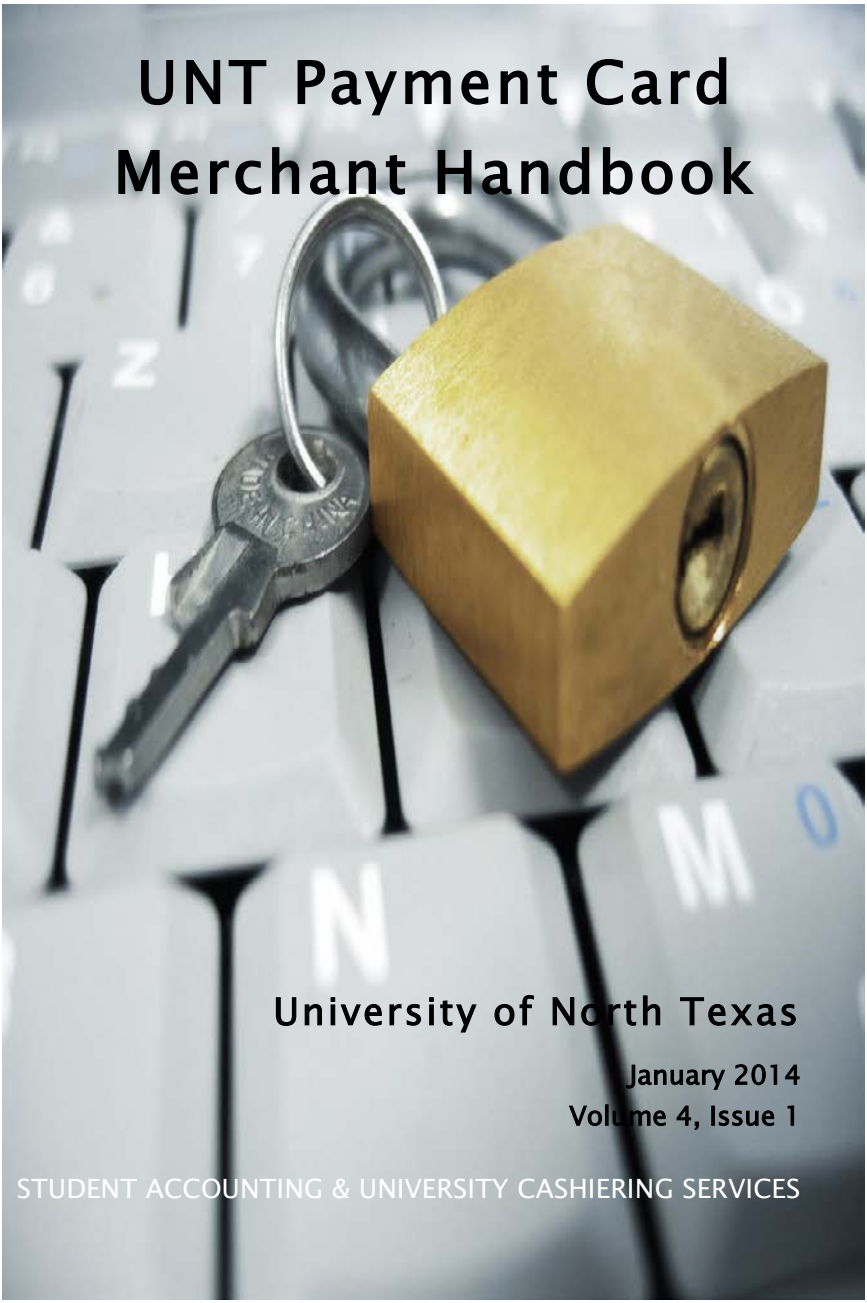
UNT Payment Card Merchant Handbook



University of North Texas

January 2014
Volume 4, Issue 1

STUDENT ACCOUNTING & UNIVERSITY CASHIERING SERVICES

Contents

The Purpose of the Handbook

The UNT Payment Card Merchant Handbook contains guidelines and policies for UNT Payment Card Merchants. Departments that accept payment 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 Payment 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 payment card merchants on campus and the processing of payment card transactions. See UNT Policy 2.2.31 http://www.unt.edu/policy/UNT_Policy/volume2/2_2_31.html

How do I accept credit card on campus?

Before determining if accepting credit cards is practical for your department, we encourage departments to ask themselves the following questions:

What type of resources do I need?
What can our office do to get ready for eCommerce?
How much technical efforts will there be?
Will accepting credit cards as a form of payment add any value/revenue to my project?

If an UNT Department wants to accept credit cards as a form of payment, they must contact the Student Accounting and University Cashiering Services for approval. The department will be required to complete a "User Feasibility Questionnaire". The department may obtain the questionnaire by submitting a request to the Cashier Area Supervisor of Student Accounting and University Cashiering Service at pam.johnson@unt.edu .

How does my department accept credit cards online?

Student Accounting has contracted with Nelnet Business Solutions to offer an eCommerce solution that would be cost effective for departments and at the same time ensure PCI DSS compliance. 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.

If the department is considering an eCommerce solution, your network support and/or web developer will be responsible for developing the department's webpage. Below is some basic technical information our Student Financial Technical Team put together to assist the department's web developer.

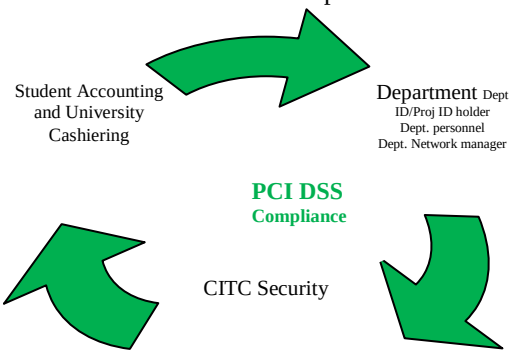
To use eCommerce Manager, there are 3 actions that are of interest to the developer:
Authentication to the Nelnet website
Handling the results of the transaction at the Nelnet website
Handling the Nelnet End of Day File for reconciliation or reporting needs

The PCI Security Standards Council ("PCI SSC") owns, maintains and distributes the PCI Data Security Standard (DSS) and all its supporting documents.
PCI DSS is a set of comprehensive requirements for enhancing payment account data security; developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. Merchant compliance validation has been prioritized based on the volume of transactions, the potential risk, and the exposure introduced into the payment system.
All merchants (departments) will fall into one of the four merchant levels based on VISA transaction volume over a 12-month period.

Level/Tier[1]	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region[2]	*Annual Report on Compliance ("ROC") by *Qualified Security Assessor ("QSA") Quarterly network scan by *Approved Scan Vendor ("ASV") *Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	*Annual Self-Assessment Questionnaire ("SAQ") *Quartely network scan by ASV *Attestion of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	*Annual SAQ *Quarterly network scan by ASV *Attestation of Compiance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	*Annual SAQ recommended *Quarterly network scan by ASV if applicable * Compliance validation requirements set by acquirer

[1]- Comprised entries may be escalated at regional discretion
[2]-Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1

Following PCI DSS requirements is critical and can assist in preventing a security breach. If payment 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 payment 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 core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

PCI Data Security Standard	
Build and Maintain a Secure Network	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	3. Protect stored data Encrypt transmission of cardholder data and sensitive information across public networks 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	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	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

**Source: Security Standards Council*

How will UNT comply with PCI DSS?

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

A	Card-not-present (ecommerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	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

**Source: Security Standards Council*

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 Campus Guard to provide the scan and to provide assistance in achieving compliance.
- Complete penetration test by qualified internal staff or 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 Student Accounting, CITC Security and Internal Audit to ensure compliance.

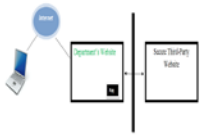
What is my Validation Type?

SAQ A (11-question questionnaire): SAQ A merchants do not store data on their systems or premises.

Your location (department):

- accepts only card-not-present transactions
  - e-commerce or mail/telephone-order
- Does not store, process or transmit any cardholder data on your systems or premises, but relies entirely on a third party to hand all these functions.
- Has confirmed the third party(s) handling storage, processing and/or transmission of cardholder data is PCI compliant.
- Retains only paper reports and/or paper receipts with cardholder data and these documents are not received electronically; **and**
- does not store any cardholder data in electronically format

This option would never apply to merchants with face-to-face POS environment.



SAQ B (29-question questionnaire): SAQ B merchants are only imprint machines or only standalone, dial-out terminals. No Electronic Cardholder Data Storage.

Your location (department):

- Uses only an imprint machine and/or uses only standalone, dial-out terminal (connected via a phone line to your processor) to take your customers' payment card information.
- The standalone, dial-out terminal(s) are not connected to any other system within your environment.
- The standalone, dial-out terminal(s) are not connected to the Internet
- Does not transmit cardholder data over a network (either an internal network or the Internet)
- Retains only paper reports and/or paper receipts, not received electronically; **and**
- Does not store cardholder data in electronic format.


or


SAQ C-VT (51-question questionnaire): SAQ C-VT merchants are web-based virtual terminals, no electronic cardholder data storage.

Your location (department):

- Only payment processing is done via a virtual terminal accessed by an Internet-connected web browser.
- Virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider.
- Accesses the PCI DSS compliant virtual terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems).
- Does not have software installed that causes cardholder data to be stored. (for example, there is no software for batch processing or stored-and-forward)
- Does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached)
- Does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet)
- Retains only paper reports and/or paper receipts, not received electronically; **and**
- Does not store any cardholder data in electronic format.

SAQ C (80-question questionnaire): SAQ C merchants have payment application systems connected to the Internet, no electronic cardholder data storage.

Your location (department):

- Has a payment application system and an Internet connection on the same device and/or same local area network (LAN).
- The payment application system/Internet device is not connected to any other system within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems)
- Is not connected to other locations and any LAN is for a single store only
- Retains only paper reports and/or receipts, not received electronically;
- Does not store cardholder data in electronic format; **and**
- Payment application software vendor uses secure techniques to remote support to the payment application system.

SAQ D (286-question questionnaire): SAQ D merchants do not meet the descriptions of SAQ A through C, describe above.

- While many of the organization completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some of the requirements do not apply.
- For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology.

Responsibility of the Dept ID/ Proj ID Holder

- 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 .

- The Dept ID/Proj ID holder along with their departmental network manager is responsible for completing a Self-Assessment Questionnaire (SAQ) and an Attestation of Compliance annually.

    - The PCI Self-Assessment Questionnaire is an important validation tool that will be used by merchants to demonstrate compliance with PCI DSS.

    - UNT has contracted with Campus Guard to provide the questionnaire online at www.Campus Guard.net .

    - The Attestation of Compliance certifies the accuracy of the information provided on the questionnaire.

- After completing and passing the questionnaire, the department will work with their network manager and UNT CITC Security Team to determine if an internal scan is needed for each location (department). 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 in the cardholder data environment 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 in the cardholder data environment scanned.
  - Third-party security assessor will perform external scans at least every three months.
  - Annual penetration testing completed by third-party security assessor.

- The Dept ID/Proj ID holder will be responsible to ensure their location (merchant) is following the University payment 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 or reconcile payment card transactions) immediately in their department to the UNT ITs Security Office and the Cashier Area Supervisor in Student Accounting and University Cashiering Services.

- The Dept ID/Proj ID holder must 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 cardholder data.

  - 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 cardholder data, including documentation, must be stored in a secure area at all times.
- The cardholder data shall not be printed on receipts.
- Insure payment 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 payment card data.
- Keep duties that are related to payment card processing segregated for accountability. The employee who processes the payment card transaction should balance their daily activity; however, a different employee should be responsible for reconciling the activity each month.
- If suspected compromise of cardholder data, 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. Employee should not do anything else on the suspected comprised workstation. Until CITC security advises, the network cable should be unplugged from the workstation in question.
- 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 must 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 payment card transactions should not be involved with the monthly reconciliation.

    - Reconciliation- A thorough reconciliation of payment card transaction would include the following documentation:

        - The reports generated from the payment 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 payment 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 payment card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity).
- Become permanently prohibited from processing payment card transactions.
- **Most important: The University's reputation (brand) is damaged.**
- If suspected cardholder data 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 any materials or records that contain cardholder data if a breach is suspected or confirmed.
    - Do not log into workstation/computer of suspected comprise.

Non-Compliant UNT Merchant

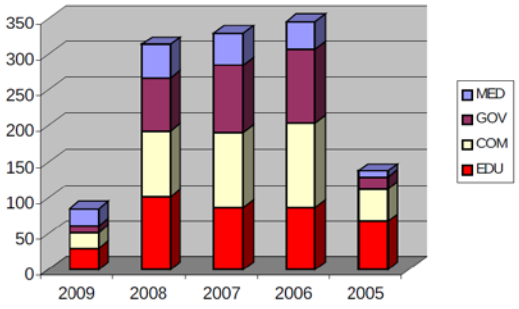
- **If a merchant is found to be non-compliant with PCI DSS, UNT Policy for accepting credit card and/or UNT established best practices , Student Accounting and University Cashiering Services with the assistance of CITC Security may require the non-compliant merchant to cease acceptance of credit cards 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.



Higher Education is consistently in the top 2

Source: Privacy Rights Clearinghouse 2005-2009

Protecting Cardholder data

- Payment card payment information should be kept secured and confidential at all times.
    - Cardholder data should be secured in a locked safe or file cabinet.
    - The area designated to store cardholder data should be restricted to the Dept ID/Proj ID holder and/or any department designee responsible for processing or researching a transaction.
    - Any payment card point of sale terminal should be placed in a secure area to prevent access to data within the terminal.
    - Access to payment 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 cardholder data) should only display the last four digits of the account number.
- Pin pads or any magnetic strip readers should not be attached to a payment card terminal or computer. Security track data may not be stored in any device used for payment 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.
- Payment card payment information cannot be stored on computers or networks, regardless of encryption.
- Cardholder data must be transmitted and received in a secure manner.
    - If your department received payment card payment information by a secure fax and/or mail, all digits of the card number except the last four, must be removed before retaining for your records.
    - Cardholder data must not be sent to a fax application with an IP address.

- Fax machines must be in secured area (room with a locking door) with no through traffic and with limited access.
- Cardholder data must not be received by email.

- Payment 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 Data[2]	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.

Payment Card Processing

-e Commerce Transactions

Departmental merchants that process payment card transactions using a web-based product must follow additional guidelines to be compliant with PCI DSS requirements. A department interested in processing payment card transactions with a web-based product (eCommerce) must 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.
    - Payment card payment information is collected at QuikPay's website and processed for authorization.
    - Cardholder data 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 payment card processor for the university. As the payment card processor, Wells Fargo assists with equipment recommendations to ensure the University is using PCI DSS compliant hardware and software.

- Any changes in technology related to payment 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 forwarded to the department designated contact employee. A reply and all support documentation must be returned in writing within two (2) working days.

- Supported documentation will include a signed sales receipt and/or signed written authorization from the cardholder and/or their authorized user.

- 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.

Payment Card Deposits

- All payment 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 payment card sales.

- Each payment 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.

Payment Card Refunds

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

Payment 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

- Approved Companies & Providers (PA-DSS)
  - https://www.pcisecuritystandards.org/approved_companies_providers/index.php

- Treasury Institute for Higher Education
  - http://www.treasuryinstitute.org

- Privacy Rights Clearinghouse
  - http://www.privacyrights.org/