INTRODUCTION

Many, if not most, of the State's agencies accept payment cards (i.e., credit cards, debit cards, charge cards, etc.) to collect money for taxes, licenses, other services and goods. They do so to accommodate the wishes of the constituency and to make the collection process more efficient and economical for the State.

These transactions and the systems that process them are constantly under attack by those attempting to acquire information that may be used for illicit purposes. This information includes personal data such as Social Security Numbers, dates of birth, addresses, bank account numbers, medical data, etc.

To combat these attacks, the major credit card issuers created the Payment Card Industry Security Standards Council (hereinafter referred to as PCI).

The PCI requires all entities that store, process or transmit cardholder data to maintain payment security. This requirement extends to the State of Arizona, its agencies and those individuals or organizations with whom the State contracts to store, process or transmit cardholder data.

The PCI communicates its requirements through its technical and operational security standards. Compliance with these standards is mandatory and failure to comply with them may result in an entity's being barred from accepting, processing, storing or transmitting payment card transactions and/or data.

Three agencies within the Government of the State of Arizona are principally responsible for the oversight and administration of PCI requirements:

- *The Office of the State Treasurer* (OST). Credit card contracts fall within the statutory jurisdiction of the OST. The OST has, therefore, overall responsibility for compliance with PCI compliance.

- *The Office of the Secretary of State* (SOS). A division of the SOS, the Arizona State Library, Archives and Public Records (LAPR), is responsible for records retention policies and practices for State Government.

- *The Arizona Department of Administration* (ADOA). Several divisions of ADOA are involved with PCI compliance. The Arizona Strategic Enterprise Technology (ASET) division is responsible for statewide oversight of information technology (IT) hardware and software. The State Procurement Office (SPO) is responsible

for letting IT contracts. The General Accounting Office (GAO) issues accounting policies and has jurisdiction over its automated accounting system.

At its highest level, compliance with the PCI standards requires:

- Hardening payment card processing systems—hardware and software—to protect them from attacks; hardening standards must be applied to all newly acquired devices prior to their being added to the common desktop environment.

- Issuing policies and procedures—including, but not limited to, this section of SAAM—to be followed by all those dealing with the processing of payment cards.

- Mandating and administering appropriate, periodic training of all those who produce software that processes, stores or forwards payment card data, as well as those who handle such data and manage those who handle such data.

- Passing an annual audit of compliance with the PCI standards.

It is to facilitate the accomplishment of these goals that this policy is issued.

Failure to comply with the PCI standards may result in dire consequences for State and its agencies, including substantial fines and the suspension or termination of the State's or an agency's merchant status (i.e., authorization and ability to use payment cards to expedite collections).

Even more calamitous would be the illicit acquisition of cardholders' data because of the State's failure to properly safeguard these data. Such an event could result in severe economic and reputational damage to the State.

Cardholder data includes any personally identifiable data associated with a cardholder such as account number, expiration date, card validation code, etc.

In the context of this section of SAAM, a payment card refers to either a credit card or a debit card used by an individual or organization to remit a payment to the State or one of its agencies. It does not refer to the P-Card, CTA, ETC or other procurement or payment cards used by the State or its agencies to effect a purchase or payment.

Payment card processing refers to the use of any application, device or manual procedure to accept remittances to the State for services, goods, taxes, fines, etc.

This is the first of what may be a series of SAAM sections dealing with PCI compliance.

POLICY

1. Agencies that accept payment cards must comply with the policies and/or procedures and/or directives issued by the OST, SOS or ADOA relating to PCI compliance.

2. State-operated or State-contracted environments that process or transmit cardholder data must comply with PCI standards (a link to the PCI website containing those standards is provided later herein).

3. Access to cardholder data must be controlled. Controlling access includes:

3.1. Limiting access to cardholder data to those with a valid business purpose for access to such data.

3.2. Restricting physical access to computer hardware that processes or transfers cardholder data to those individuals with a valid business purpose for accessing such data.

3.3. Password protecting access to computer files and programs that process or transfer cardholder data.

3.4. Tracking and monitoring access to computers, networks and websites that process or transfer cardholder data.

3.5. Testing, on a periodic basis, but no less than annually, all controls required and established to protect cardholder data.

4. Agencies must adopt policies and procedures that ensure PCI compliance.

4.1. An agency may elect to produce and publish general policies and procedures relating to PCI compliance that incorporate by reference policies and procedures issued by the PCI, that can be found on the PCI website listed hereinbelow, and/or the OST, ASET, LAPR or the GAO.

4.2. In addition to general agency policies relating to PCI compliance, an agency must produce and publish policies and procedures specific to its operating environment as it relates to the processing and transmitting of payment card data.

4.3. An agency's payment card operating environment includes, but is not limited to, elements such as:

4.3.1. Websites, operated by the agency or by a third-party processor, collecting remittances by way of payment card.

4.3.2. Telephonic acceptance of payment card data must be limited to call centers with proper data disposal processes and policies that prevent the storage of certain credit card data.

4.3.3. Processing payment card data by way of dedicated payment card terminal.

5. Training of personnel involved in the processing of payments cards, whatever their role, is mandated by PCI.

5.1. The State will annually conduct required training based upon an employee's role or roles.

5.2. This training will be administered by the OST, ASET and/or other organizations of or contracted by the State.

5.3. Agencies will be required to participate in the effort to identify relevant staff and their roles.

5.4. Agency management will be required to assure that relevant staff attend and successfully complete requisite training.

6. No third-party application that processes payments or interacts with any Payment Processor may be hosted on State-owned IT without compliance with ADOA security requirements, policies and standards. All cloud hosted services are required to complete and comply with the "Moderate" Arizona Baseline Security Controls available on the ADOA security requirements, policies and standards website.

7. PCI requires that an annual audit be conducted to ensure compliance with its standards.

7.1. PCI auditors will be engaged by the State.

7.2. Agencies must cooperate with PCI auditors during the audit.

7.3. Agencies must cooperate in correcting any deficiencies reported by the PCI auditors on a timely basis.

7.4. It is to be noted that a single deficiency may result in the termination or suspension of the State's or an agency's ability to process payment cards.

8. Logs documenting compliance with PCI standards must be retained by agencies. Examples of such logs include, but are not limited to:

8.1. Attendance lists recording staff attendance at required training.

8.2. Sign-in sheets for those entering a data center.

8.3. Computer-generated logs reflecting access to systems or applications.

9. Agencies will receive electronic notification of PCI events (audits, training, etc.) by the GAO, OST, LAPR, ASET and/or SPO.

10. Except with the written permission of the OST, agencies must use one of the following to process their credit card receipts:

10.1. The State's web portal, maintained by ASET.

10.2. The online facilities offered by the State-contracted bank.

11. Additional, more detailed information relating to PCI can be found on the following websites:

11.1. Payment Card Industry Security Standards Council

https://www.pcisecuritystandards.org/

11.2. Office of the Secretary of State: Library, Archives and Public Records

https://www.azlibrary.gov/arm

11.3. Office of the State Treasurer

http://www.aztreasury.gov/

11.4. Arizona Department of Administration:

11.4.1. Arizona Strategic Enterprise Technology

https://aset.az.gov/

11.5. General Accounting Office

https://gao.az.gov/

11.6. State Procurement Office

https://spo.az.gov/