

UNT Credit/Debit Card Merchant Handbook



University of North Texas

May 2009

Volume 1, Issue 2

STUDENT ACCOUNTING & UNIVERSITY CASHIERING SERVICES

Table of Contents

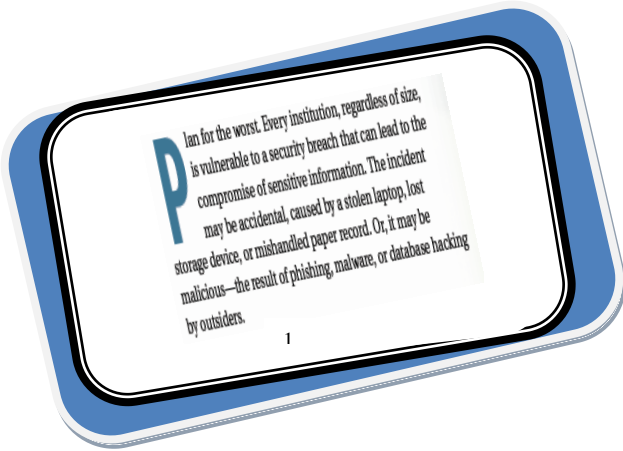
The Purpose of the Handbook	1
General Overview	2
How will UNT comply with PCI DSS?	4
What is my Validation Type?	5
Responsibility of the Dept ID/ Proj ID Holder	8
Responsibility of Dept. ID/Proj ID.....	10
And Department Designee.....	10
Segregation of Duties.....	11
Cardholder Data Compromised	12
Non-Compliant UNT Merchant.....	13
Protecting Credit/Debit Card Information	15
Credit/Debit Card Processing	17
Commerce Manager	18
Disputes/Chargebacks.....	19
Credit/Debit Card Deposits	20
Credit/Debit Card Refunds	20
Credit/Debit Card Sanctions	21
Handouts/Reference websites	23

The Purpose of the Handbook

The UNT Credit/Debit Card Merchant Handbook contains

guidelines and policies for UNT Credit/Debit Card Merchants.

Departments that accept credit/debit card payments should become familiar with the guidelines and policies listed with this handbook.



Each UNT Merchant must be

PCI DSS compliant. Working with their Departmental Network Manager, CITC Security Team and Student Accounting and University Cashiering Services, each department will be able to complete the appropriate questionnaire and scan, if required, in order to attain compliance. This compliance must be renewed yearly.

The UNT Credit/Debit Card Merchant Handbook and the yearly training will be updated as new requirements and changes occur. This handbook and the annual training should be considered a guide for learning best practices for the university.

General Overview

Student Accounting and University Cashiering Services is responsible for managing all aspects of establishing credit/debit card merchants on campus and the processing of credit/debit card transactions. See UNT Policy 2.2.31

http://www.unt.edu/policy/UNT_Policy/volume2/2_2_31.html

CISP is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.

In 2004, the CISP requirements were incorporated into an industry standard known as Payment Card Industry (PCI) Data Security Standard (DSS) resulting from a cooperative effort between Visa and MasterCard to create common industry security requirements. Visa Inc. maintains data security compliance programs endorsing the PCI DSS.

CISP compliance is required of all merchants, payment applications and service providers that store, process or transmit credit/debit cardholder data.

The PCI Security Standards Council ("PCI SSC") owns, maintains and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Visa Inc, however, continues to manage all CISP compliance enforcement and validation initiatives. In addition, the former QDSC (Qualified Data Security Company) Program has also transitioned to the PCI SSC. Please refer to the [PCI DSS](#) page for more information.

Following PCI DSS requirements is critical and can assist in preventing a security breach. If credit/debit card data is compromised and the university is out of compliance with PCI DSS, the university could be responsible for significant fines, the cost of re-issuing all cards associated with the compromise and permanently prohibited from processing credit/debit cards.

It is the responsibility of Student Accounting and University Cashiering Services to provide UNT merchants the information required to remain compliant with PCI DSS. However, it is the responsibility of the Dept. ID/Proj ID holder to insure their department is following the established policies and procedures. Student Accounting and University Cashiering Services will provide annual training to insure departments receive the current information for PCI compliance.

The PCI DSS offers a single approach to safeguarding sensitive data for all card brands. Other card companies operating in the U.S. have also endorsed the PCI DSS within their respective programs. Using the PCI DSS as its framework, Visa's compliance program provides the tools and measurements needed to protect against cardholder data exposure and compromise. The [PCI DSS](#) consists of twelve basic requirements categorized as follows:

PCI Data Security Standard	
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to 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	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

**Source: Security Standards Council*

How will UNT comply with PCI DSS?

- Student Accounting and University Cashiering Service will provide credit/debit card merchant training annually.
 - Dept ID/Proj ID Holders MUST complete.
 - Department Designees MUST complete. (Department Designees is anyone in your department who can process credit card transactions.)

- Merchants will complete PCI Self-Assessment Questionnaire annually with the assistance of their Network Manager.
 - Must be completed by each merchant (location)

- Self-Assessment Questionnaires are based upon SAQ Validation Type (see chart below)

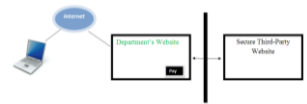
Type 1	Card-not-present (ecommerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants	A
Type 2	Imprint-only merchants with no electronic cardholder data storage	B
Type 3	Stand-alone dial-up terminal merchants, no electronic cardholder data storage	B
Type 4	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage	C
Type 5	All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ	D

**Source: Security Standards Council*

What is my Validation Type?

Type 1 Merchant, SAQ A (11 question questionnaire)

- For Card-not-present merchants only
 - E-commerce, MOTO (Mail Order/Telephone Order)
 - Never applies in a face-to-face POS environment
- Card processing is outsourced
 - No cardholder data stored, processed, or transmitted on your systems
- Third party confirms it is PCI compliant
- Only paper records, **not** received electronically
- No cardholder data is stored electronically



Type 2 Merchant, SAQ B (24 question questionnaire)

- For merchants who use imprinters
 - Zip-zap machines
- Do not transmit cardholder data over either phone or internet
- Only paper records, **not** received electronically
- No cardholder data is stored electronically



Type 3 Merchant, SAQ B (24 question questionnaire)

- For merchants with stand-alone dial-up terminals
 - Brick-and-mortar, MOTO (Mail Order/Telephone Order)
- Dial-up terminals only connected to processor
 - i...e., not connected to any other systems
- Terminal not connected to internet
- Only paper records, **not** received electronically
- No cardholder data is stored electronically



Type 4 Merchant, SAQ C (32 question questionnaire)

- Payment application and internet connection on the same device
 - Card-present or card-not-present merchants
 - Can be POS or shopping cart application
- Device is not connected to any other systems
- Only paper records, **not** received electronically
- No cardholder data is stored electronically
- Payment application vendor provides remote support securely
- Required Network Scan by qualified third-party security assessor
- Complete Penetration Test by qualified third-party security assessor



Type 5 Merchant, SAQ D (226 questions)

- Any Merchant not Type 1-4
- Required Penetration Scan by qualified third-party security assessor
- Complete Penetration Test by qualified third-party security assessor

How will UNT Comply with PCI DSS continued...

- Attend annual training.
- Complete appropriate Self-Assessment Questionnaire (SAQ).
- If required Complete internal network scan with CITC.

- Make any corrections recommended from internal scan prior to scheduling independent scan.

- Complete network scan by an independent third party vendor, if required.
 - UNT has contracted with Trustkeeper to provide the scan and to provide assistance in achieving compliance.

- Complete penetration test by an independent third party vendor, if required.

- Enforce the use of Nelnet's QuikPay or other product for eCommerce transactions and use hardware and software that is PCI DSS compliant.

- Collaborate with Internal Audit to insure compliance.

Responsibility of the Dept ID/ Proj ID Holder

- The Dept ID/Proj ID holder along with their departmental network manager is responsible for completing a Self-Assessment Questionnaire (SAQ) annually.
 - The PCI Self-Assessment Questionnaire is an important validation tool that will be used by merchants to demonstrate compliance with PCI DSS.
- If needed, (SAQ C and D) after completing and passing the questionnaire, the department will work with their network manager and UNT CITC Security Team to schedule an internal scan. Any issues will need to be addressed prior to scheduling the security scan from a third party vendor.
- PCI Data Security Standard (PCI DSS) may require a security scan for merchants to help validate compliance with PCI DSS.
 - PCI Data Security Standard (PCI DSS) requires all Internet-facing IP address to be scanned for vulnerabilities.
 - To comply with the PCI Security Scanning requirement, merchants must have their web sites or IT infrastructures with Internet facing IP addresses scanned.
 - External scans will be performed monthly by third-party security assessor.
 - Annual penetration testing completed by third-party security assessor.
- The Dept ID/Proj ID holder will be responsible to insure their location (merchant) is following the University credit/debit card guidelines including PCI Data Security Standard (PCI DSS) requirements.

- The Dept ID/Proj ID holder will be responsible to report personnel changes (employees who process credit/debit card transactions) immediately in their department to the Cashier Area Supervisor in Student Accounting and University Cashiering Services.
- The Dept ID/Proj ID holder should get approval from the Student Accounting and University Cashiering Services before purchasing any new equipment and/or software related to credit card processing.
- Departmental merchants are required to complete annual training and sign a security agreement confirming the department (merchant) is following the PCI Data Security Standard (PCI DSS) requirements for safeguarding credit/debit card information.
 - The Dept ID/Proj ID holder and any Department Designee are required complete the training and sign the agreement.

Responsibility of Dept. ID/Proj ID And Department Designee

- The department designee must comply with UNT Policy and Procedures in regards to Payment Card Industry Data Security Standard (PCI DSS) requirements. See 2.2.31 http://www.unt.edu/policy/UNT_Policy/volume2/2_2_31.html
- All credit/debit card information, including documentation, must be stored in a secure area at all times.
- The credit card numbers shall not be printed on the receipt.
- Insure credit/debit card data is not downloaded or stored on a computer or network within the department. Do not share login names and passwords to systems that access credit/debit card data.
- Keep duties that are related to credit/debit card processing segregated for accountability. The employee who processes the credit/debit card transaction should balance their daily activity; however, a different employee should be responsible for reconciling the activity each month.
- If credit/debit card information is compromised, any department designee should inform the Dept ID/Proj ID holder to ensure the department's network manager, CITC Information and Security Team, Internal Audit and the Cashier Area Supervisor of Student Accounting and University Cashiering Services are contacted immediately.
- Dept ID/Proj ID holder and any department designee are responsible for completing annual credit card merchant training offered through Student Accounting and University Cashiering Services.
- Dept ID/Proj ID holder and department designee are responsible for notifying Student Accounting and University Cashiering Services prior to any changes/upgrades to equipment and/or software used to process credit card transactions.
- The Dept ID/Proj ID holder and the department designee should get approval from the Student Accounting and University Cashiering Services before purchasing any new equipment and/or software related to credit card processing.

Segregation of Duties

- The Dept. ID/Proj ID holder is responsible for departmental segregation of duties.
 - Any individual who processes credit/debit card transactions should not be involved with the monthly reconciliation.
 - Reconciliation- A thorough reconciliation of credit/debit card transaction would include the following documentation:
 - The reports generated from the credit/debit card terminal, YourPay or QuikPay should be reconciled to department's internal receipts daily or when transactions have been processed.
 - The reports generated from the credit/debit card terminal, YourPay or QuikPay should be reconciled to the accounting entries generated in the Financial Reporting Office and to the Departmental Management Budget Report.
 - Access to the Departmental Management Budget Report is available at my.unt.edu for monthly reconciliation.

Cardholder Data Compromised

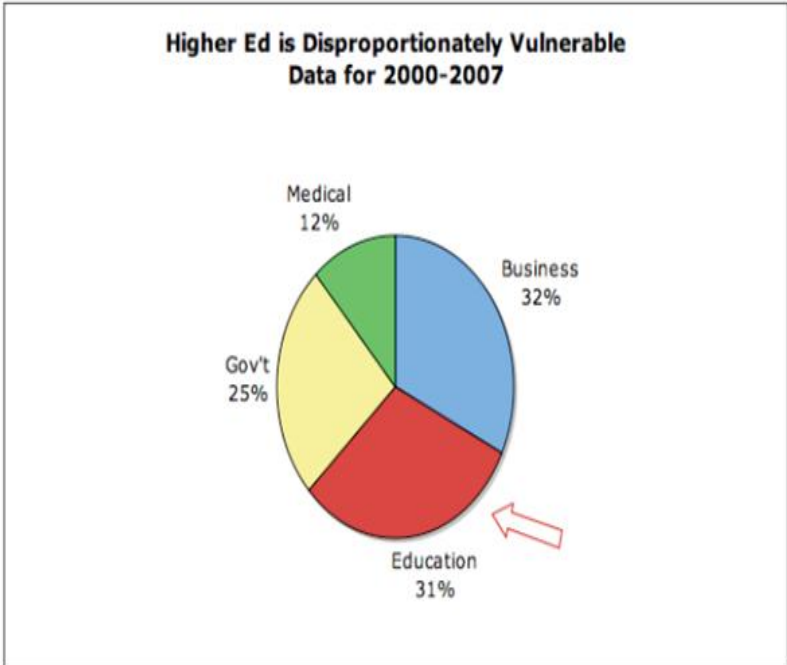
If cardholder data for which you are responsible is compromised, the university may be subject to the following liabilities and fines associated with each instance of non-compliance:

- Potential fines of up to \$500,000 (in the discretion of Visa and MasterCard).
- All fraud losses incurred from the use of the compromised account numbers from the date of the compromise going forward.
- The cost of re-issuing all cards associated with the compromise.
- The cost of any additional fraud prevention/detection activities required by the card associations (i.e. a forensic audit) or cost incurred by credit/debit card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity).
- Become permanently prohibited from processing credit/debit card transactions.
- Most important: The University's reputation (brand) is damaged.
- If credit/debit card information is compromised the Dept ID/Proj ID or departmental designee should immediately contact their network manager, CITC Information Security Team, Internal Audit and the Cashier Area Supervisor in Student Accounting and University Cashiering Services.
 - The department (merchant) must provide suspected or confirmed loss or theft of any materials or records that contain cardholder data.

Non-Compliant UNT Merchant

- **If a merchant is found to be non-compliant with PCI DSS Standards, UNT Policy for accepting credit card and/or UNT established best practices , Student Accounting and University Cashiering Services with the assistance of CITC Security may require the non-compliant merchant to cease acceptance of credit cards immediately.**
- **Any non-compliant website and any non-compliant point-of-sale locations will be required to cease operation until deemed compliant.**
- **It is the responsibility of the merchant to work with Student Accounting, CITC Security and their Network Manager to become compliant.**
- **After CITC and Student Accounting have verified compliance, the merchant will be allowed to resume credit card activities**

Educational institutions are disproportionately vulnerable to security breaches.



“Education institutions represent a relatively small part of the payment system and the total population. Where there are a few thousand Higher Education institutions, D&B lists over 14 million businesses. It is therefore disturbing to find that Education and Business represent roughly the same percent of breaches.”

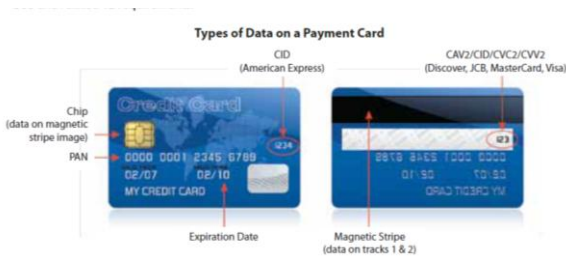
<http://www.walterconway.com/index.html>

Protecting Credit/Debit Card Information

- Credit/debit card payment information should be kept secured and confidential at all times.
 - Credit/debit card information should be secured in a locked area (room or closet).
 - The area designated to store credit/debit card information should be restricted to the Dept ID/Proj ID holder and/or any department designee responsible for processing or researching a transaction.
 - Any credit/debit card point of sale terminal should be placed in a secure area to prevent access to data within the terminal.
 - Access to credit/debit card data should be restricted to those individuals whose job requires such access.
- The customer and merchant receipt (as well as any other form that may contain credit/debit card information) should only display the last four digits of the account number.
- Pin pads or any magnetic strip readers should not be attached to a credit/debit card terminal or computer. Security track data may not be stored in any device used for credit/debit card processing.
 - Security data/track is defined as the data elements stored within the magnetic stripe on the back of a card, as well as the cardholder validation code (the three or four digit value printed on the signature panel of the card).
 - The information includes all the data required to commit fraud on a cardholder's account.
 - Only payment information may be stored:
 - Payment information includes: the cardholder's name, account number, expiration data and authorization code.
- Credit/debit card payment information cannot be stored on computers or networks, regardless of encryption.

- Credit/debit card information must be transmitted and received in a secure manner.
 - If your department received credit/debit card payment information by fax and/or mail, all digits of the card number except the last four, must be marked through before retaining for your records.
 - Credit/debit card information should not be sent to a fax application with an IP address.
 - Fax machines should be in secured area (room with a locking door) with no through traffic and with limited access.
 - Credit/debit card information should not be received by email.
- Credit/debit card receipts should be stored according to UNT's record retention schedule. All receipts must be shredded after that time. Currently, UNT retention schedule is 3 years plus fiscal year.

<http://www.unt.edu/compliance/recordsretention.shtml> see Series Item # 4.2.002, number 44, Cash Receipts.



Guidelines for Cardholder Data Elements

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name ¹	Yes	Yes ¹	No
	Service Code ¹	Yes	Yes ¹	No
	Expiration Date ¹	Yes	Yes ¹	No
Sensitive Authentication Data²	Full Magnetic Stripe Data ³	No	N/A	N/A
	CAV2 / CVC2 / CVV2 / CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

¹ These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

² Sensitive authentication data must not be stored after authorization (even if encrypted).

³ Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

Credit/Debit Card Processing

–e Commerce Transactions

Departmental merchants that process credit/debit card transactions using a web-based product must follow additional guidelines to be compliant with PCI DSS requirements. A department interested in processing credit/debit card transactions with a web-based product (eCommerce) should contact the Cashier Area Supervisor in Student Accounting and University Cashiering Services **before** purchasing and/or contracting with vendor.

- eCommerce is defined as conducting business communications and transactions over networks and through computers.
- Student Accounting maintains a partnership with NelNet/QuikPay as the University's eCommerce (online payment provider).
 - QuikPay is certified compliant with PCI DSS requirements.
 - Credit/debit card payment information is collected at QuikPay's website and processed for authorization.
 - Credit/debit card information is not transmitted over the university network.
 - For smaller departments*, Student Accounting and University Cashiering Services offers a Nelnet product called Commerce Manager (see Commerce Manager below)

***Department will have to apply for this service**

- Wells Fargo, our acquiring bank, is the credit/debit card processor for the university. As the credit/debit card processor, Wells Fargo assists with equipment recommendations to insure the University is using PCI DSS compliant hardware and software.
 - YourPay is a web based point of sale product offered through Wells Fargo for processing credit/debit card transaction. YourPay is certified as a compliant service provider.

- A computer workstation used for processing credit/debit card payments must be a dedicated computer terminal. A dedicated computer terminal should not have access to email, the ability to download programs or utilize any applications other than Windows or XP.
- Departments that use a web based product for credit/debit card processing, should implement a procedure to delete temporary files with include cookies and clear the history using “Tools” on the menu bar in Internet Explorer.
- Any changes in technology related to credit/debit card processing in your office should be reported to the Cashier Area Supervisor in Student Accounting and University Cashiering Services prior to implementing the change/upgrade.

Commerce Manager

Commerce Manager is a web-based payment system designed to host multiple departments. Commerce Manager allows individual departments across campus to conduct business and accept payments online while maintaining central control of accounting and security.

Below is some basic technical information the Student Financial Technical Team put together to assist departments.

To use Commerce Manager, there are 3 actions that are of interest to the developer:

- Authentication to the Nelnet website
- Handling the results of the transaction at the Nelnet website
- Handling the Nelnet End Of Day File for reconciliation or reporting needs

If a department is interested in using Commerce Manager, they should email the Cashier Area Supervisor at pam.johnson@unt.edu in the Student Accounting and University Cashiering Services Office.

Disputes/Chargebacks

- Disputes/chargebacks from cardholders will be sent directly to Student Accounting and University Cashiering Services. The information will be faxed to the department designated contact employee. A reply and all support documentation must be returned in writing within two (2) working days.
- It is the merchants' responsibility to maintain all documentation on credit card transactions. Any questions regarding disputes/chargebacks should be directed to Student Accounting and University Cashiering Services.
- The Dept ID/Proj ID will be charged back for a dispute/chargeback if the departmental representative does not provide the support documentation for the transaction in question by the requested time.

Credit/Debit Card Deposits

- All credit/debit card transactions for sales and services provided by the University must be deposited to a university dept ID or proj ID.
- UNT Financial Reporting will generate the accounting entry that credits the dept ID/ proj ID for credit/debit card sales.
- Each credit/debit card merchant determines which dept ID/proj ID will receive the credit for the deposit.
- Contact UNT Financial Reporting (ext. 4875) to have funds allocated to another dept ID/proj ID or split among several dept ID/proj ID's.
- The department should verify all credit card transactions are deposited accurately by reviewing the daily detail transaction reports produced from EIS monthly.

Credit/Debit Card Refunds

- Any refunds should be returned to the source of payment, therefore, credit card refunds should be returned to the credit card.

Credit/Debit Card Sanctions

The following sanctions will apply to any UNT Merchants who fails to complete the annual required training, self-assessment questions and network scan, if necessary.

- A month in advance of expiration, a notice will be sent by the Cashier Area Supervisor to the Dept ID holder, department designated employee, and technical support indicating that the required SAQ must be completed by the specified deadline. The Assistant Director of Operations of SAUCS will be copied on this email.
- A week prior to the expiration, a reminder will be sent by the Assistant Director of Operations to the Dept ID holder, Dept ID supervisor, Department Chair, Department Dean, department designated employee, and the technical support including the first notice and stressing the importance of completing the required SAQ, completing required scans (if needed) and or required training before the stated deadline. The Director of SAUCS will be copied on this email.
- A week after the compliance deadline has expired; the Assistant Director will send a second notice to the Dept ID holder stressing the critical need to complete requirements for compliance. The Director of SAUCS, Dept ID supervisor, Department Chair, Department Dean, the Department's Vice President, the Associate Vice President of Finance/Administration, Controller, Vice President of Finance/Administration, Internal Audit and the CITC Security Team will be copied on this email.
- Two weeks after the third notice, the Director of SAUCS will send a notice indicating that access to take credit cards will be terminated if action towards compliance is not achieved. The Dept ID supervisor, the Department Chair, the Department Dean, the Department's Vice

President, the Associate Vice President of Finance/Administration, Controller, the Vice President of Finance/Administration, Internal Audit and the CITC Security Team will be copied on this email, as well as the UNT System Compliance Officer will be copied.

- If compliance is not achieved after the previous notices, the Director of SAUCS will instruct the Assistant Director of Operations and Cashier Area Supervisor to contact either CITC Security Team and/or Wells Fargo Merchant Services to begin the termination process, depending upon which type of equipment is used by the department.
- Reinstatement of services will occur after PCI DSS compliance has been achieved.

NOTE: If there are extenuating circumstances and/or the department is working towards compliance, there will be an exception for administrative review by the Associate Vice President of Finance/Administration, Controller or Vice President of Finance/Administration.

Handouts/Reference websites

- Payment Card Industry (PCI) Data Security Standard
 - <https://www.pcisecuritystandards.org>

- Visa's Payment Application Best Practices (PABP)
 - http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html#anchor_1
 - Click on Payment Application Best Practices

- Treasury Institute for Higher Education
 - <http://www.treasuryinstitute.org>
 1. "Straight Talk About Data Security", by Walter Conway and Dennis W Reedy, http://www.treasuryinstitute.org/resource/library/BOM_DataSecurity.pdf