Engineering and Flood Control	C-VT	7/12/2021
Health Department	B-IP	5/28/2021
HealthyMe Clinic SL Gov. Center	D	8/4/2021
Justice Courts	C	8/9/2021
Library Services	B-IP	8/4/2021
Parks and Recreation – Golf	C	7/29/2021
Parks and Recreation Centers	C	8/23/2021
Planetarium	C	5/10/2021
Recorder	C	6/4/2021
SMG - 3 venues	C	5/21/2021
Solid Waste Management	C	9/8/2021
Surveyor	C-VT	4/26/2021
Treasurer	C-VT	7/27/2021
USU Extension Services	B-IP	7/1/2021

In 2021, we found that Solid Waste Management changed SAQ types from B-IP to C. This change was due to their implementation of an additional payment method in the form of an online bill pay system that allows customers to pay using a computer or personal device. Additionally, we requested only an AOC from the HealthyMe Clinic, instead of an SAQ and AOC. We did so since the clinic is managed by Intermountain Medical Group (IMG), but accepts revenue on behalf of the County, and we anticipated that IMG completed their own annual compliance assessment.

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 three County-owned facilities including: the Calvin L. Rampton Salt Palace Convention Center, the Mountain America Exposition Center, and the Salt Lake County Equestrian Park.
- 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.

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

Due to the Coronavirus pandemic state of emergency, 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 2021. Even though some of these changes and modifications to operations were significant for some County agencies, we found that the changes did not significantly affect any agency's SAQ type or substantially alter 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 21 of the County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2021, 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. In addition, despite the ongoing Coronavirus pandemic in 2021, the County's compliance validation efforts were timely, effective, and completed in accordance with Countywide policy and PCI DSS requirements.

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 – 2020 Payment Card Revenues

County Agencies – 2020 Payment Card Revenues & Transactions			
Agency	**Total Payment Card Revenue**	**Total Number of Payment Card Transactions**	**Category**
Aging and Adult Services	$86,532	2,054	Human Services
Animal Services	$446,101	11,543	Public Works
Archives	$998	76	Other Services
Arts & Culture	$1,806,784	9,795	Community Services
Assessor's Office	$2,281,294	6,569	Property Taxes
Clerk's Office	$476,335	11,495	Other Services
Criminal Justice Services	$80,856	1,434	Human Services
Engineering and Flood Control	$40,423	185	Public Works
Health Department	$2,363,100	20,229	Human Services
HealthyMe Clinic SL Gov. Center ①	$21,450	828	Other Services
Justice Courts	$792,354	5,913	Other Services
Library Services	$312,582	32,938	Community Services
Parks and Recreation Centers	$5,076,472	233,609	Community Services
Parks and Recreation Golf Courses	$8,143,454	176,995	Community Services
Planetarium	$693,436	30,318	Community Services
Recorder's Office	$158,055	2,893	Other Services
SMG - Equestrian Park ①	$150,608	737	Community Services
SMG - Mountain America Expo Center ①	$400,558	15,270	Community Services
SMG - Salt Palace Convention Center ①	$264,708	9,869	Community Services
Solid Waste Management	$8,824,255	167,192	Public Works
Surveyor's Office	$84,291	441	Other Services
Treasurer's Office	$17,253,332	6,640	Property Taxes
USU Extension Services ①	N/A	N/A	Other Services
Total 2020 Payment Card Revenues ②	**$49,757,977**	**747,023**	

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, and Heartland.

① Non-county entities required to provide only their annual AOC to comply with Countywide Policy 1400-7
② COVID effect on total revenue: Overall there was a 39% decrease in revenue in 2020. Community Services accounted for 95% of this decrease in revenue with a 64% reduction from 2019 to 2020.