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

April 2018
Report Number 2018-01

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

April 2018
Report Number 2018-01

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.

STATE OF UTAH
COUNTY
AUDITOR
1896
SALT LAKE COUNTY

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

SALT LAKE
COUNTY

Date: April 6, 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 2018-01). 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 2017.

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
James Cooper, Division Director, Library Services
Martin Jensen, Division Director, Parks and Recreation

This Page Left Blank Intentionally

Table of Contents

This Page Left Blank Intentionally

Executive Summary

Background

Salt Lake County entities processed $87,856,620 in payment card transactions in 2016.

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 2016, County agencies processed almost 1.2 million payment card transactions totaling $87,856,620, 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 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.

In our audit, we determined whether all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2017. We also examined whether all county agencies that accept payment cards ensured that all employees that handle or have access to cardholder data, completed annual IT security awareness training, as required by Countywide Policy.

What We Found

We found that Library Services and Parks and Recreation could not verify that all employees who had access to cardholder data, had completed security awareness training in 2017. (p. 11)

We found that the Library Services Division and the Parks and Recreation Division had employees who had not completed the annual IT security awareness training by the September 30, 2017 deadline. In Library Services, we found that nine employees who were required to complete the training, had not done so by September 30th. Although Parks and Recreation reported that a total of 69 employees had completed the training, they could not provide an accurate count of the total number of employees who handle cardholder data.

Parks and Recreation did not maintain an accurate list of the names of all employees that had access to cardholder data, and therefore were required to complete the IT security awareness training annually. (p. 13)

The Parks and Recreation Division operates 19 recreation centers, six golf courses, and both the Wheeler Historic Farm and Millcreek Canyon toll booth, throughout the County. These facilities accept payment cards and have county employees that have access to cardholder data that is processed and transmitted. During our audit, we found that Parks and Recreation could not provide an accurate listing of employees working at these facilities who had access to cardholder data in their point of sale systems.

What We Recommend

To ensure that all county entities follow Countywide Policy 1400-7:

We recommend that Library Services and Parks and Recreation management ensure that all employees with access to cardholder data complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.

To ensure that all county entities can accurately track employees who have completed the required annual IT security awareness training:

We recommend that Parks and Recreation management implement a process to identify all employees with access to cardholder data and require that all those employees complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.

Summary of Agency Response

We received a response to the audit from both Library Services and Parks and Recreation regarding the recommendations given. Each agency outlined an action plan that included the actions that management will take to remediate the issues identified, the person or persons responsible for implementing the action plan, and a due date for completion.

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 2016, County agencies processed almost 1.2 million payment card transactions totaling $87,856,620, 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 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.

On February 28, 2017, the County Council ratified an amendment to the enforcement section of Countywide Policy 1400-7. The amended portion of **Countywide Policy 1400-7, *"Information Technology Security-Payment Card Industry Data Security Standard Policy,"* Section 5.0 Enforcement** states:

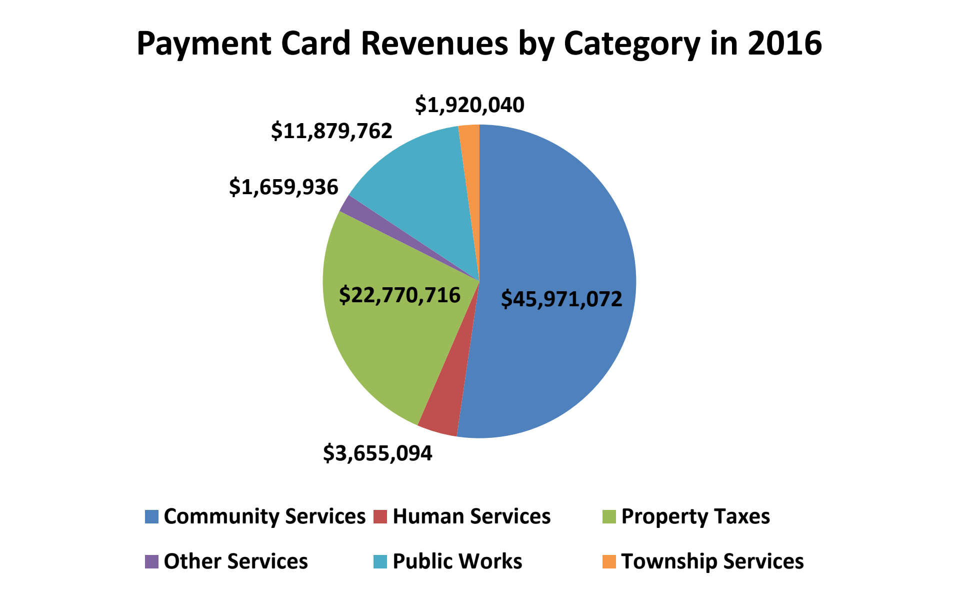
> *"County agencies that accept, process, transmit or store cardholder data will demonstrate their compliance with the Payment Card Industry Data Security Standard (PCI_DSS) annually to the County Auditor by September 30th of each year. Agencies found to be non-compliant will have a 6-month grace period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

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 2016, is shown in Figure 1.

Figure 1: Payment Card Revenues by Category in 2016.



Community Services and Property Tax Payments made up approximately 78% of the total payment card transactions in 2016.

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.

PCI Data Security Standard Goals and Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

The primary goal of the Standard is to protect cardholder data and decrease the likelihood of payment card fraud.

A recent SecurityMetrics blog conclusion[1] regarding the cost of PCI DSS compliance states that,

> *"Securing cardholder data is a challenge facing all businesses that process credit cards. Know that following the PCI DSS is a great place to start. Ignoring the PCI DSS, or going after it half-heartedly is a recipe for disaster. PCI DSS is the best way to start your data security, and ultimately cheaper than exposing your brand to a data breach."*

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
- Fraud losses
- Legal costs, settlements, and judgments
- Fines and penalties
- Termination of ability to accept payment cards

In another SecurityMetrics blog[2], the author outlines the financial costs a data breach could cause including the following:

- **Merchant processor compromise fines:** $5,000 - $50,000
- **Forensic investigation:** $12,000 - $100,000+
- **Onsite QSA assessments following the breach:** $20,000 - $100,000
- **Free credit monitoring for affected individuals:** $10 - $30 per card
- **Card re-issuance penalties:** $3 - $10 per card
- **Breach notification costs:** $2,000 - $5,000+
- **Technology repairs:** $2,000 - $10,000+
- **Increase in monthly card processing fees:** +

[1] SecurityMetrics blog *How Much Does PCI Compliance Cost?* by Gary Glover, VP of Assessments, QSA, CISSP

[2] SecurityMetrics blog *How Much Does a Data Breach Cost Your Organization?* by David Ellis, Director of Forensic Investigations, CISSP, QSA, PFI

- **Legal fees:** +
- **Civil judgments:** +

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. We identified the correct SAQ type that each County entity should complete for PCI DSS compliance validation 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 Appendix B.

Part of the process of demonstrating PCI DSS compliance validation involves ensuring employees who handle cardholder data complete a security awareness training program. The County has a training program that meets this need for most employees. A handful of temporary employees can complete an in-house training with subject matter approved by the County's Information Services Division ("County IS").

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.

Objectives

Our overall audit objectives were as follows:

Objective 1 – PCI DSS Compliance Validation Requirements

- Determine whether all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2017.

Objective 2 – Annual Security Awareness Training

- Determine if county agencies that accept payment cards ensured that all employees that handle or have access to cardholder data, completed annual security awareness training, as required by Countywide Policy 1400-7.

Scope and Methodology

In 2017, we identified and evaluated PCI DSS compliance for 23 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 and determining if employees that handle cardholder data completed the required annual security awareness training.

We utilized the information and documentation obtained in 2016 and noted any possible changes in the payment card environment from the prior year. We asked each agency to furnish a list of all employees in their agency that handle cardholder data and confirmed that they had completed the annual security awareness training.

We collaborated with each entity and County IS, to ensure that SAQs were completed in a timely manner during 2017. 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 1 – PCI DSS Compliance Validation Requirements

Determine whether all county entities that accept payment cards met the appropriate PCI DSS compliance validation requirements during 2017.

As part of our role in facilitating the PCI DSS validation process with County entities in 2017, we requested copies of the most recent validation documentation that each County agency had completed. We reviewed past SAQs and AOC forms, and compared them with the current SAQ responses from 2017.

In 2016, we added five non-County agencies to be evaluated 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 those five non-county agencies as County agencies. They include the Salt Palace Convention Center, South Towne Expo Convention Center, the Equestrian Park, the USU Extension, and the Wasatch Front Waste & 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.**
- **Reviewing the 2017 SAQ to determine if the proper SAQ-type was completed based on each county entity's payment card processing environment.**
- **Determining the proper SAQ type if a 2016 SAQ was not completed.**
- **Reviewing the 2017 SAQ and AOC to determine if all sections were completed and answered correctly to the best of their knowledge.**

Accomplishing the steps above involved 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 2017, beyond those that we had identified in the audit steps listed. We determined that the same agencies identified in 2016 as being in scope, were unchanged for 2017. Additionally, we verified that all agencies identified were within 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)*

Furthermore, we contacted each agency to inform them of the amended portion of the revised countywide policy that changed the completion date to demonstrate compliance with the PCI DSS Policy to September 30th, each year.

We found that all 23 agencies that were required to complete the SAQ and AOC forms, had completed these forms by September 30, 2017. We noted 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 23 agencies and the completion dates of their forms. Completion dates represent the final version of the forms.

Table 1: County Agencies, SAQ Type(s), 2017 Completion Dates.

County Agencies – SAQ Type(s) – 2017 Completion Dates		
County Agency	**2017 SAQ type(s)**	**2017 Completion Date**
Aging and Adult Services	A	July 10
Animal Services	B-IP	April 26
County Assessor	A	July 14
Center for the Arts	C	August 17
Criminal Justice Services	B	May 31
County Clerk	B-IP	March 20
Engineering and Flood Control	C-VT	August 4
Health Department	B	July 12
HealthyMe Clinic	B	September 13
Justice Court	B-IP	August 7
Library Services	B-IP	September 25
Parks and Recreation – Recreation Centers	C	August 29
Parks and Recreation – Golf Courses	C	August 29
Clark Planetarium	P2PE	May 30
Planning and Development	B-IP & C-VT	September 27
Solid Waste Management	C	September 19
County Surveyor	C-VT	March 8
County Treasurer	C-VT	July 10
Wasatch Front Waste & Recycling District	B-IP	May 30

USU Extension Services	B-IP	July 31
SMG – Salt Palace	B-IP & C-VT	August 8
SMG – South Towne Expo	B-IP & C-VT	August 8
SMG – Equestrian Park	B-IP & C-VT	August 8

All twenty-three agencies that were required to, completed an SAQ and AOC by the annual September 30 deadline.

In conjunction with County IS, we identified changes in the payment card environment from 2016 that could have changed the SAQ type in 2017. We did not include Clark Planetarium in this process of accessing changes because they did not complete the forms in 2016.

In 2017, we requested the completion of an SAQ and AOC for all types identified for each agency. Nineteen of the 23 (83%) agencies were required to complete only one SAQ type. However, some entities had numerous ways 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.

Objective 2 – Annual Security Awareness Training

> **Determine whether county agencies that accept payment cards ensured that all employees that handle or have access to cardholder data, completed annual security awareness training, as required by Countywide Policy 1400-7.**

County IS administers a security awareness training program through an online web-based application, that is available to all county employees that have a valid county network login. The Standard requires that any entity that processes, stores, or transmits cardholder data, must maintain an information security policy for all personnel. As part of this requirement, the Security Council guidelines state that each entity should maintain a current information security awareness training program for all employees who handle payment card transactions or have access to cardholder data.

Countywide Policy 1400-7, *"Payment Card Industry Data Security Standard Policy,"* Section 3.1.5, states:

> *“PCI-DSS compliance requires . . . that County agencies that accept, process, transmit or store cardholder data shall provide annual security awareness training to employees that have access to cardholder data. This training is available through County Information Services.” (CWP 1400-7, 3.1.5, p. 3)*

In 2017, we noted that four county agencies (see Table 2) that were managed by an external management contractor. Each of the four verified their compliance with the Standard Requirement 12.6, by noting that they maintained an information security awareness training program for their employees on their SAQs for 2017.

Table 2: County Agencies Operated by an External Management Contractor.

County Agencies Operated by an External Management Contractor		
County Agency	**External Management Contractor**	**Confirmed Compliance SAQ Requirement 12.6**
Salt Palace	SMG	Yes
South Towne Expo	SMG	Yes
Equestrian Park	SMG	Yes
HealthyMe Clinic	Intermountain Medical Group	Yes

All four of the county agencies there were managed by an external contractor verified compliance with the Standard requirement 12.6, by maintaining a security awareness training program in their SAQ.

Three county agencies (see Table 3) confirmed they did not have any employees that handled cardholder data, and therefore were not required to ensure that employees had taken the County's security awareness training. We found that all payment card transactions and handling and processing of cardholder data was outsourced in these three agencies.

Table 3: County Agencies Exempt from Security Awareness Training.

County Agencies Exempt From Security Awareness Training		
Agency	**Number of Employees That Handle Cardholder Data**	**Security Awareness Training Required**
Aging and Adult Services	0	Not applicable
County Assessor	0	Not applicable
County Surveyor	0	Not applicable

Three County agencies had no employees that handle cardholder data and were exempt from validating compliance with the Standard requirement 12.6.

Our audit findings and recommendations in the area of annual security awareness training were as follows:

FINDING 2.1: We found that Library Services and Parks and Recreation could not verify that all employees who had access to cardholder data, had completed security awareness training in 2017.

Risk Rating: 3 (High)

We identified 16 county agencies that had employees that were required to complete the security awareness training offered by County IS in 2017. In the prior section, we explained reasons for the other seven agencies not being required to complete the training. Table 4 shows the number of employees that handled cardholder data compared to those that completed the training in each of the 16 agencies that were required to complete the training program.

Table 4: Agencies, Security Awareness Training Program, Number of Employees Complete by September 30 Deadline.

Agencies – Security Awareness Training Program– September 30 Completion			
County Agency	**Required to Comply with Security Awareness Training?**	**No. of Employees Required to Complete Security Awareness Training**	**No. of Employees Complete by September 30th Deadline**
Animal Services	Yes	23	23
Center for the Arts	Yes	28	28[3]
Criminal Justice Services	Yes	12	12
County Clerk	Yes	18	18
Engineering and Flood	Yes	2	2
Health Department	Yes	57	57
Justice Court	Yes	13	13
Library Services	Yes	264	255
Parks and Recreation – Recreation Centers	Yes	Uncertain	69
Parks and Recreation – Golf Courses	Yes	Uncertain	
Clark Planetarium	Yes	20	20
Planning and Development	Yes	8	8
Solid Waste Management	Yes	9	9
County Treasurer	Yes	26	26
Wasatch Front Waste & Recycling District	Yes	7	7
USU Extension Services	Yes	5	5

The yellow shading shows that three agencies could not confirm that all county employees with access to cardholder data successfully completed the security awareness training by the September 30, 2017 deadline.

As shown in Table 4, we found that the Library Services Division (“Library Services”) and the Parks and Recreation Division (“Parks and Recreation”), including the Golf program, had employees who had not completed the security awareness training by the September 30, 2017 deadline. In Library Services, we found that nine employees who were required to complete the training, had not done so by September 30th. Parks and Recreation reported that a total of 69 employees had completed the training, but they could not provide an accurate count of the total number of employees who handle cardholder data, an issue we discuss in detail in the next section.

Countywide Policy 1400-7, *"Payment Card Industry Data Security Standard Policy,"* Section 3.1.5, states:

[3] Seventeen of twenty-eight employees completed a County IS approved in-house security awareness training at Center for the Arts. These temporary employees did not have a domain name to access the online web-based training application.

> *"PCI-DSS compliance requires . . . that County agencies that accept, process, transmit or store cardholder data shall provide annual security awareness training to employees that have access to cardholder data." (CWP 1400-7, 3.1.5, p. 3)*

Furthermore, **Countywide Policy 1400-7, *"Payment Card Industry Data Security Standard Policy,"* Section 5.0 Enforcement,** states:

> *"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." (CWP 1400-7, 3.1.5, p. 3)*

After discussing this issue with both Library Services and Parks and Recreation management, we found that management had overlooked the requirement for completing the security awareness training by September 30th for all employees.

RECOMMENDATION

- ***We recommend that Library Services and Parks and Recreation management ensure that all employees with access to cardholder data complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.***

FINDING 2.2: Parks and Recreation did not maintain an accurate list of the names of all employees that had access to cardholder data, and therefore required to complete the security awareness training annually.

Risk Rating: 3 (High)

The Parks and Recreation Division operates 19 recreation centers, six golf courses, and both the Wheeler Historic Farm and Millcreek Canyon toll booth, throughout the County. These facilities accept payment cards and have county employees that have access to cardholder data that is processed and transmitted. During our audit, we found that Parks and Recreation could not provide an accurate listing of employees working at these facilities who had access to cardholder data in their point of sale systems.

Parks and Recreation management provided a list of 69 employees with system access rights, but disclosed that there were additional employees, not listed or tracked, who also had the same access rights as those listed. Parks and Recreation has both regular (merit) and temporary employees who process sales transactions at many different locations. Management has not implemented a process that would track employees who have access to cardholder data, especially considering the high rate of turnover among their temporary employees.

Countywide Policy 1400-1, *"Acceptable Use Policy,"* Section 3.1.2, Access and Control, states:

> *"County agency management is responsible for granting users' access to IT resources and systems, which is limited to that which is required to do their work, and for revoking user access in a timely manner." (CWP 1400-1, 3.1.2, p. 2)*

When county managers do not require a coordinated effort to identify and track all employees that have access to cardholder data and require those employees to complete the security awareness training, then the risk that cardholder data could be misused, or the risk of a data breach are significantly increased. A data breach could have severe negative consequences for the County, including fines, litigation, and a loss of public trust.

RECOMMENDATION

- ***We recommend that Parks and Recreation management implement a process to identify all employees with access to cardholder data and require that all those employees complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.***

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 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 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 2016 Payment Card Revenue

County Agencies – 2016 Payment Card Revenues & Transactions – Categories			
Agency	**Payment Card Revenue 2016**	**Number of Payment Card Transactions 2016**	**Category**
Aging & Adult Services	$32,795	187	Human Services
Animal Services	384,431	11,976	Public Works
Assessor	11,499,627	9,036	Property Taxes
Center for the Arts	15,936,431	98,828	Community Services
Criminal Justice Services	278,075	4,337	Human Services
Clerk	714,734	16,824	Other Services
Engineering & Flood	20,274	100	Public Works
Health Department	2,468,415	27,388	Human Services
HealthyMe Clinic	43,730	1,924	Other Services
Justice Courts	842,761	6,606	Other Services
Library Services	845,150	69,460	Human Services
Parks & Rec. Centers	15,253,371	313,813	Community Services
Parks & Rec. Golf	9,241,374	165,524	Community Services
Planetarium	1,306,469	54,415	Community Services
Planning & Develop.	1,920,040	6,294	Township Services
Solid Waste Management	8,296,594	83,497	Public Works
Surveyor	58,711	307	Other Services
Treasurer	11,271,089	4,716	Property Taxes
Wasatch Front Waste Recycling	3,178,464	50,856	Public Works
USU Extension Services	30,659	370	Human Services
SMG - Salt Palace	3,357,716	207,843	Community Services
SMG - South Towne Expo	677,762	57,443	Community Services
SMG - Equestrian Park	197,948	979	Community Services
2016 Payment Card Revenues	**$87,856,620**	**1,192,723**	

Agency Responses

Agency Response – Parks and Recreation

FINDING 2.1: We found that Library Services and Parks and Recreation could not verify that all employees who had access to cardholder data, had completed security awareness training in 2017.

	AGREE/		TARGET
RECOMMENDATION(S)	**DISAGREE**	**ACTION PLAN**	**DATE**
We recommend that Library Services and Parks and Recreation management ensure that all employees with access to cardholder data complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.	Agree	Parks & Recreation will continue to use its point of sale systems to identify all employees with access to cardholder data and will continue to require all employees who gain system access that includes access to cardholder data to complete training immediately. To ensure that all employees with access to cardholder data complete the security awareness training annually, Parks & Recreation will designate a month each year during which all existing employees with access to cardholder data will be required to complete the security awareness training.	9/30/2018

FINDING 2.2: Parks and Recreation did not maintain an accurate list of the names of all employees that had access to cardholder data, and therefore required to complete the security awareness training annually.

	AGREE/		TARGET
RECOMMENDATION(S)	**DISAGREE**	**ACTION PLAN**	**DATE**
We recommend that Parks and Recreation management implement a process to identify all employees with access to cardholder data and require that all those employees complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.	Agree	Parks & Recreation will continue to use its point of sale systems to identify all employees with access to cardholder data and will continue to require all employees who gain system access that includes access to cardholder data to complete training immediately. To ensure that all employees with access to cardholder data complete the security awareness training annually, Parks & Recreation will designate a month each year during which all existing employees with access to cardholder data will be required to complete the security awareness training.	9/30/2018

Agency Response – Library Services

FINDING 2.1: We found that Library Services and Parks and Recreation could not verify that all employees who had access to cardholder data, had completed security awareness training in 2017.

RECOMMENDATION(S)	AGREE/ DISAGREE	ACTION PLAN	TARGET DATE
We recommend that Library Services and Parks and Recreation management ensure that all employees with access to cardholder data complete the security awareness training annually, as required by the PCI DSS and Countywide Policy 1400-7.	Agree	As the September 30, 2017 deadline approached, the Library was working with its full-time staff as well as numerous part-time staff to complete the training. There were two main issues that created difficulty in achieving full compliance in the allotted time frame. The first issue related to a lack of total County-wide available licenses to complete the training. Once County IT was able to acquire the needed licenses, Library staff were able to initiate the online security awareness training process. However, staff experienced a problem with the SANS software due to being unable to change their password because the key had expired (a 90-minute limit) when they tried to change their password. The response time lag for the delivery of the password change link from the SANS software became impractical and often did not arrive until the time limit had expired, resulting in user frustration. This required multiple attempts before staff were able to initiate and complete the training. Due to the varying schedules for our part-time staff, not all were able to successfully complete the training by the September 30, 2017 deadline. Shortly after the September 30th deadline, all required Library staff had successfully completed the security awareness training, except one employee who was out on extended leave due to surgery.	12/31/2017