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

November 2020

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

November 9, 2020

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 2020.

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.

By its nature, this report focuses on issues, exceptions, findings, and recommendations for improvement. The focus should not be understood to mean that we did not find various strengths and accomplishments. 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, CIA, CGAP
Salt Lake County Auditor

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

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 2019, County agencies processed almost 1.1 million payment card transactions totaling $81,549,487 in revenues. 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.

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 outsourced contractors that process payment card transactions on behalf of the County, met the PCI DSS compliance validation requirements during 2020, 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 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 21 County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2020, did so by the September 30, 2020 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 annual Attestation of Compliance 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 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. While not required to do so, the Healthy-Me Clinic also provided a copy of their completed SAQ to the Auditor as well.

The Coronavirus (COVID-19) Pandemic Did Not Have a Significant Impact on PCI DSS Compliance Validation Requirements

The nationwide emergency declaration on March 13, 2020 due to the outbreak of the COVID-19 Coronavirus resulted in the closure of most County facilities. Payment card processing procedures throughout County facilities had to be modified to ensure continuity of operations, while at the same time adhering to local and state public health orders. These modifications emphasized minimizing or eliminating in-person payment card transactions and implementing contactless payment procedures, such as customer-only contact with payment card readers, and over-the-phone or online payment options.

We found that although some of the changes did have an impact on the way that County employees completed payment card transactions, specifically with the implementation of contactless payment procedures, these changes did not significantly affect each agency's Self-Assessment Questionnaire type or substantially change their PCI DSS compliance validation requirements. County employees should be commended for adapting to these changes quickly, while ensuring 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 or non-county entities that were required to demonstrate their compliance with the PCI DSS in 2020, 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, a contract amendment was adopted for the three County venues managed by SMG, that requires SMG to adhere to Countywide Policy 1400-7 and the PCI DSS compliance validation requirements. Despite the many challenges that County agencies faced during the COVID-19 Coronavirus pandemic in 2020, the County's compliance validation efforts were timely, effective, and completed in accordance with Countywide policy and PCI DSS requirements.

Table of Contents

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 2019, County agencies processed almost 1.1 million payment card transactions totaling $81,549,487 in revenues. 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 $81,549,487 in payment card transactions during 2019.

The County Treasurer sets up and manages merchant accounts for County agencies that require the ability to accept payment cards, and 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.

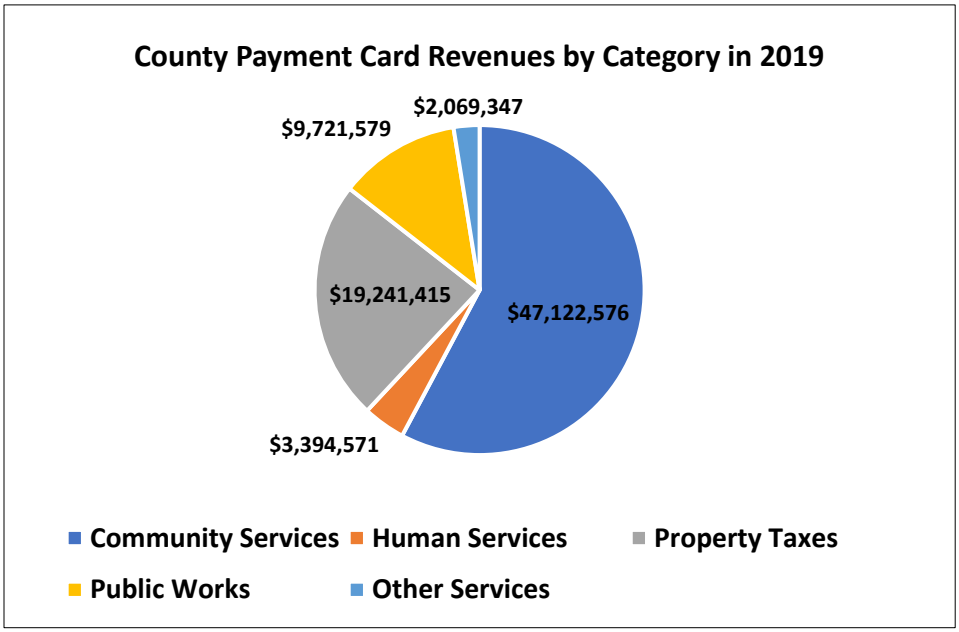
County agencies that accept payment cards must demonstrate compliance with the PCI DSS annually. Countywide Policy 1400-7, "Information Technology Security-Payment Card Industry Data Security Standard Policy," Section 5.0, Enforcement, states:

> *"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)*

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

Figure 1. County Payment Card Revenues by Category in 2019. *Community Services, which includes items such as fitness and recreation center passes, youth sports registrations, planetarium dome theater tickets, and library fines and fees, made up approximately 58% of the County's total payment card transaction revenue in 2019.*



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, Heartland, and PayPal.

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 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.

Figure 2. 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 and Systems	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. Protect all systems against malware 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. Identify and authenticate access to system components. 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."*

The Ponemon study also estimates the cost of each compromised record involving personally identifiable information ("PII"), including payment card information, at $150 per record, per incident. 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, 2020 Cost of a Data Breach Report.*

> *information and other personally identifiable information 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,

> *"Overall, malicious attacks registered as the most frequent root cause [of data breaches] (52% of breaches in the study), versus human error (23%) or system glitches (25%), at an average total cost of $4.27 million [per data breach incident]."*

The study indicated that the primary mitigating factors to data breach costs included cybersecurity insurance, having a data breach incident response team that knows what to do in the event of a breach, and ensuring that a chief information security officer (or "CISO") is involved in setting cybersecurity policy and IT decision making.

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.

[2] https://www.pcisecuritystandards.org/pci_security/why_security_matters, September 23, 2020.

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 2020, 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.
- Evaluate the impact of the Coronavirus (COVID-19) pandemic on the County's payment card processing environment and determine if it changed or significantly affected any County agency's PCI DSS compliance validation requirements in 2020.

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 2020 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 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. 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 agencies before we were able to determine if all areas of the forms were completed correctly.

In 2019, we identified a total of 25 County or non-county entities that were required to submit an annual SAQ and AOC to demonstrate their compliance with the PCI DSS. Due to organizational changes and changes to County policy requirements, we determined that there was a total of 18 County agencies and three non-county entities that were required to demonstrate their compliance in 2020.

Table 1. Changes to PCI DSS Compliance Validation Requirements in 2020. *Due to organizational and County policy changes, the number of County agencies required to provide an annual SAQ and AOC to the Auditor's Office was 18 in 2020. 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 2020			
County Entity	**Required Documentation**		**Explanation**
	2020	**2019**	
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*
Mayor's Financial Administration	N/A	SAQ & AOC	*No payment card transactions in 2020*
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*
Planning and Development	N/A	SAQ & AOC	*No longer a County entity in 2020*
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*

Non-County Entities Required to Submit an AOC			
Healthy-Me Clinic	AOC	SAQ & AOC	*Policy Change – Outsourced Contractor Requirements*
SMG (Salt Palace, MA Expo, Equestrian Park)	AOC	SAQ & AOC	*Policy Change – Outsourced Contractor Requirements*
USU Extension Services	AOC	SAQ & AOC	*Policy Change – Outsourced Contractor Requirements*
Wasatch Front Waste and Recycling	N/A	SAQ & AOC	*No longer in scope*

We found that all 21 County and non-county entities that were required to demonstrate their compliance with the PCI DSS in 2020, did so by the September 30, 2020 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 2. Entity – SAQ Type(s) – 2020 Completion Dates. *All twenty-one County or non-county entities agencies that were required to demonstrate their compliance with the PCI DSS, completed an SAQ and/ or AOC by the annual September 30 deadline.*

Entity – SAQ Type(s) – 2020 Completion Dates		
County Agency	**2020 SAQ Type(s)**	**2020 Completion Date**
Aging and Adult Services	C	May 20
Animal Services	C	July 13
Archives	A	June 3
Arts & Culture	C	July 23
Assessor's Office	A	July 1
Clerk's Office	B-IP	July 13
Criminal Justice Services	B-IP	June 26
Engineering and Flood Control	C-VT	July 10
Health Department	B-IP	July 9
Healthy-Me Clinic	B	June 26
Justice Court	C	August 5
Library Services	B-IP	August 5
Parks and Recreation Centers	C	July 14
Parks and Recreation Golf Courses	C	July 14
Planetarium	C	June 1
Recorder's Office	C	June 17
SMG (Salt Palace, MA Expo, Equestrian)	C	May 19
Solid Waste Management	B-IP	September 8
Surveyor's Office	C-VT	June 10
Treasurer's Office	C-VT	June 29
USU Extension Services	B-IP	May 29

Outsourced Contractors Demonstrated PCI DSS Compliance

On August 4, 2020, the Salt Lake County Council ratified amendments to Countywide Policy 1400-7, "Information Technology Security: Payment Card Industry Data Security Standard Policy." The amendments greatly enhanced the effectiveness of ensuring that cardholder data handled by on-site contractors and service providers on behalf of the County is safe and secure. These policy updates included:

1. Clarifying the scope of the policy.
2. Requiring that contracts with vendors that process payment card transactions or collect payment card revenue on behalf of the County demonstrate their compliance with the PCI DSS at least annually.
3. Requiring that all contract agreements with outsourced service providers or on-site contractors that handle cardholder data on behalf of the County, include mandatory compliance with Countywide Policy 1400-7, and the PCI DSS.
4. Clarifying a County agency's responsibilities when outsourcing or engaging with onsite contractors, to ensure that the contractor or service provider complies with Countywide Policy 1400-7 and the PCI DSS.

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 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:

- 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. While not required to do so, the Healthy-Me Clinic also provided a copy of their completed SAQ to the Auditor as well.

The Coronavirus (COVID-19) Pandemic Did Not Have a Significant Impact on PCI DSS Compliance Validation Requirements

The nationwide emergency declaration on March 13, 2020 due to the outbreak of the COVID-19 Coronavirus resulted in the closure of most County facilities. Payment card processing procedures throughout County facilities had to be modified to ensure continuity of operations, while at the same time adhering to local and state public health orders. These modifications emphasized minimizing or eliminating in-person payment card transactions and implementing 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 although some of the changes did have an impact on the way that County employees completed payment card transactions, specifically with the implementation of contactless payment procedures, these changes did not significantly affect each agency's Self-Assessment Questionnaire type or substantially change their PCI DSS compliance validation requirements. County employees should be commended for adapting to these changes quickly, while ensuring 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 or non-county entities that were required to demonstrate their compliance with the PCI DSS in 2020, 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, a contract amendment was adopted for the three County venues managed by SMG, that requires SMG to adhere to Countywide Policy 1400-7, "Information Technology Security: Payment Card Industry Data Security Standard Policy," and the PCI DSS compliance validation requirements. Despite the many challenges that County agencies faced during the COVID-19 Coronavirus pandemic in 2020, 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 – 2019 Payment Card Revenues

County Agencies – 2019 Payment Card Revenues & Transactions			
Agency	**Payment Card Revenue 2019**	**Number of Payment Card Transactions 2019**	**Category**
Aging and Adult Services	$ 67,030	2,560	Human Services
Animal Services	$ 626,325	14,523	Public Works
Archives	$ 2,187	140	Other Services
Arts & Culture	$ 20,679,995	103,568	Community Services
Assessor's Office	$ 1,996,876	5,988	Property Taxes
Clerk's Office	$ 807,672	17,730	Other Services
Criminal Justice Services	$ 260,098	4,304	Human Services
Engineering and Flood Control	$ 49,171	183	Public Works
Health Department	$ 3,067,443	30,858	Human Services
Healthy-Me Clinic (SLCo Gov. Center)	$ 44,270	1,721	Other Services
Justice Courts	$ 975,545	7,554	Other Services
Library Services	$ 880,111	94,968	Community Services
Mayor's Financial Administration ①	$ 2,040	24	Other Services
Parks and Recreation Centers	$ 15,754,170	345,689	Community Services
Parks and Recreation Golf Courses	$ 6,400,400	165,781	Community Services
Planetarium	$ 1,746,090	79,606	Community Services
Planning and Development ②	$ 348,377	1,081	Public Works
Recorder's Office	$ 161,833	4,228	Other Services
SMG - Equestrian Park	$ 212,049	803	Community Services
SMG - Mountain America Expo Center	$ 963,101	29,109	Community Services
SMG - Salt Palace Convention Center	$ 486,657	18,250	Community Services
Solid Waste Management	$ 8,697,705	117,673	Public Works
Surveyor's Office	$ 75,799	311	Other Services
Treasurer's Office	$ 17,244,538	6,267	Property Taxes
Total 2019 Payment Card Revenues	**$ 81,549,487**	**1,052,919**	

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 Mayor's Financial Administration, although not in scope for 2020 did receive payments on behalf of Salt Lake County in 2019.
② Planning and Development, although not in scope for 2020, did receive payment card revenue on behalf of Salt Lake County in 2019 prior to becoming part of an independent tax district.