The University of Texas Rio Grande Valley

Brownsville • Edinburg • Harlingen

THE UNIVERSITY OF TEXAS RIO GRANDE VALLEY
OFFICE OF AUDITS & CONSULTING SERVICES

Payment Card Industry Data Security Standards

Report No. 16-06

The University of Texas Rio Grande Valley

Brownsville • Edinburg • Harlingen

July 15, 2016

Dr. Guy Bailey, President
The University of Texas Rio Grande Valley
2102 Treasure Hills Blvd., Suite 3.115
Harlingen, TX 78550

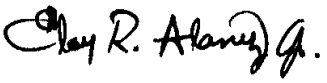
Dear Dr. Bailey,

As part of our fiscal year 2016 Audit Plan, we have completed an audit on the Payment Card Industry Data Security Standards (PCI DSS) for The University of Texas Rio Grande Valley (UTRGV). The objective of this audit was to provide an assessment of UTRGV's compliance with PCI DSS requirements. The scope of this audit consisted of identifying current UTRGV merchants, hosting providers, and payment processors. We selected the UTRGV merchants with the greatest volume of processing payment cards and tested these merchants in the areas of protecting cardholder data and regular monitoring and testing of networks where cardholder data is housed.

Overall, we concluded that UTRGV protected stored and transmitted cardholder data; however, it was not fully compliant with specific PCI DSS requirements such as quarterly scans conducted by an approved scanning vendor. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,



Eloy R. Alaniz, Jr., CPA, CIA, CISA
Chief Audit Executive

cc: Chris King, Athletics Director
UTRGV Internal Audit Committee
UT System Audit Office
Governor's Office of Budget, Planning and Policy
Sunset Advisory Commission
State Auditor's Office
Legislative Budget Board

Table of Contents

The University of Texas Rio Grande Valley
Brownsville • Edinburg • Harlingen

Payment Card Industry Data Security Standards

EXECUTIVE SUMMARY

Protecting credit card information is a major concern for all entities that accept credit card payments. The University of Texas Rio Grande Valley (UTRGV) accepts credit and debit card payments for tuition and a variety of services it provides. It is the responsibility of the University to protect the information it collects to process these payments, and failure to safeguard payment card data may result in loss of confidence, legal costs, fines and penalties, and loss of ability to accept credit cards.

The payment card industry has come up with ways to mitigate the risk associated with payment card processing. Major credit card companies have joined to create the Payment Card Industry (PCI) Security Standards Council. It was created to encourage and enhance payment card data security and to promote consistent data security measures. To do this, it created the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a baseline of technical and operational requirements designed to safeguard payment card data.

PCI DSS is a group of six goals and 12 accompanying requirements. The principles are as follows:

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

The objective of this audit was to provide an assessment of UTRGV's compliance with PCI DSS requirements. The scope of this audit consisted of identifying current UTRGV merchants, hosting providers, and payment processors. We selected the UTRGV merchants with the greatest volume of processing payment cards and tested these merchants in the areas of protecting cardholder data and regular monitoring and testing of networks where cardholder data is housed.

Overall, we concluded that UTRGV protected stored and transmitted cardholder data; however, it was not fully compliant with specific PCI DSS requirements such as quarterly scans conducted by an approved scanning vendor.

Payment Card Industry Data Security Standards

BACKGROUND

The University of Texas Rio Grande Valley (UTRGV) was created by the Texas Legislature on December 7, 2012, and it combined the resources and assets of The University of Texas-Pan American (UTPA) and the University of Texas-Brownsville (UTB) effective September 1, 2015.

UTRGV enrolled its first class in the fall of 2015 and the majority of the revenue received comes from tuition and services provided to students. Students and individuals that receive services from the University have the option to pay with credit and debit cards. This option involves collecting payment card information and processing it for payment. Data used in this process needs to be protected from being used to commit fraudulent activities.

Major credit card companies have joined efforts to assist in the security of payment card information. They have created the Payment Card Industry Security Standards Council. Its founding members include: American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. This council provides resources to safeguard payment card data. One of the resources it provides is the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of requirements that help mitigate the risks associated with handling payment card data. Below is a high level overview of PCI DSS.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	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. Protect all systems against malware 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. Identify and authenticate access to system components
	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

AUDIT OBJECTIVE

The objective of this audit was to provide an assessment of UTRGV's compliance with PCI DSS requirements.

AUDIT SCOPE & METHODOLOGY

The scope of this audit consisted of identifying current UTRGV merchants, hosting providers, and payment processors. We selected the UTRGV merchants with the greatest volume of processing payment cards and tested these merchants in the areas of protecting cardholder data and regular monitoring and testing of networks where cardholder data is housed. To accomplish the audit objective, we performed the following:

- Gained an understanding of processes that collect card payments.
- Gained an understanding of applicable PCI DSS requirements.
- Requested guidance from the University of Texas System - Office of Shared Business Operations.
- Interviewed the Associate Comptroller for Treasury Operations and Information Technology staff.
- Interviewed staff from the Office of the Chief Information Security Officer.
- Tested PCI DSS requirements.

This audit was conducted in accordance with guidelines set forth in The University of Texas System's Policy 129 and *The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing.*

AUDIT RESULTS

PCI DSS Requirements

According PCI, not protecting payment card data may bring potential liabilities. Some of these liabilities may include:

- Loss of trust
- Diminished sales
- Cost of reissuing new payment cards
- Fraud losses
- Higher subsequent costs of compliance
- Legal costs, settlements and judgments
- Fines and penalties
- Termination of ability to accept payment cards

Because of these potential liabilities it is very important that payment card information is protected. A robust and comprehensive PCI DSS program minimizes the likelihood of losing payment card data and facing the aforementioned liabilities. A PCI DSS program includes responsibilities that must be clearly defined. PCI compliance should be achieved via a partnership between finance and information technology. At the time of this audit, it was understood that ownership of the PCI DSS process needed to be shared by the Information Technology and Treasury Operations staff. However, ownership and the responsibilities for PCI compliance have not been clearly defined by UTRGV's executive management.

Recommendation:

1. The Vice President for Finance and Public Policy should work with Information Technology to define roles and responsibilities for ensuring PCI DSS compliance.

Management Response:

1. Management concurs with the recommendation noted above. The Office of Finance and Public Policy, CIO, and CISO will develop and implement policy guidelines with the goal of ensuring that business processes for accepting electronic payments comply with the 12 components of PCI DSS. Each of the 12 components has undergone an initial review and the office of Treasury, CIO, or CISO, or a combination of these offices have been identified as the responsible party for each of the 12 PCI DSS components.

   CISO, in collaboration with CIO and Treasury, will develop and maintain an information security policy to ensure that strong controls that are appropriately integrated with the University's financial and information technology systems are put in place.

Implementation Date:

November 30, 2016

The level of protection on payment card information depends on the merchant[1] level. UTRGV has 20 merchant account numbers[2]. Each department (merchant) that processes payment cards has two merchant account numbers. The table below lists all UTRGV merchants that process payment cards.

[1] PCI defines a merchant as any entity that accepts payment cards bearing the logos of any of the five members of Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

[2] A merchant account number is a bank account that allows businesses to accept payment cards.

UTRGV Merchants that Process Payment Cards	
Online Payments	Student Union Game Room
Bursar	Theatre Arts
Coastal Studies	Athletics
Library	Student Union
Student Health	Parking and Transportation

In addition to the merchants above, UTRGV has businesses that are contracted through Campus Auxiliary Services. These entities do not have UTRGV merchant account numbers, except the game room in the Student Union.

Merchant level is based on the number of payment card transactions per year. There are four merchant levels and they are determined by credit card companies. The table below describes Visa's merchant levels and the requirements needed to comply with PCI-DSS.

Visa PCI Compliance Validation[3]		
Category	**Criteria**	**Requirements**
Level 1	Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region	**Every year:** • File a Report on Compliance by Qualified Security Assessor or Internal Auditor if signed by officer of the company. We recommend the internal auditor obtain the PCI SSC Internal Security Assessor certification. • Submit an Attestation of Compliance Form **Every quarter:** • Conduct a quarterly network scan by an Approved Scan Vendor
Level 2	1 to 6 million Visa transactions annually across all channels	**Every year:** • Complete a Self-Assessment Questionnaire • Submit an Attestation of Compliance Form **Every quarter:** • Conduct a quarterly network scan by an Approved Scan Vendor
Level 3	20,000 to 1 million Visa e-commerce transactions annually	**Every year:** • Complete a Self-Assessment Questionnaire • Submit an Attestation of Compliance Form **Every quarter:** • Conduct a quarterly network scan by an Approved Scan Vendor
Level 4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	**Every year:** • Complete a Self-Assessment Questionnaire • Submit an Attestation of Compliance Form **Every quarter:** • Conduct a quarterly network scan by an Approved Scan Vendor

[3] **Source:** https://usa.visa.com/support/small-business/security-compliance.html

Due to UTRGV's first year of operations and lack of payment card history, level 4 was recommended by UT System's Office of Shared Business Operations. Level 4 is the lowest PCI DSS protection level, and it is adequate for UTRGV. For the lowest level of protection, PCI recommends an annual self-assessment, but requires quarterly network scans conducted by a PCI DSS approved scanning vendor. The self-assessment is optional unless required by acquirer[4]. UTRGV's acquirer, Global Payments, requires an annual self-assessment. UTRGV had neither completed a self-assessment nor had it conducted quarterly network scans by a PCI DSS approved scanning vendor.

Recommendation:

2. The Associate Comptroller for Treasury Operations should initiate and work with Information Technology to complete a PCI DSS self-assessment. A self-assessment needs to be performed on an annual basis or when a major change to UTRGV's payment card processing environment occurs.

Management Response:

2. Management concurs with recommendation and will set guidelines to ensure that the PCI DSS self-assessment questionnaires are completed on an annual basis or when a major change to UTRGV's payment card processing environment occurs.

Implementation Date:

July 31, 2016

Recommendation:

3. The Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) should coordinate quarterly network security scans with a PCI DSS approved scanning vendor. Scans should meet PCI DSS requirements.

Management Response:

3. The CIO and CISO will work with Treasury and Global Payments to define the scanning requirements and based on this will identify and secure the services of an approved PCI scanning vendor. Will also work with the CISO's office to update security procedures to capture scanning needs if required.

[4] According to PCI an acquirer is an "entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance."

Implementation Date:

December 31, 2016

Service Providers[5]

UTRGV partners with payment card processing service providers called CORE Business Technologies (CORE), MICROS Systems (MICROS), and Class Software from Active Network.

CORE services two UTRGV merchants, online payments and the Bursar's Office. These services include a web portal for students to pay tuition, fees, and services and a cashiering system used by the Bursar's Office.

MICROS primarily provides payment card services to Campus Auxiliary Services. These are contracted services that include beverage vending, food services, snack vending, etc. Entities that make up these services do not have UTRGV merchant account numbers, except the game room in the Student Union.

The Wellness and Recreational Sports Complex (WRSC) outsources their payment card processing. Their card processing is part of Class Software from Active Network. This software helps the WRSC manage recreation activities, including registration, scheduling, memberships, and point-of-sale. The payment card process is included in the point-of-sale module.

We selected CORE and MICROS for testing because they both house credit card information in UTRGV computing facilities. For this test, we verified that the service provider's software was on the list of PCI validated payment applications. Software applications used by UTRGV were on the list of PCI validated payment applications; however, the software version numbers listed could not be independently verified or did not match the versions used by UTRGV.

The version number for CORE's iPayment Revenue Portal did not have version information. Therefore, Information Technology had to contact CORE to provide the version number. The number provided by CORE was on the list of PCI validated payment applications.

The MICROS application is listed on the list of PCI DSS validated payment applications. However, the version number of 5.0 is not listed. The PCI DSS list only showed versions: 4.12, 5.2, and 5.4. We performed additional research and determined that version number 5.0 was PCI-DSS compliant.

[5] PCI defines service providers as business entities that are not payment brands, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.

We also verified that service providers had written agreements with UTRGV that included service providers' acknowledgements of their responsibility for securing data in their possession. CORE's and MICROS' contracts with UTRGV included an acknowledgement of their responsibility for securing data in their possession.

Finally, we tested whether UTRGV maintained a program to monitor service providers for compliance with PCI DSS at least annually. At the time of this audit, UTRGV had requested CORE's and MICROS' PCI DSS compliance information.

Protect Stored Cardholder Data

The main purpose of PCI DSS is to protect cardholder data. In this section we tested key PCI DSS requirements from section 3 - protect stored cardholder data. We tested cardholder data stored in hardware housed in UTRGV computing facilities and selected CORE and MICROS for testing. Cardholder data in these systems was tested for the following PCI DSS requirements:

- 3.2 - Do not store sensitive authentication data after authorization.
- 3.3 - Mask the payment card number (the first six and last four digits are the maximum number of digits to be displayed).
- 3.4 - Render payment card number unreadable anywhere it is stored.

CORE and MICROS met the PCI DSS requirements tested.

CONCLUSION

Overall, we concluded that UTRGV protected stored and transmitted cardholder data; however, it was not fully compliant with specific PCI DSS requirements such as quarterly scans conducted by an approved scanning vendor.

Norma L. Ramos

Norma Ramos, CIA, CGAP
Director

Isabel Benavides

Isabel Benavides CIA, CGAP, CFE
Assistant Director

Jose A. Gomez

Jose Gomez, MS, CISA
Senior Information Technology Auditor