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 2018
Report Number 2018-12

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

October 2018
Report Number 2018-12

Scott Tingley, CIA, CGAP
Salt Lake County Auditor

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

Audit Manager:
Shawna Ahlborn

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

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, 2018

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 2018-12). 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 2018.

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
Honorable Judge Shauna Graves-Robertson
Steven Calbert, Administrative and Fiscal Manager, Salt Lake County Justice Court

SALT LAKE
COUNTY

Table of Contents

Executive Summary

Background

Salt Lake County entities processed $80,528,676 in payment card transactions in 2017.

Salt Lake County organizations accept credit and debit cards as payment for a wide variety of goods and services provided to County residents and customers. In 2017, County agencies processed over 1.2 million payment card transactions totaling $80,528,676, ranging from fitness and recreation center passes to theater tickets, youth sports registrations, library fines and fees, 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 ("DSS") is a set of 12 requirements, created and maintained by the PCI Security Standards 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 2018.

What We Found

Salt Lake County Justice Court employees had processed payment card transactions on County computers without appropriate firewall protection, potentially exposing cardholder data each time a transaction was processed. (p. 10)

We found that Salt Lake County Justice Court ("Justice Court") employees were using their desktop computers at their workstations to process payment card transactions by accessing a website payment portal without appropriate firewall protection in place, potentially exposing cardholder data to hackers or others with malicious intent. Upon discovery of the issue, Justice Court management stopped the practice immediately, and evaluated options and formulated a plan to mitigate the risk.

What We Recommend

To ensure that all county entities are compliant with the requirements set forth by the Payment Card Industry Security Standards Council:

We recommend that Justice Court management take immediate steps to find another secure solution for accepting and processing payment cards.

Summary of Agency Response

We issued a single recommendation in our report and the Justice Court took the following action(s) to remediate the issue(s) identified:

> *Upon discovery of the issue by Audit Services, Justice Court employees immediately stopped using the payment portal to process payment card transactions over the phone. They returned to using the compliant card reader to process payment card transactions over the phone.*
>
> *Furthermore, in September 2018, County IS assisted Justice Court management in locking down a computer that could only access the Justice Court online payment portal that redirects to a third-party provider to enter cardholder data. The computer is used to conveniently process payment card transactions for phone orders and uses a dedicated network segment secured with a firewall.*

Introduction

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 2017, County agencies processed over 1.2 million payment card transactions totaling $80,528,676, 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 PCI DSS annually. *Countywide Policy 1400-7, "Information Technology Security-Payment Card Industry Data Security Standard Policy," Section 5.0 Enforcement* states that:

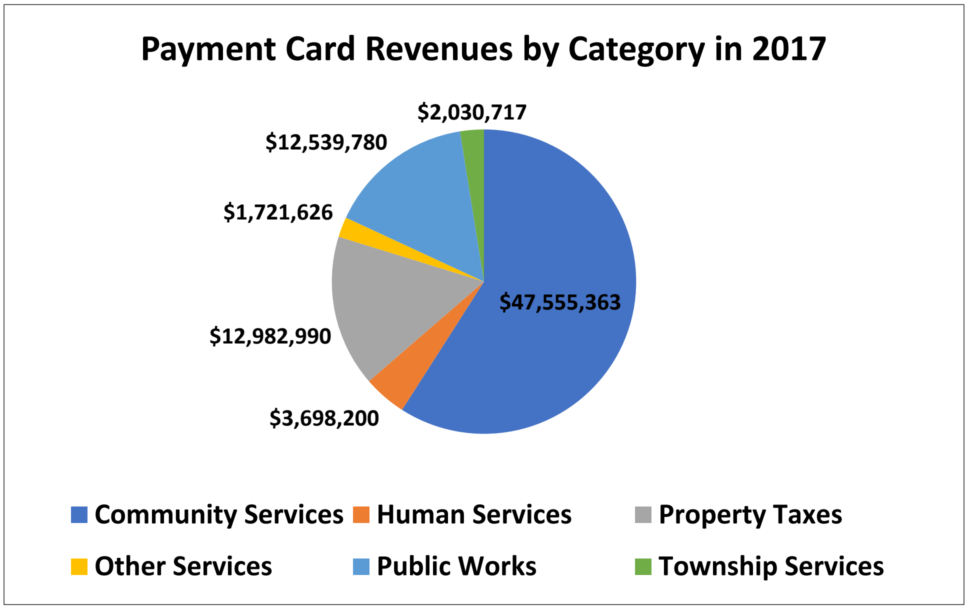
> *"County agencies that accept, process, transmit or store cardholder data will demonstrate their compliance with the Payment Card Industry Data Security Standard (PCI_DSS) annually to the County Auditor by September 30th of each year. Agencies found to be non-compliant will have a 6-month grace period 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 six major categories:

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

The total dollar amount of payment card transactions in each of the six categories during 2017, is shown in Figure 1.

Figure 1. Payment Card Revenues by Category in 2017. *Community services made up approximately 59% of the total payment card transaction revenue in 2017.*



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 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 $148. 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 $148."*

[1] Benchmark research sponsored by IBM Security, independently conducted by Ponemon Institute LLC, July 2018, *2018 Cost of a Data Breach Study: Global Overview*

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

In a recent article[2] published on the Business Insider website, they noted the following:

- Data breaches are on the rise. Since January 2017, at least 16 retailers were hacked and likely had information stolen from them.
- A report from cybersecurity firm Shape Security showed that almost 90% of the login attempts made on online retailers' websites are hackers using stolen data.
- Many of these breaches were caused by flaws in payment systems that were taken advantage of by hackers.

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 2018.

[2] Business Insider, August 22, 2018, *If you shopped at these 16 stores in the last year, your data might have been stolen*

Scope and Methodology

In 2018, 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 2017 and noted changes in the payment card environment from the prior year. In addition, we identified two agencies that started accepting payment cards in 2018.

We collaborated with each entity and County IS, to ensure that SAQs were completed in a timely manner during 2018. 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 2018

> **Determine if all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2018.**

As part of our role in facilitating the PCI DSS validation process with County entities in 2018, we reviewed past SAQs and AOC forms, and compared them with the current SAQ responses from 2018. We identified two agencies, the Recorder's Office and Archives, that started accepting payment cards in 2018 when the Treasurer's Office notified us that they had set up merchant accounts for those agencies.

We evaluated six non-County agencies 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 six non-county agencies as County agencies:

- SMG managed Equestrian Park
- SMG managed Mountain America Expo Center (formerly, South Towne Expo Center)
- SMG managed 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 2018 SAQ and AOC to determine if all sections were completed and answered correctly to the best of their knowledge.**

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 2018, beyond those that we had identified in the audit steps listed. We determined that 23 of the same agencies identified in 2017 as being in scope, were unchanged for 2018 plus two more added in 2018. 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, 2018. 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), 2018 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) – 2018 Completion Dates		
County Agency	**2018 SAQ type(s)**	**2018 Completion Date**
Aging and Adult Services	C	September 28
Animal Services	C	May 16
Archives	C	May 8
Assessor's Office	A	June 28
Center for the Arts	C	September 13
Clerk's Office	B-IP	March 22
Criminal Justice Services	B	July 20
Engineering and Flood Control	C-VT	August 1
Health Department	B-IP	July 5
HealthyMe Clinic	B	September 7
Justice Court	C	September 24
Library Services	B-IP	September 6
Parks and Recreation Centers	C	July 20
Parks and Recreation Golf Courses	C	July 18
Planetarium	C	May 24
Planning and Development	B-IP & C-VT	July 23
Recorder's Office	C	August 14
SMG – Equestrian Park	B-IP & C combo	September 20
SMG – Mountain America Expo Ctr.	B-IP & C combo	September 20
SMG – Salt Palace Convention Center	B-IP & C combo	September 20
Solid Waste Management	C	August 28
Surveyor's Office	C-VT	March 22
Treasurer's Office	C-VT	August 3
USU Extension Services	B-IP	August 2
Wasatch Front Waste & Recycling	B-IP	April 24

In conjunction with County IS, we identified changes in the payment card environment from 2017 that could have changed the SAQ type in 2018. Further, we identified County agencies of the Recorder's Office and Archives that had begun to accept payment cards in 2018 and determined the correct SAQ type.

In 2018, we requested the completion of an SAQ and AOC for all types identified for each agency. Twenty one of the 25 (84%) agencies were required to complete only one SAQ type. However, some entities had numerous 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, both the Auditor and County IS 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.

Findings and Recommendations

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

Risk Rating: 1 / 5 (Very Low)

We found that Justice Court employees were using their desktop computers at their workstations to process payment card transactions by accessing a website payment portal without appropriate firewall protection in place, potentially exposing cardholder data to hackers or others with malicious intent. The infrastructure is available at the Salt Lake County Government Center to protect cardholder data by properly segregating and securing 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 processing of payment card transactions and 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.

We found that Justice Court employees were using unsecured computer workstations without any firewall protections to access an external website payment portal to process payment card transactions over the phone. In person payment card transactions at the Justice Court were still being processed with PCI DSS compliant card readers.

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."*

Justice Court management had made a change to the payment card environment for processing phone payments without understanding the risks of the change that was made. 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 Justice Court management take immediate steps to find another secure solution for accepting and processing payment cards.

Action Taken

Upon discovery of the issue by Audit Services, Justice Court employees immediately stopped using the payment portal to process payment card transactions over the phone. They returned to using the compliant card reader to process payment card transactions over the phone.

Furthermore, in September 2018, County IS assisted Justice Court management in locking down a computer that could only access the Justice Court online payment portal that redirects to a third-party provider to enter cardholder data. The computer is used to conveniently process payment card transactions for phone orders and uses a dedicated network segment secured with a firewall.

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 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 that are included in and managed via a validated, PCI SSC-listed 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 2017 Payment Card Revenue

County Agencies – 2017 Payment Card Revenues & Transactions – Categories

Agency	Payment Card Revenue 2017	Number of Payment Card Transactions 2017	Category
Aging and Adult Services	$29,250	276	Human Services
Animal Services	551,719	13,623	Public Works
Archives	0	0	Other Services
Assessor's Office	1,740,010	5,197	Property Taxes
Center for the Arts	22,851,856	121,611	Community Services
Clerk's Office	709,552	17,058	Other Services
Criminal Justice Services	237,928	4,520	Human Services
Engineering and Flood Control	47,744	158	Public Works
Health Department	2,543,351	27,297	Human Services
HealthyMe Clinic	42,601	1,812	Other Services
Justice Court	905,687	6,705	Other Services
Library Services	851,138	88,637	Human Services
Parks and Recreation Centers	15,653,067	508,008	Community Services
Parks and Recreation Golf Courses	5,793,813	150,263	Community Services
Planetarium	1,495,290	68,721	Community Services
Planning and Development	2,030,717	6,672	Township Services
Recorder's Office	0	0	Other Services
SMG – Equestrian Park	201,610	862	Community Services
SMG – Mountain America Expo Ctr.	872,644	43,241	Community Services
SMG – Salt Palace Convention Ctr.	687,083	922	Community Services
Solid Waste Management	8,375,424	97,561	Public Works
Surveyor's Office	63,786	311	Other Services
Treasurer's Office	11,242,980	4,090	Property Taxes
USU Extension Services	36,533	429	Human Services
Wasatch Front Waste & Recycling	3,564,893	58,174	Public Works
2017 Payment Card Revenues	**$80,528,676**	**1,226,148**	

Agency Response

Agency Response
Justice Court

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

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
We recommend that Justice Court management take immediate steps to find another secure solution for accepting and processing payment cards.	Agree	**Action Taken:** In September of 2018, County IS assisted Justice Court management in locking down a computer that could only access the Justice Court online payment portal that redirects to a third-party provider to enter cardholder data. The computer is used to process payment card transactions for phone orders and uses a dedicated network segment secured with a firewall.	Completed