SALT LAKE COUNTY AUDITOR'S OFFICE

Scott Tingley, CIA, CGAP
Salt Lake County Auditor

Public Report on an Information Technology Audit of

The Salt Lake County Justice Court's Compliance with the Payment Card Industry Data Security Standard

Report Date: January 2020

Background and Purpose:

The Salt Lake County Auditor's Office recently completed an audit of the Salt Lake County Justice Court's compliance with the Payment Card Industry Data Security Standard (PCI DSS). A detailed confidential audit report was issued to management of both the Justice Court and the Salt Lake County Information Technology Division (County IT). The full confidential audit report contains sensitive security-related information that if made generally available, could compromise the security of IT systems and data. The full confidential audit report is protected under the provisions of the Government Records Management Act (GRAMA).

The purpose of the audit was to determine if the applicable technical and operational controls required by PCI DSS were in place and operating effectively to adequately protect cardholder data. The Payment Card Industry Data Security Standard is a set of 12 requirements created and maintained by the PCI Security Standard Council to protect the public's cardholder data and help decrease the likelihood of payment card fraud.

The Justice Court's jurisdiction consists of unincorporated Salt Lake County and has the authority to adjudicate class B and C misdemeanors, violations of ordinances, small claims, and infractions. The Justice Court accepts credit and debit cards for the payment of court fines and fees. During 2018, the Justice Court processed over 7,000 payment card transactions.

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 the Justice Court for 2019 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 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 provider agreements, and examined quarterly external vulnerability scan results.

Audit Results:

We identified a total of 12 findings related to the audit objectives and issued recommendations for improvement for each of the findings. We received a response from the Justice Court and County IT regarding the recommendations given, which we have included at the end of the full confidential audit report. Justice Court and County IT management outlined action plans to address issues noted, the person responsible for implementing the action(s), and the target date for completion.

We truly appreciate the time and efforts of the employees of both the Justice Court and County IT throughout the audit. Our work was made possible by their cooperation and prompt attention given to our requests.