

## REPORT SUMMARY

### **Payment Card Industry Data Security Standard and Related Controls**

The State of Montana provides a diverse set of services, and citizens and businesses can pay for services using cash, check, direct billing, payment cards, etc. Payment cards include debit or credit cards which carry the major payment card brand logos such as Visa, MasterCard, or American Express. The State of Montana currently accepts payment cards for more than 400 services such as tuition, athletics tickets, and motor carrier permits. According to the most recent figures for fiscal year 2008, the State of Montana collected nearly \$300 million in revenues on over four million payment card transactions.

Current information suggests the average total cost of a data breach now exceeds \$7 million per organization. Cardholder data security has become a priority for the major payment card brands leading them to form their own association to establish and regulate security standards. The current version, Payment Card Industry Data Security Standard (PCI DSS) version 1.2, became effective October 1, 2008.

Our audit objective was to determine if policies and business processes at selected entities conform to specific requirements of the PCI DSS. The four entities included in the audit were selected based on revenues and transactions processed and included The University of Montana – Missoula, Montana State University – Bozeman, Montana State University – Billings, and the Montana Department of Transportation.

Payment card information is obtained by the four entities in three ways: paper-based transactions, point of sale devices, and web applications. Through the state term contract for credit card processing services, agencies are given discretion regarding which method(s) work best for their needs. We reviewed all three methods of obtaining payment card information for all four entities. We interviewed management and staff within individual departments and discussed procedures for handling payment card information. In addition to interviews, we conducted observations of business processes and the office environments where payment card transactions are conducted and cardholder data is stored.

Overall, we found management and staff are concerned for the security of cardholder data. However, conformity with the specific requirements of the PCI DSS can be strengthened. This report discusses our findings and includes two recommendations addressing the need to strengthen policy and cardholder data security.