SALT LAKE COUNTY AUDITOR'S OFFICE

SCOTT TINGLEY, CIA, CGAP
Salt Lake County Auditor

Public Report on an Information Technology Audit of

The Library Services Division

Release date: November 2019

Purpose:

To provide public information regarding the recent Audit of the Salt Lake County Library Services Division's compliance with Payment Card Industry Data Security Standards (PCI DSS). A more detailed report was issued to management in the Salt Lake County Community Services Division, the Information Technology Division (County IT), and the Library Services Division. The management report contains sensitive, security-related information that if generally available could compromise the security of systems and data. Management reports are confidential and have a protected status under provisions of the Government Records Management Act (GRAMA).

Background:

The Salt Lake County Auditor's Office recently completed an audit of the Salt Lake County Library Services Division's compliance with PCI DSS. Library Services consists of 18 libraries located throughout the County. Library Services provides the public with books, music, movies, magazines, and computers with internet access. Special programs, such as story time, classes, book clubs and art exhibits are also available.

Library Services accepts credit cards for the payment of fines and fees as well as for printing and faxing services. During the audit period, 92,881 credit card transactions were processed, with a total receipt value of $901,927.

Findings were generally related to gaps in written policies and procedures and administration of service providers. Several areas of strength were also recognized.

Audit Scope and Methodology:

PCI DSS is divided into six main goals, which are broken down into one or more requirements, for a total of 12, as seen in Table 1. Our audit work covered the SAQ submitted by Library Services for 2018 and consisted of a formal examination of security and operational processes included in the PCI DSS requirements.

Table 1. Overview of the PCI Data Security Standard. *The PCI DSS is divided into 6 main goals and 12 overarching requirements*.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Source: Payment Card Industry Data Security Standard Council

Testing procedures conducted were those set forth in the PCI SSC publication, “PCI Data Security Standard Requirements and Security Assessment Procedures.” During the audit, we examined network security configurations, observed business practices and procedures, reviewed management of service providers, and examined quarterly external vulnerability scan results.

We received a response from Library Services regarding the recommendations given, which we have included at the end of the management report. Library Services management outlined actions taken to address issues noted, the person responsible for implementing the action, and the date of completion.