Credit Card Procedures

The University accepts credit card payments as a convenience to its customers. University merchants may accept Visa, MasterCard or American Express cards per the terms of the university's merchant services provider contract. The Office of the North Carolina State Controller has established a Master Services Agreement (MSA) with SunTrust Merchant Services, a leading merchant card processing vendor. The MSA provides services to eligible state agencies, universities, community colleges, and local units of government on a statewide enterprise basis, allowing eligible participants to benefit from the leveraging of volume pricing.

University merchants (departments) are responsible for compliance by their third-party service providers who accept credit card payments that deposit funds to the university.

These procedures are designed to protect cardholder data; maximize university compliance with its merchant services provider contract, which includes compliance with the Payment Card Industry Data Standards (PCI DSS) and the various credit card standards; and to ensure appropriate integration with the university's financial and other systems.

The following steps are required to ensure credit card acceptance for goods and services provided for department's customers.

1. **Credit Card Acceptance Questionnaire**

   Department completes the Credit Card Acceptance Questionnaire and submits to the controller. This questionnaire has two purposes: a) Apprises the requesting department of the requirements for credit card acceptance and b) Provides the credit card acceptance committee of the intent and needs of the department who desires to accept credit cards as a method of payment.

2. **Departmental Receipting Privileges**

   Department requests receipting privileges (electronic submission to Controller). These privileges may already exist for departments who deposit payments using other methods. In these cases, the privileges need to be revised to accommodate the receipting method of accepting credit cards.

3. **Department Determines Credit Card Method**

   a. The Department must determine which method will be utilized for accepting credit cards, i.e. WEB or Point of Sales (POS) terminal, and check the applicable box on the Departmental Receipting Privileges request from. Both methods may be used by a department.
   b. Accepting credit cards by the WEB requires the use of an acceptable payment gateway, such as TouchNet, and payment of monthly transaction fees.
   c. Additional costs are associated with the POS terminal such as analog telephone costs, monthly transaction fees and the purchase or rental of the POS terminal.

4. Department Applies for Merchant Id(s)

a. Once the Departmental Receipting Privileges form with credit cards section checked has been approved, the Controller's Office will prepare the applicable merchant number request forms for the Office of the State Controller (OSC) and forward them to the departmental contact for completion.
b. As a best business practice, any request for a Visa/MasterCard merchant number will also have an American Express merchant number request form.
c. Separate merchant numbers are required for WEB and POS terminals.
d. The department must complete the highlighted areas on both forms: Description of transactions, Number of transactions, Dollar volume, Anticipated average ticket transaction size, Outlet contact Name, Title, Phone, Fax and Email. The completed forms should be returned to the Financial Systems.
e. All merchant number requests are submitted electronically to OSC. It takes 7-10 business days for the merchant numbers to be assigned. The OSC representative will assign a ticket number and forward to FirstData Merchant Services and American Express representatives.
f. The bank representative will link ('affiliate') the POS merchant number and link the WEB numbers in order for departments to take both credit cards and notify OSC when completed.
g. In addition to linking, the bank representative will assign a Merchant Id (MID), Terminal Id (TID) and Datawire Device Id (DID) numbers for WEB merchants. These numbers are required for TouchNet setup.
h. OSC will notify Financial Systems once all of the setup is completed.
i. Financial Systems will notify department that they are ready to accept cards.
j. Financial Systems will key the WEB merchant numbers in TouchNet Production after testing is completed by requesting department.

5. Point of Sale (POS) Terminal Purchases

a. POS terminals may be purchased through OSC or through other means such as using the Pcard or by requisition in Purchasing.
b. Requests for a POS terminal must also be submitted electronically by Financial Systems and at the same time as the merchant number requests.
c. In addition, requests for a POS terminal from OSC must also have the signature page faxed to OSC. It is preferred that the department scan the form with the signature of the departmental budget manager, save as a PDF and email to Financial Systems.
d. Departments purchasing a POS terminal outside OSC must also have the signature page faxed to OSC with 'Purchased outside OSC' typed in the Shipping information section. It is preferred that the department scans the form with the signature of the departmental budget manager, save as PDF and email to Financial Systems.
e. POS terminals no longer in use may be turned in to Financial Systems and held in the locked closet for a POS Loan Program. Financial Systems will contact the FirstData and request the merchant id be 'unaffiliated' or scrubbed from the terminal upon receipt.

6. TouchNet Initial Department Setup Procedures

a. Department meets with TouchNet Administrator to discuss their particular need and whether uStore or uPay/TLink is the appropriate TouchNet package.

b. If the department already has a software application they are using for their operation, the TouchNet Administrator will contact TouchNet to determine whether the vendor is a TouchNet Ready Partner (TRP). TouchNet currently charges a fee for new TRP setups which will be incurred by the requesting department.
   If the vendor is a TRP, the TouchNet Administrator and the department representative will work together to set up the uPay site in TouchNet MarketPlace TEST. The department representative will need to get information from the vendor for this setup and will also need to provide information to the vendor.
   If the vendor is not currently a TRP, the TouchNet Administrator and the department representative will work together to connect the vendor and TouchNet's TRP Program Director to discuss becoming part of the TRP program. If the vendor chooses not to become part of the TRP program, they can still use uPay to connect to TouchNet. There again, the department representative will need to get information from the vendor for the uPay setup and will also need to provide information to the vendor.
   If the department doesn't already have a software application that meets their particular business need, a uStore is typically the avenue which will be recommended to the department, for which there is currently no fee.
c. If the department does not currently have a software application that meets their business need and uStore will not suffice, the department has the option of purchasing software to assist their operation and will need to go through the Bidding and Contractual process through Purchasing. The Purchasing department is aware that TouchNet is UNCW's preferred payment gateway and the requirement of TouchNet connectivity for credit card processing needs to be included in the specifications of the RFP/bid.
d. If neither uStore nor uPay/TLink will work for the department's business need, the department will need to return to the Controller's Office for authorization to use a Payment Gateway other than TouchNet. In this case, the TouchNet Administrator's interaction in the process is completed at this stage of the process.
e. The TouchNet Administrator will request the Merchant Id Manager to create a merchant in the TEST TouchNet Payment Gateway for the requesting department. Upon notification that it is created, the TouchNet Administrator will approve the merchant ID changes within TouchNet, create the merchant Host System Account and contact TouchNet to request a TEST Payment Gateway Credit Card Merchant reset.
f. Upon notification that the reset has occurred, the TouchNet Administrator will contact the department to schedule a time to work on the MarketPlace setup together. At this time, the TouchNet Administrator will send the Request for Access to the department representative so that access requests can begin to be prepared by the department staff and submitted to the TouchNet Administrator.
g. Toward the end of the testing phase of the department's MarketPlace setup, the TouchNet Administrator will schedule TouchNet deposit transmittal training for the appropriate department staff, inviting the Cashier Supervisor as well. Depending on the particular MarketPlace setup required, Fulfiller training may also be required and scheduled by the TouchNet Administrator.
h. Upon successful completion of MarketPlace testing, the TouchNet Administrator will request the department's merchant ID be set up in Production TouchNet by the Merchant ID Manager. Upon notification that it is created, the TouchNet Administrator will approve the merchant ID changes within TouchNet, create the merchant Host System Account and contact TouchNet to request a Production Payment Gateway Credit Card Merchant reset.

i. Upon notification that the reset has occurred, the TouchNet Administrator will create the skeleton of the uPay/TLink or uStore in Production, set up user access based on the access requests received, and contact the department so they can set up their MarketPlace uPay/TLink site or uStore in Production.
j. The department is responsible for setting up their site in Production and once this is completed, they will contact the TouchNet Administrator to schedule a test transaction in Production. This is necessary to ensure the Merchant ID setup is correct.
k. Upon satisfactory completion of a test transaction in production, the TouchNet Administrator will void the transaction per the department request so the test transaction is not art of the night's settled batch.
l. The TouchNet Administrator will notify the Cashier's Office that the department's site is now live in Production TouchNet.

7. Payment Gateway other than TouchNet, requires more PCI security/scans

TouchNet is the preferred payment gateway. Any exceptions to TouchNet requires the approval of the Controller and the University Security Officer in the IT Department. Additional compliance to Payment Card Industry Data Security Standards (PCI DSS) is required such as periodic system scans which are performed by the University Security Officer in the IT Department. The annual PCI DSS survey is also completed by the University Security Officer.

8. Credit Card Deposit Requirements

a. All credit card transactions must be brought to the Cashier Office daily regardless of the dollar amount. The Daily Deposit and Reporting Law (G.S. 147-77) requires each State agency to deposit all funds on a daily basis and to report the same on a daily basis.
b. Departments accepting credit cards by telephone or in person must ensure the security and confidentiality of the card holders' information.
c. Credit card number that are written down must be destroyed after the transaction is processed. Disposal of cardholder data must be cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
d. The credit card must be present for in person transactions with proof of cardholder identification; letters or notes of authorization from the cardholder are not acceptable.
e. Adhere to the ***Instructions for Preparing a Deposit Transmittal for Credit Card Transactions*** either Point of Sale (POS) or web credit card transactions as provided the Finance receipting training course.

9. Credit Card Fees

University departments that provide credit card merchant services are responsible for related equipment and supply costs, processing fees, and fines and penalties resulting from noncompliance with University, State, and payment card industry policies. The processing fees for payments by credit card include interchange fees, assessment and switch fees, and merchant service fees. The schedule of fees for merchant card services can be found on the North Carolina Office of the State Controller (NCOSC) website. This schedule applies to merchant card services acquired through the NCOSC, pursuant to the Master Services Agreement (MSA) with SunTrust Merchant Services, LLC (STMS), dated August 1, 2006.

University departments accepting credit cards should charge credit card fees to the same funding source as the revenue source, the department is required to obtain approval from the Credit Card Acceptance Committee.

Appropriated State funds (General funds) cannot be charged credit card transaction fees. Departments may use trust or auxiliary funds provided the revenue source is not derived from student fees.

10. Compliance Security of Credit Card Users' Data

All staff accepting credit cards must adhere to the thirteen PCI DSS requirements:

Build and maintain; a secure network

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 in a secure location
4. Disposal of cardholder data must be cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
5. Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a vulnerability management program

6. Use and regularly update anti-virus software.
7. Develop and maintain secure systems and applications.

Implement strong access control measures

8. Restrict access to cardholder data by business need-to-know.
9. Assign a unique ID to each person with computer access.
10. Restrict physical access to cardholder data.

Regularly monitor and test networks

11. Track and monitor all access to network resources and cardholder data.
12. Regularly test security systems and processes (i.e. annual penetration tests, which are different than the vulnerability scanning requirement).

Maintain an information security policy

13. Maintain a policy that addresses information security.

Compensating controls may be a consideration if a requirement cannot be met due to legitimate technical or documented business constraints.

11. Reconciliation

All credit card terminals and web applications must be closed out and reconciled on a daily basis. In addition to normal reconciliation functions, the reconciler will ensure that all transaction receipts, both processed and voided, are dually accounted. Reconciliations must compare all credit and debit card payments processed using original supporting documentation,

with the Banner fund/account in the general ledger. Reconciliations must be maintained by the department and are subject to review.

a. Credit card transactions must be **reconciled daily**:
    - The total amount of credit card receipts for POS transactions must match the credit card transaction amount reported on the deposit transmittal.
    - The total amount of credit card transactions reported on the vendor reports (TouchNet or Blackboard) must match the amount entered on the deposit transmittal.