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 2019
Report Number 2019-17

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

October 2019
Report Number 2019-17

Scott Tingley, CIA, CGAP
Salt Lake County Auditor

Cherylann Johnson, MBA, CIA, CFE, CRMA
Chief Deputy Auditor

Shawna Ahlborn
Audit Services Division Administrator

Audit Staff:
Colleen Hilton

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

Date: October 1, 2019

To: The Citizens of Salt Lake County, the County Mayor and County Council

From: Scott Tingley, Salt Lake County Auditor

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

TRANSMITTAL LETTER

Transmitted herewith is our report, **An Audit of Salt Lake County's Compliance with the Payment Card Industry Data Security Standard** (Report Number 2019-17). An Executive Summary of the report can be found on page 1. 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 2019.

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 Services Division throughout the audit. Our work was made possible by their cooperation 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
Mark Evans, Associate Director of Information Security
Martin Jensen, Division Director, Parks and Recreation Division
Jon Daich, Director of Finance, SMG Property Management, Inc.

Table of Contents

Executive Summary

Background

Salt Lake County organizations accept credit and debit cards (“payment cards”) for a wide variety of goods and services provided to County residents and customers. In 2018, County agencies processed approximately 1.2 million payment card transactions totaling $96,847,989, ranging from fitness and recreation center passes to theater tickets, youth sports registrations, library fines and fees, 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 the County provides.

The Payment Card Industry (“PCI”) Data Security Standard (“Standard”) is a set of 12 requirements, created and maintained by the PCI Security Standard Council (“Security 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.

In our audit, we determined whether all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2019.

What We Found

Cardholder data may have been exposed when using County computers to process some payment card transactions. (p. 10).

We found that Parks and Recreation Center employees were using their desktop computers at their workstations to process payment card transactions by accessing the point of sale (POS) software application without appropriate firewall protection in place, potentially exposing cardholder data to hackers or others with malicious intent.

Some contracts for outsourced management services did not include an acknowledgement of responsibility for the security of cardholder data. (p. 11).

We found that the current contracts with SMG for management services at the Salt Palace Convention Center, Mountain America Expo Center, and the Equestrian Park did not include a stipulation to comply with Countywide Policy 1400-7, *Payment Card Industry Data Security Standard Policy*.

What We Recommend

To eliminate the potential of exposing cardholder data:

Access rights to enter cardholder data into the POS application on County computer workstations should be terminated.

ACTION TAKEN: As of October 14, 2019, the site configuration for all recreation centers using the POS application was set to not allow manual entry of payment card data.

To ensure that service providers acknowledge their responsibility for the security of cardholder data:

Contracts should include the stipulation that SMG agrees to comply with Countywide Policy 1400-7 "Payment Card Industry Data Security Standard Policy."

ACTION TAKEN: An amendment to one of the two contracts to include the expectation to comply with Policy 1400-7 was drafted by the District Attorney's Office.

Please refer to the main sections in the report for more details about these and other findings and recommendations.

Introduction

Background and Purpose

Salt Lake County organizations accept credit and debit cards ("payment cards") for a wide variety of goods and services provided to County residents and customers. In 2018, County agencies processed almost 1.2 million payment card transactions totaling $96,847,989, ranging from fitness and recreation center passes to theater tickets, youth sports registrations, library fines and fees, 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 the County provides.

The County Treasurer sets up and manages merchant accounts for County agencies that request the ability to accept payment cards, and payment card transactions are processed through a major merchant bank. In some cases, payment card transactions are processed through a third-party vendor, on-behalf of county agencies, by an outsourcing agreement. Property tax payments by credit or debit card are an example of outsourced payment card transactions at the County.

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

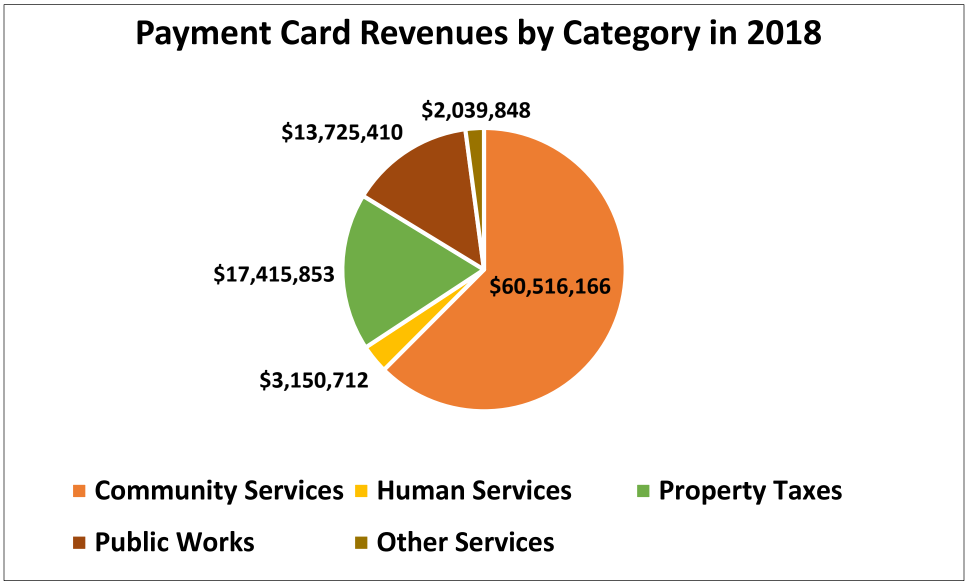
> *"County agencies that accept, process, transmit or store cardholder data will demonstrate their compliance with the Payment Card Industry Data Security Standard (PCI-DSS) annually to the County Auditor by September 30th of each year. Agencies found to be non-compliant will have a 6-month grace period 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." (CWP 1400-7, 5.0, p. 3-4)*

For the purposes of this audit, we categorized County payment card transactions 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 2018, is shown in Figure 1.

Figure 1. Payment Card Revenues by Category in 2018. *Community services made up approximately 62% of the total payment card transaction revenue in 2018.*



The Payment Card Industry Data Security Standard

The Payment Card Industry ("PCI") Data Security Standard ("Standard") is a set of 12 requirements, created and maintained by the PCI Security Standard Council ("Security Council"). The Security Council is a private sector body, made up of all the major payment card brands (e.g., American Express, Discover, MasterCard, Visa, and JCB International). 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 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. Figure 2 lists the goals and specific requirements of the Standard.

Figure 2. PCI Data Security Standard Goals and Requirements. *The primary goal of the Standard is to protect cardholder data and decrease the likelihood of payment card fraud.*

PCI Data Security Standard 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.

Securing cardholder data is a challenge facing all merchants that process payment cards. Complying with 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, they define a data breach 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 our study, we identified three main causes of a data breach: malicious or criminal attack, system glitch, or human error. The costs of data breach vary according to the cause and the safeguards in place at the time of the data breach."*

Further, in the study, Ponemon equates the cost of each comprised record as $150, an increase of 1.3 percent since 2018. Ponemon defines a comprised record as,

> *"information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. One example is a retail company's database with an individual's name associated with credit card information and other personally identifiable information . . . In this year's study, the average cost to the organization per compromised record was $150."*

[1] Benchmark research sponsored by IBM Security, study conducted by Ponemon Institute LLC, *2019 Cost of a Data Breach Report*

Some of the negative effects of a data breach involving cardholder data could include the following:

- Loss of confidence by cardholders and customers
- Diminished revenues
- Costs of reissuing new payment cards
- Fraud losses
- Legal costs, settlements, and judgments
- Fines and penalties
- Termination of ability to accept payment cards

The Ponemon study further noted that,

> *"malicious attacks were the most common and most expensive root cause of breaches. . . Since 2014, the share of breaches caused by malicious attacks surged by 21 percent, growing from 42 percent of breaches in 2014 to 51 percent of breaches in 2019. . . While malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half (49 percent) of the data breaches studied in the report."*

The PCI DSS Compliance Validation Process

The Security Council requires that all payment card merchants validate that they are compliant with the Standard at least annually. Depending on their annual volume of payment card transactions, and the types of information systems that are used, some smaller merchants can validate their compliance through a self-assessment process.

In the self-assessment validation process, merchants are required to complete a Self-Assessment Questionnaire ("SAQ") and attest to their compliance with the Standard with an Attestation of Compliance ("AOC") form. For the majority of the County agencies, we identified the correct SAQ type that should be completed for PCI DSS compliance validation based on our understanding of the payment card environment and made sure that County fiscal managers and IT managers were aware of the correct SAQ type that applied to their specific organization. For reference, we have provided a listing of County entities and their appropriate SAQ type, in table one of the Audit Results.

When a County entity uses a third-party vendor to either manage a County facility, or process payment card transactions on behalf of the County, then the guidelines of the Standard state that the County is responsible for ensuring that the third-party vendor validates their compliance with the Standard at least annually. Copies of completed SAQs and AOCs must be sent to the County's merchant bank once a year as well. Detailed descriptions of each SAQ type are provided in Appendix A, for reference.

Objective

Our overall audit objective was to determine whether all county entities that accept payment cards met the PCI DSS compliance validation requirements during 2019.

Scope and Methodology

In 2019, we identified and evaluated PCI DSS compliance for 25 County entities that accept payment cards as a form of payment for goods or services. Our audit focused on determining the correct merchant level and SAQ type for each entity.

We utilized the information and documentation obtained in 2018 and noted changes in the payment card environment from the prior year. We identified two agencies that accepted payment cards in 2018 and 2019 on a temporary basis.

We collaborated with each entity and County Information Services (IS), to ensure that SAQs were completed in a timely manner during 2019. We reviewed each entity's SAQ to determine whether all sections of the forms were filled out completely and correctly based on our understanding of each agency's payment card processing environment.

We used a preliminary survey, emails, phone conversations, and site visits to assess each agency's payment card processes and examined their current payment card environments. We also worked with County IS to provide technical assistance to County entities as needed.

Audit Results

Objective – PCI DSS Compliance Validation Requirements 2019

Determine if all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2019.

As part of our role in facilitating the PCI DSS validation process with County entities in 2019, we reviewed past SAQs and AOC forms, and compared them with the current SAQ responses. We identified two agencies, the District Attorney's Office and Mayor's Finance Administration, that accepted payment cards in 2018 and 2019 respectively on a temporary basis after the Treasurer's Office notified us that they had set up merchant accounts for those agencies.

We evaluated four non-County entities for compliance, based on the scope of the policy. **Countywide Policy 1400-7, *"Information Technology Security PCI DSS Policy,"* Section 1.0, Scope,** states:

> *"The scope of this policy includes any County Agency that accepts, stores, processes, or transmits credit card information (electronically or on paper), its employees, volunteers, or 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." (CWP 1400-7, 1.0, p. 1)*

For purposes of this report, we are including the following four non-county entities as County agencies:

- SMG for the managed venues of the Equestrian Park, Mountain America Expo Center, and Salt Palace Convention Center
- IMG managed HealthyMe Clinic
- USU Extension Services at the Salt Lake County Government Center
- Wasatch Front Waste and Recycling District

The process to determine County compliance with PCI DSS included the following steps:

- **Identifying all County agencies that accept payment cards, and therefore all county agencies required to validate their compliance with the Standard.**
- **Identifying the payment card environment for each agency to determine the correct SAQ type to be completed.**
- **Reviewing the 2019 SAQ and AOC to determine if all sections were completed and answered correctly to the best of their knowledge.**
- **Reviewing contractors and contract terms.**

Accomplishing the steps above involved the completion of a preliminary survey by the agencies, meeting face to face, phone conversations, and email exchanges with the agencies.

In addition, we verified with County IS, that no other county agencies had been provided access to the Salt Lake County cardholder data environment during 2019, beyond those that we had identified in the audit steps listed. We determined that the same agencies identified in 2018 as being in scope, were unchanged for 2019 plus two more added in 2019. We verified that all agencies identified were within the scope of the policy.

We found that all 25 agencies that were required to complete the SAQ and AOC forms, had completed these forms by September 30, 2019. We note that some agencies completed more than one version of the forms, if earlier versions had not been correctly completed.

Countywide Policy 1400-7, *"Payment Card Industry Data Security Standard Policy,"* Section 3.1.1, states:

> *"PCI-DSS compliance requires . . . that County agencies that accept, process, transmit or store cardholder data shall complete the appropriate SAQ and AOC for their merchant category." (CWP 1400-7, 3.1.1, p. 3)*

Table 1 shows a list of these 25 agencies and the completion dates of their forms. Completion dates represent the final version of the forms.

Table 1: County Agencies, SAQ Type(s), 2019 Completion Dates. *All twenty-five agencies that were required to, completed an SAQ and AOC by the annual September 30 deadline.*

County Agencies – SAQ Type(s) – 2019 Completion Dates		
County Agency	**2019 SAQ type(s)**	**2019 Completion Date**
Aging and Adult Services	C	June 18
Animal Services	C	May 23
Archives	C	June 17
Arts & Culture fka: Center for the Arts	C	September 26
Assessor's Office	A	May 23
Clerk's Office	B-IP	April 29
Criminal Justice Services	B-IP	August 29
District Attorney's Office	A	June 21
Engineering and Flood Control	C-VT	July 31
Health Department	B-IP	June 12
HealthyMe Clinic	B	September 5
Justice Court	B-IP	September 13
Library Services	B-IP	September 26
Mayor's Finance	A	July 16
Parks and Recreation Centers	C	September 27
Parks and Recreation Golf Courses	B-IP	August 19
Planetarium	C	June 20
Planning and Development	B-IP & C-VT	May 30
Recorder's Office	C	August 22
SMG – 3 managed venues	C	September 24
Solid Waste Management	B-IP	August 27
Surveyor's Office	C-VT	May 7
Treasurer's Office	C-VT	August 29
USU Extension Services	B-IP	July 2
Wasatch Front Waste & Recycling	B-IP	April 30

In conjunction with County IS, we identified changes in the payment card environment from 2018 that could have changed the SAQ form type to be completed in 2019. Further, we identified County agencies of the District Attorney's Office and Mayor's Finance Administration that accepted payment cards in 2018 and 2019 respectively on a temporary basis and determined the correct SAQ type.

In 2019, we requested the completion of an SAQ and AOC for all types identified for each agency. Twenty four of the 25 (96%) agencies were required to complete only one SAQ type. Only one entity had different methods of accepting payment cards, which required more than one type of SAQ be completed.

After we received the first SAQ and AOC forms from the agencies, we reviewed them to determine if all required areas were completed correctly to the best of our knowledge and understanding of each agency's payment card environment. If any deficiencies were identified, we would contact the agency to correct any error(s) in the forms and have them resubmit them for our review. This process would sometimes take several contacts with the agencies, either via email, phone, or in person, before all areas of the forms were completed and verified.

We also reviewed the SMG contract with the County for management services provided by SMG for the three County owned venues of the Salt Palace Convention Center, Mountain America Expo Center, and Equestrian Park. This review was conducted after concerns were raised by the County IS Director of Information Security.

Findings and Recommendations

Finding 1: Salt Lake County Parks and Recreation employees had processed payment card transactions on County computers without appropriate firewall protection, potentially exposing cardholder data each time a transaction was processed.

We found that Parks and Recreation Center employees were using their desktop computers at their workstations to process payment card transactions by accessing the point of sale (POS) software application without appropriate firewall protection in place, potentially exposing cardholder data to hackers or others with malicious intent. The desktop computers were also being used to allow access to the internet via browsers, emails, etc. Cardholder data was not protected by properly segregating and securing the computer workstations with a firewall.

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

PCI DSS Requirement 1, states:

> *All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to*

> *and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.*

The Parks and Recreation management and employees were unaware of the risks posed by entering payment card data directly into the POS application on a computer that was also utilized for other computer applications and email.

An unknown number of payment card transactions were processed on County computers without proper firewalls in place, potentially exposing cardholder data to being breached.

Recommendation

> We recommend that the access rights to enter payment cardholder data into the POS application on County computer workstations be terminated.
>
> **ACTION TAKEN:** As of October 14, the site configuration for all recreation centers using the POS application was set to not allow manual entry of payment card data.

Finding 2: The contracts with SMG to provide facility management services for the County did not acknowledge that they are responsible for the security of cardholder data for payment card transactions made on behalf of the County.

SMG is a venue management group that specializes in managing publicly owned facilities. SMG has been contracted by Salt Lake County to manage three venues: Salt Palace Convention Center, Mountain America Expo Center, and Equestrian Park. Each of these County owned venues accept payment cards for a variety of goods and services including rent, telecommunications, marquee advertising, parking, etc.

While reviewing the contracts between SMG and the County, we determined there was not an acknowledgement by SMG of the expectation to comply with Countywide Policy 1400-7 "Payment Card Industry Data Security Standard Policy." County Policy emphasizes the responsibility to comply with PCI DSS for the security of payment cardholder data.

PCI DSS Requirement 12, states:

> *"Maintain a policy that addresses information security for all personnel. A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, 'personnel' refers to full-time and part-time employees, temporary employees, contractors and consultants who are 'resident' on the entity's site or otherwise have access to the cardholder data environment."*

The absence of the requirement in the SMG contract to comply with Policy 1400-7 was not previously identified.

Without a written acknowledgement, then contractors who accept payment cards on behalf of the County, may not be as committed to maintaining proper security of cardholder data, nor bear any responsibility in the event of a data breach.

Recommendations

We recommend that amendments be made to the current contracts between SMG and the County to include the expectation for SMG to comply with Countywide Policy 1400-7 "Payment Card Industry Data Security Standard Policy."

ACTION TAKEN: An amendment to one of two of the SMG contracts to include the expectation to comply with Countywide Policy 1400-7 has been drafted by the District Attorney's Office.

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.

Appendix B: County Agencies 2018 Payment Card Revenue

County Agencies – 2018 Payment Card Revenues & Transactions – Categories

Agency	Payment Card Revenue 2018	Number of Payment Card Transactions 2018	Category
Aging and Adult Services	41,269	500	Human Services
Animal Services	622,072	14,052	Public Works
Archives	1,094	110	Other Services
Arts & Culture fka: Center for the Arts	33,253,607	121,524	Community Services
Assessor's Office	2,015,492	5,430	Property Taxes
Clerk's Office	839,346	18,636	Other Services
Criminal Justice Services	261,644	4,480	Human Services
District Attorney's Office	8,400	84	Other Services
Engineering and Flood Control	54,503	201	Public Works
Health Department	2,812,309	29,738	Human Services
HealthyMe Clinic	53,115	2,108	Other Services
Justice Court	976,157	7,152	Other Services
Library Services	901,928	92,881	Human Services
Mayor's Finance	0	0	Other Services
Parks and Recreation Centers	15,725,298	345,116	Community Services
Parks and Recreation Golf Courses	6,976,859	164,578	Community Services
Planetarium	1,542,918	65,478	Community Services
Planning and Development	1,065,704	2,823	Public Works
Recorder's Office	91,707	3,943	Other Services
SMG – Equestrian Park	210,934	895	Community Services
SMG – Mountain America Expo Ctr.	60,974	854,420	Community Services
SMG – Salt Palace Convention Ctr.	1,050,202	46,842	Community Services
Solid Waste Management	7,760,627	122,550	Public Works
Surveyor's Office	70,029	345	Other Services
Treasurer's Office	15,400,361	5,739	Property Taxes
USU Extension Services	35,490	348	Human Services
Wasatch Front Waste & Recycling	4,222,504	63,975	Public Works
2018 Payment Card Revenues	**$96,847,989**	**1,180,502**	