Report on PCI DSS Audit #15-123 and PCI DSS Integrated Audit #15-208

We have completed our audit of the Payment Card Industry Data Security Standard (PCI DSS). This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures on a global basis. It provides a baseline of technical and operational requirements designed to protect account data that applies to all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. Below is a general overview of the 12 PCI DSS requirements:

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Protect all systems against malware and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
The security requirements of PCI DSS apply to all system components included in or connected to the cardholder data environment. The cardholder data environment is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data. System components include network devices, servers, computing devices, and applications.

**EMV Standard**
In the wake of numerous large-scale data breaches and increasing rates of counterfeit card fraud, U.S. card issuers have migrated to a new technology as of October 1, 2015 to protect consumers and reduce the costs of fraud. Europay, MasterCard, and Visa (EMV) is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. For merchants and financial institutions, the switch to EMV involves adding new in-store technology and internal processing systems, as well as complying with new liability rules. For consumers, it involves activating new cards and learning new payment processes.

Historically, UTHealth and UTP have experienced low chargeback rates as a percentage of overall sales (less than 1% for both entities for 2013 and 2014). A strategy is in place to rollout leased EMV equipment for new sites as well as replace older terminals on an as-needed basis. This strategy is in alignment with the Shared Business Operations unit of UT System and other UT entities. In addition, UTP is currently reviewing options related to revenue cycle including the credit card module, which would require a change in credit card payment equipment.

**Credit Card Receipts Procedure**
Treasury’s Credit Card Receipts Procedure defines and outlines the policy with regard to the acceptance and handling of credit card transactions. It is UTHealth’s policy to not process, transmit, or store any cardholder data on its servers (or paper storage) which indicates the card number, the 3 or 4 digit security number, or any PIN numbers. UTHealth’s record of payment only includes the last four digits of a card number for reference purposes. As such, UTHealth’s network would not be subject to the security requirements of PCI DSS.

Cardholder data must be expeditiously destroyed by crosscut shredder or placed in locked, limited access loss prevention “to be shred” storage containers which are approved by Treasury. Credit card processing devices are required to be inspected on a daily basis to identify any signs of tampering such as forced opening, missing or changed security labels or markings, removal of cables, scratches, or the addition of foreign device into or onto the equipment or replacement by a difference device. If tampering is suspected, employees are instructed to stop processing payments through the device, limit access, refrain from touching the device, and immediately contacting UT Police and Treasury.

**ITPOL-014 PCI Digital Security Standards**
Per ITPOL-014 PCI Digital Security Standards (ITPOL-014), UTHealth follows the best practices for protecting cardholder information as defined by PCI DSS, specifically relating to information used in the processing, storage, and transmission of cardholder information. UTHealth must adhere to these standards to limit its liability and to continue processing credit card payments. All UTHealth merchants must be registered through the Finance Office before accepting and processing credit card information. An annual Self-Assessment Questionnaire (SAQ) is completed by the Office of Information Security in conjunction with the Finance Office and the
Office of the CIO. The storage and destruction of PCI DSS-related records must meet or exceed UTHealth Records Retention policies for sensitive information.

OBJECTIVES

The objective of this audit was to determine compliance with requirements of PCI DSS.

SCOPE AND METHODOLOGY

Through a review of PCI DSS compliance statements, online credit card click-through points, service provider agreements, and controls around credit card terminals, Auditing and Advisory Services (A&AS) performed an audit of PCI DSS compliance.

A&AS noted that IT Security is currently working on a project to implement a virtual network of credit card transactions for the parking systems by the end of October 2015. The new private network will bypass the unsupported operating systems hosted by the vendor at a remote site in order to ensure PCI DSS compliance. As this project is ongoing, it was not included in the scope of our audit.

AUDIT RESULTS

PCI DSS Compliance

PCI DSS section 12.8.4 requires the monitoring of service providers' PCI DSS compliance at least annually. Treasury informed A&AS that the following vendors provide credit card processing for UTHealth:

- ACI Worldwide/Official Payments - processes online tuition payments, conference attendee/vendor payments, etc.

- Texas NICUSA LLC (Texas.Gov) - processes payments for a range of services, including payments to the Bursar’s Office, continuing education, etc.

- Global Payments Direct, Inc. - processes payments for all credit card terminals at UTHealth, including UTP clinics.

For each credit card processing vendor, A&AS obtained evidence of PCI DSS compliance for 2015. We noted that Treasury obtains evidence of PCI DSS compliance from credit card processing vendors during the due diligence period; however, ongoing monitoring of PCI DSS compliance is not performed.

Recommendation #1:
We recommend that Treasury obtain evidence of PCI DSS compliance for all credit card processing vendors on an annual basis. This should also include “middle-man” credit card processing vendors.

Management's Response:
We agree with recommendation and will obtain evidence of PCI DSS compliance for all credit card processing vendors (including “middle-men”) on an annual basis.
Credit Card Terminals
A&AS obtained the list of UTHealth and UTP locations utilizing credit card terminals from Treasury and judgmentally selected ten locations for testwork. After consulting the Credit Card Receipts Procedure, we visited each location, examined the credit card terminals, and interviewed onsite personnel about the processes and knowledge surrounding their use. The following issues were noted:

- Personnel at 7 locations were not aware of the requirement for physically inspecting the credit card terminals prior to opening for business.
- Personnel at 6 locations were not aware of the procedures required when an individual claims to be a repair person and requests access to a credit card terminal.
- Personnel at 5 locations were not aware of how to handle credit card payments if terminals are inoperable or phone lines are down.
- Personnel at 4 locations were not aware of the procedures required when tampering of credit card terminals is suspected.
- Three locations use the Hypercom T-7 Plus terminal, which is capable of storing and displaying full credit card numbers.
- Personnel at 2 locations were not aware of the requirement for securing credit card terminals during non-business hours.
- Personnel at 2 locations disclosed that they have received unsolicited credit card numbers via email and that they delete the emails in these cases.
- Two locations did not restrict access to credit card terminals during business hours.
- Two locations reported that the clinic staff has not received formal training on credit card processing.
- One location utilizes an application (Raiser’s Edge) to record and transmit credit card numbers through UTHealth’s network to a cloud vendor site.
- One location maintained four additional credit card terminals that were not included on the inventory listing provided by Treasury.
- One location maintains a fax machine for collecting credit card information. The fax machine has the capability of electronically storing incoming faxes (including credit card numbers); however, this functionality was turned off at the time of our site visit.
- One location uses a carbon copy receipt form for manual credit card processing.

Recommendation #2:
We recommend that Treasury and UTP perform an analysis to determine whether all applicable personnel have received formal training around internal policies dealing with PCI DSS standards. Based on the results of the analysis, Treasury and UTP should consider whether new or additional training is warranted.

Management’s Response 2a:
We agree with the recommendation and will perform an analysis to determine whether all applicable personnel at UTHealth have received formal training around internal policies dealing with PCI DSS standards. Based on the results of our analysis, we will determine whether any new or additional training is warranted. If additional training is warranted, Treasury will work
with the necessary UTHealth departments to design and disseminate the materials to key personnel in the most effective manner – i.e., online training, in-person training, FAQ communication via targeted email, etc.

Responsible Party: James Vitt
Implementation Date: May 31, 2016

Management’s Response 2b:
We agree with the recommendation and UTP Operations (with UTHealth Treasury oversight) will perform an analysis to determine whether all applicable personnel at UTP have received formal training around internal policies dealing with PCI DSS standards. Based on the results of our analysis, we will determine whether any new or additional training is warranted. If additional training is warranted, Treasury will work the UTP Operations to design and disseminate the materials to key personnel in the most effective manner – i.e., online training, in-person training, FAQ communication via targeted email, etc.

Responsible Party: James Vitt and Andrew Casas
Implementation Date: May 31, 2016

Recommendation #3:
We recommend that Treasury update its policies and procedures to provide guidance around:

- Situations in which credit card terminals are inoperable or phones lines are down.
- Collection of credit card information via form templates and faxes.
- Unsolicited credit card information received via email.
- Approvals required before the activation of credit card payment modules within existing applications.

Management’s Response:
We agree with the recommendation and will update the Treasury policies and procedures to provide guidance around situations in which credit card terminals are inoperable or phones are down, the collection of credit card information via form templates and faxes, unsolicited credit card information received via email, and the approvals required before the activation of credit card payment modules within existing applications.

Responsible Party: James Vitt
Implementation Date: May 31, 2016

Recommendation #4:
We recommend that Treasury conduct an inventory of all credit card terminals, including the four additional terminals noted above that were not in Treasury’s inventory records, and determine if a periodic inventory of all components is warranted. Additionally, we recommend that the Hypercom T-7 Plus terminals and any other older credit card terminals be replaced or upgraded to be PCI DSS compliant.
**Management’s Response:**
We agree with the recommendation and will conduct an inventory of all credit card terminals and determine if a periodic inventory of all components is warranted. Additionally, we will either replace or upgrade the Hypercom T-7 Plus terminals to ensure they are PCI DSS compliant. Treasury will explore the possibility of utilizing the Capital Asset Management Inventory team in this endeavor.

*Responsible Party:* James Vitt  
*Implementation Date:* January 31, 2016

**Recommendation #5:**
We recommend that the Raiser’s Edge application be configured to meet PCI DSS requirements.

**Management’s Response:**
We agree with the recommendation and will no longer enter credit card numbers into the Raiser’s Edge application. If we decide to take advantage of this functionality in the future, we will work with IT Security to configure the application to be in compliance with PCI DSS requirements.

*Responsible Party:* Lisa Christison and Amar Yousif  
*Implementation Date:* October 12, 2015

**Online Credit Card Payments**
It is UTHealth’s policy to not store any personal credit card information on its servers which indicates the card number, the 3 or 4 digit security number, or any PIN numbers. UTHealth’s record of payment may not include more than the last four digits of an account number for reference purposes.

A&AS worked with Finance to identify the online credit card click-through points at UTHealth. A total of 23 were identified including online credit card payment of tuition, fees, continuing education, and conference enrollments. A&AS verified that each click-through point links to an external credit card vendor site (not UTHealth’s servers). No exceptions were noted.

**Agreements & Policies**
PCI DSS requires that agreements with service providers contain an acknowledgement (Acknowledgement) that the service provider is responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of UTHealth, or to the extent that they could impact the security of UTHealth’s cardholder data environment. The exact wording of the Acknowledgement depends on the agreement, the details of the service being provided, and the responsibilities assigned to each party. Additionally, the wording of the PCI annual compliance statement could serve as this Acknowledgement if applicable.

A&AS obtained the Texas NICUSA, LLC (Texas.Gov) and Official Payments Corporation (ACI) agreements and verified that each contains the required Acknowledgement. The agreement between UTHealth and Global Payments, Inc. (Global Payments) is included in a UT system-wide agreement that we were unable to obtain; however, the Acknowledgement is implied in the most recent annual PCI compliance statement obtained by A&AS. No exceptions were noted.
PCI DSS also requires:
- A security policy be established, published, maintained, and disseminated.
- Security policies and operational procedures for restricting physical access to cardholder data be documented, in use, and known to all parties.
- The security policy be reviewed at least annually and updated when the environment changes.

A&AS obtained ITPOL-14 and the Credit Card Receipt Procedure and verified that they are posted on the UTHealth intranet and address the restriction of physical access to cardholder data. Additionally, we confirmed that ITPOL-14 is reviewed and updated on an annual basis. No exceptions were noted.

CONCLUSION

UTHealth is in compliance with the majority of PCI DSS requirements; however, recommendations were made in order to address compliance gaps, including the annual monitoring of vendors for PCI DSS compliance, providing new and/or additional training, the updating of Treasury policies and procedures, conducting an inventory of all credit card terminals, upgrading or replacing older credit card terminals, and ensuring that the Raiser’s Edge application can meet PCI DSS requirements.

We would like to thank the Treasury and IT Security staff and management who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

cc: Audit Committee
Michael Tramonte
Richard Miller
Amar Yousif
Andrew Casas
Lisa Christison
Cathy Findley
James Vitt
Tracy Fry-Longoria
Donna Valenzuela

Audit Manager: Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned: Lieu Tran
Issue Date: October 27, 2015