Payment (Credit/Debit) Card Processing Procedures

I. Executive Summary and Purpose

All University departments and entities shall process inbound payment (credit/debit) card transactions through approved mechanisms/systems, processors, and equipment. The merchant services provider, which is contracted by the North Carolina Office of the State Controller (NC OSC) and by the University, must be utilized for the processing of payment card transactions.

These procedures are required in direct support of the UNC Charlotte Payment (Credit/Debit) Card Processing Standard. This document sets forth details and procedural requirements for the implementation of payment card processing at UNC Charlotte or the outsourcing of that processing to a third party. More detailed information may be referenced in the UNC Charlotte Merchant Manual (currently in development).

The procedures' scope, revisions, exceptions, and compliance are noted in the Payment Card Processing Standard.

II. Definitions

Definitions may be referenced within the eCommerce Glossary and/or the Payment Card Industry Security Standards Council (PCI SSC) website.

III. General Requirements

Oversight

A. All departments accepting credit/debit cards for payment must comply with the UNC Charlotte Payment (Credit/Debit) Card Processing Standard.

B. The Vice Chancellor of Business Affairs (VCBA) directs all payment card processing activity and related compliance validation at The University of North Carolina at Charlotte (UNC Charlotte). The oversight of card processing operations is delegated to the eCommerce Office (eCO) which resides within the Controller's office.

C. UNC Charlotte is a state agency and as such must operate under the authority of the State of North Carolina statutes, policies, and guidelines. These policies dictate that all card processing be conducted through the Master Services Agreement (MSA) contracted by NC OSC. To comply with that state policy:

   1. All accounts for card processing must be established through NC OSC via eCO. Campus academic and administrative units, organizations, affiliates, and employees shall *not* establish accounts for the acceptance of payment cards outside of this established means, or utilize other mechanisms which bypass the established setup and approval of card processing activities.

2. The outsourcing of payment card processing as well as the contracts associated with that activity must be approved by eCO and other University entities as required.

3. All card processing activities are subject to the PCI SSC specifically the Standards overseen by the Council: the Payment Card Industry Data Security Standards (PCI DDS), the Payment Application Data Security Standard (PA-DSS), and the Pin Transaction Security Requirement (PCI- PTS).

4. All card processing must adhere to North Carolina General Statutes and applicable policies. NC OSC provides oversight for UNC Charlotte payment card processing.

D. UNC Charlotte Information and Technology Services (ITS) oversees governance of data security, use of IT systems, evaluation and recommendations of technologies, and provides direction and support for the security and networking of campus infrastructure utilized for card processing systems.

Security of Card Data

E. University staff and entities are prohibited from storing the Primary Account Number (PAN) or Sensitive Authentication Data (SAD), physically or electronically (e.g., computer hard drives, CDs, Disks, and other external storage media), after authorization of the transaction.

F. UNC Charlotte academic and business units are prohibited from establishing web sites to receive and/or process CHD outside of the allowed eCommerce web infrastructure.

G. All payment card transactions processed over digital/IP lines must be configured so that the transaction data is processed *only* on the segregated PCI network. University card processing must not take place on the main University network. Merchants are responsible for ensuring that proper configuration of network devices is in place. ITS and eCO will assist as needed.

H. Third parties, including student organizations, may not process payment cards over the University wired or wireless network without the approval of the Vice Chancellor for Business Affairs (VCBA) or his/her designee. Transactions may be processed on cellular devices that do not interface with the University network.

I. In some cases, University departments may support student organizations with specified special status (e.g., student government organizations). If such a student organization website is hosted on a University server, it will not be allowed to link out for payment processing; it is prohibited. Externally hosted (i.e., not hosted at/or by UNC Charlotte) student organization webpages that include payment processing, must have a visible disclaimer readily viewable on the site stating that the site is ***not*** the University or a part of it.

J. The PAN must be masked when displayed (the first six and last four digits are the maximum number of digits to be displayed). In most cases where truncation is needed, only the last four digits of the PAN should be displayed. Only personnel with a legitimate business need should be able to see the full PAN.

K. Cardholder Data (CHD), the PAN, and/or SAD are not to be left unattended or disclosed to others.

L. To the extent possible on electronic transactions, the sale transaction shall *not* take place on University computers or network resources. Any instance where this occurs must be fully disclosed, in advance, to eCO and approved in advance by that office in conjunction with ITS.

M. UNC Charlotte academic and business units are prohibited from accepting CHD via email, fax, or any electronic means including end-user messaging technology.

   1. If an email is received by University staff that contains CHD, the CHD shall not be used to process the transaction and the email must be permanently deleted from the recipient's mailbox. A new email must be created to reply to the sender with instructions on the proper procedures for submitting their card transaction for processing. ("Reply" must not be used because the card information is not to be resent over the network.)
   2. If acceptance of CHD via fax is needed for business operations, approval must be requested and obtained through eCO. A request including business justification must be submitted to eCO. If fax usage is approved for card acceptance, then an analog fax setup must be used (vs. digital). Approved analog fax machines must reside in a physically secure location with controlled/ restricted access limited to those individuals who have completed the Requirements for Card Processing.

N. If acceptance of CHD via mail/hard copy is needed for business operations, approval must be requested and obtained through eCO. The academic/business unit will be responsible for documenting internal processes to handle the CHD per PCI DSS and eCO processes. The CHD must be secured with access to it limited to only those individuals who have completed the Requirements for Card Processing. The CHD must not be retained after authorization. The security code is not to be to requested on any mailed in or hard copy forms.

O. Merchants approved to receive physical documents which contain the PAN, must ensure those documents are:
   1. Processed on approved devices as they are received.
   2. Stored in a physically secure location until the transactions are processed, should there be any delay in processing.
   3. Accessible only by staff that have completed the Requirements for Card Processing.
   4. Securely destroyed so that all CHD is rendered unreadable once the transaction is processed or documentation is no longer needed.

P. At the time of disposal, all hard-copy materials containing the PAN and/or SAD must be crosscut shredded, incinerated, or pulped so that the CHD is rendered incapable of being reproduced or retrieved. All disposal methods must meet or exceed the PCI DSS requirement for destruction.

Q. All card transactions must be keyed into approved devices. Desktop or laptop computers, tablets, or other electronic devices are deemed "virtual terminals" if utilized by merchant staff or provided for customers for the entry of CHD. Such setups, or virtual terminals, are not to be used for entry of CHD by staff or customers unless approved by eCommerce and set up by ITS. Contact eCommerce for approval. The completion and submission of the *EC-Virtual Terminal Request* form will be required.

R. Only designated personnel, who have completed the individual Requirements for Card Processing, may have access to CHD, interface with customer card transactions, and/or obtain access to card reporting or administrative portals. Access to system components and CHD will be limited to only those individuals whose job requires such access. Access requests are to be submitted to eCO using the eCommerce form *EC-Access Request to Reporting Systems*, or at the following URL: https://imaging.uncc.edu/imagenowforms/fs?form=eCommerce_Systems_Access.

S. Personnel granted access to card reporting and/or administrative portals are prohibited from copying, moving, and storing CHD onto local hard drives and removable electronic media unless explicitly authorized to do so by eCO for a defined business need. If a business need is authorized, the data must be protected in accordance with all applicable PCI DSS Requirements.

T. Designated personnel that are approved to interface with CHD, customers, or portals are subject to University Policy 101.23, Employment-Related Background Checks and Criminal Activity Reporting.

U. Access of eCommerce reporting systems from off campus must be conducted on University owned equipment that is updated with current antivirus and required patches. These reporting systems (e.g., TouchNet, ClientLine, Online Merchant Services, CEO Portal) are not to be accessed via personally owned computers and devices.

V. Physical security and storage of infrastructure components that control or interface with card processing systems is managed by University ITS.

W. Information security incidents or concerns should be reported to University ITS. The UNC Charlotte Standard for Managing Information Security Incidents as well as the Guideline for Reporting Information Security Incidents provides guidance regarding action to be taken if a security incident is suspected or confirmed. See section IX of this document for additional detail.

Card Acceptance

X. Any University unit wishing to accept payment cards for goods and/or services must complete the *EC-Application to Process Payment Cards (EC-APP)* (path: S:\Campus

Merchants\eCommerce Forms\ EC-APP - Application to Process Payment Cards) form and submit that to eCommerce@uncc.edu.

Y. Business manager approval is required for all card processing.

Z. The acceptance of gifts, donations, or sponsorships must first be approved through University Advancement before public facing sites are enabled for acceptance of those monies.

AA. Upon approval to process card transactions, eCO will work with the campus unit to determine the appropriate merchant account to be utilized for the processing of card transactions. The eCO will request a merchant account, if a separate merchant account is necessary, for the college or department through NC OSC.

BB. The eCO will work with the campus entity regarding the means by which card transactions will be accepted:

1. Online - Card Not Present (CNP)
2. In person - Card Present (CP)

The eCO will facilitate the establishment of all CNP and/or CP operations for approved set ups as well as submit orders for Point of Sale (POS) terminal equipment to be utilized.

CC. If specialized software and/or systems are required for processing, eCO (in conjunction with the University ITS) will work with the campus entity to approve that processing and ensure that processing standards and security measures are met.

DD. All departments or units issued a merchant account will be required to:

1. Complete the *EC-Merchant Agreement*.
2. Submit business processes for card processing at least annually to eCommerce, and when significant changes to the card processing environment occur.
3. Submit card data flow diagrams to eCommerce.
4. Complete required Self-Assessment Questionnaires (SAQs) and associated validation documentation requirements.
5. Attest to compliance with PCI DSS.
6. Ensure staff meet all requirements for card processing.

EE. Currently, UNC Charlotte accepts four major payment cards: Visa, MasterCard, American Express, and Discover *(please note: Diners' Club and JCB are accepted under the Discover agreement).* It is expected that all University merchants engaged in the acceptance of card transactions accept all card types supported by the University and no others.

FF. Audits will be performed periodically by the UNC Charlotte Internal Audit Department to confirm card processing complies with PCI DSS and University standards and procedures.

Daily Responsibilities

GG. All merchants are subject to University Policy 602.4, Handling Cash, Checks, and Other Monetary Receipts.

HH. On a daily basis, the department must balance transactions and settle their sales electronically to the merchant services provider.

II. All merchants are subject to North Carolina law and policies. Specifically, merchants must:

1. Prepare appropriate deposit documentation and submit it to the University Cashiers via the Financial Transaction Request (FTR) form by 12:00 noon on the day that the settlement of funds for card transactions is reflected in the banking settlement reports.
2. Provide appropriate back-up documentation to substantiate the deposit.
3. Provide deposit documentation on a timely basis for amounts debited or credited directly to the merchant account due to chargebacks, retrievals, refunds, reversals, or other activity which affects the merchant account funds.

JJ. Departments shall maintain adequate records of the sales transactions. Daily sales totals, logs, etc. substantiating revenue should be stored in accordance with state record retention policies and the current MSA.

KK. Reconciliation of all transactions must be performed on a regular basis. Transactions and account charges deposited to the University Cashiers must be reconciled and verified before the deposit is submitted. Supervisory review of accounts reflecting refunds, chargebacks, reversals and card fees should be conducted at minimum on a monthly basis.

IV. Requirements for All Payment Card Transactions

A. Return, refund, and/or cancellation policies must be disclosed to the cardholder before the cardholder enters their card information for processing. Signs disclosing the policy must be clearly visible at the Point of Sale (POS) for face to face transactions or web site/online portal utilized for the merchant for internet transactions.

B. All customer receipts must truncate the PAN so that only the last four digits are printed on the merchant and the customer copy of the receipts. The receipts must not display the card expiration date or SAD.

C. All POS terminal and internet transactions must be batched and transmitted to the merchant card processor on a daily basis. Transactions are not to be held and batched at a later time.

D. The settlement of all funds must be reported to the University Cashiers no later than noon of the day that the funds appear in the settlement account. Current procedures for the deposit of those funds must be followed. Currently, sales totals (net of refunds) must be submitted on a Payment Book Receipt (PBR) deposit form along with a copy of the sales report from the card processor. A copy of the gateway batch settlement report (totals reports, *not* detail) must be included for internet transactions. The settlement tape from the POS terminal is no longer required to be included for POS terminal transactions; the merchant is to retain the settlement tape for audit purposes. The Payment Book Receipt (PBR) form is available on the Financial Services website; it may be located under Transaction Type on the Financial Transaction Request (FTR) form.

Transactions that occur on Friday, Saturday, and Sunday (or over holiday periods) must be deposited in the same manner (as above) on Monday (or the following business day) to the University Cashiers. A separate deposit must be created for each day that transactions occurred. The transactions are not to be combined for the weekend (or holiday period) and deposited on one form for multiple days.

F. Sponsorship monies collected must be accounted for and viewable to University Advancement. All monies received for sponsorships are to be deposited to account code 102654; the preferred departmental fund number may be used. A report detailing the donor information is to be attached to the deposit. Please see: *University Advancement Procedures: Corporate Sponsorship* for more detailed information. (A copy may be accessed at: S:\Campus Merchants\Helpful Documentation\Corporate Sponsorships Process 2018.)

G. It is important that all campus merchants reconcile their payment card transactions. For POS transactions, the terminal settlement tape should be reconciled to the card processors' settlement report POS transactions. For internet transactions, the gateway reports should be reconciled to the banking reports, and third party reporting systems (if applicable). Banner fund and account numbers must be reviewed periodically to ensure that they accurately reflect reported sales, refunds, and fees. Departmental staff is responsible for reconciling the card transaction activity and accurately reporting those amounts to the University Cashiers through the deposit process. The merchant, not the Cashiers, is responsible for pulling the settlement reports, and reconciling the amounts. If the use of a generic merchant account is approved by eCO for a campus entity, eCO will provide the appropriate sales reports to the entity for the deposit; it is the merchant's responsibility to make the deposit.

H. The Cashier's Office will compare the sales amount submitted per the Payment Book Receipt (PBR) form to the merchant card processor records and banking funding reports. They will inform the merchant of discrepancies. All discrepancies should be resolved within 24 hours so that sales can be posted to the departmental account in the UNC Charlotte accounting system on a timely basis.

I. Access to eCommerce reporting systems must be requested by the merchant for the purpose of providing appropriate personnel with required reports for reconciliation, research, and deposit. Accesses will be restricted to the least privilege needed to perform job responsibilities. Access requests must be submitted to eCommerce@uncc.edu on the *EC-Access Request to Reporting Systems* form or at the following URL: https://imaging.uncc.edu/imagenowforms/fs?form=eCommerce_Systems_Access.

J. Merchants are responsible for investigating and responding to disputes, retrievals, and chargebacks, and should do so on a timely basis.

V. Additional Requirements for Point-of-Sale (POS) Transactions

K. All Card Present (CP) transactions must be captured on equipment approved by and/or obtained through eCO in conjunction with NC OSC. All card transactions will be processed on equipment compatible with the processing platform(s) of the University's merchant services provider. The University's merchant services provider is determined by UNC Charlotte in accordance with the NC OSC MSA.

L. Departments requiring customized equipment for POS transactions must contact eCO before such equipment is purchased, leased, rented, or utilized. The eCO will work in conjunction with University ITS to review and approve special requests. Additional information and/or external consultation may be required. The requestor will bear all external costs related to the exception approval process.

M. Current procedures for acceptance of CP (i.e. a face to face transaction) and CNP (i.e. a transaction accepted over phone or fax and entered manually into an approved POS device) transactions must be followed. Those may be referenced in the UNC Charlotte Merchant Manual (currently in development), or at the web sites of participating card companies (e.g., Visa, MasterCard, and American Express).

N. POS terminals must be protected from tampering and tracked. Physical access to and oversight over terminals shall be limited to personnel who have completed the Requirements for Card Processing. If terminals are customer facing, they should be monitored while in use and secured when not in use. Terminals must be inspected for tampering on a regular basis and reports associated with inspections returned to eCommerce on a monthly basis. Any suspicious behavior or indications of device tampering or substitution must be reported to eCommerce. If terminals fail and are replaced by the merchant through the merchant services provider, eCO must be notified. The identity of any third-party persons claiming to be repair or maintenance personnel must be verified, prior to granting them access to modify or troubleshoot devices. The eCO must be notified if third-party persons are granted access to terminals.

VI. Additional Requirements for Internet Transactions

O. All internet based Card Not Present (CNP) transactions must be captured on approved web interfaces. Any newly established processing setup for internet based transactions must utilize a designated University payment gateway and platform. TouchNet Information Systems, Inc. is the primary designated gateway processor and online transaction platform.

P. All payment card processing for the University will be coordinated through eCommerce. No individual department or campus entity shall enter into a contract which includes card processing functions or outsources card processing functions to a third party without approval of eCO in conjunction with ITS.

Q. Departments must contact eCO prior to purchase of specialized software or equipment so that customized processing applications are reviewed for compliance with standards, procedures, contract requirements, and feasibility. The eCO in conjunction with University ITS, the Office of Legal Affairs, Internal Audit Department, and the applicable computer support unit will work with the department to ensure that processing standards, safeguarding measures, and legal requirements are met. Additional information and/or external consultation may be required. The requestor will bear all costs related to the external review, if required, for the approval process.

R. Approved third party software/equipment must be implemented according to the third party guidelines. Default vendor passwords and settings must be modified to unique passwords or settings before the system is installed on the University network or utilized for card processing.

S. Customer CHD must be entered or captured on approved third party hosted websites or payment gateway interfaces and *not* on University computers or network resources.

T. All data requested and collected through online shopping carts and web portals must comply with the University Guideline for Data Handling.

U. If a merchant is processing card transactions online and has no approved means to accept card transactions at an event (in a face to face environment), they must either not accept payment at the event or accept cash or checks. If cash or checks are to be accepted, the merchant is responsible for following all cash handling policies (University Policy 602.4, Handling Cash, Checks, and Other Monetary Receipts). They will need to request a Receipt Book from the Cashiers to provide the required receipt to the customer for monies received at the event if the monies are to be deposited to a University account. If monies are to be deposited to a non-University account, a receipt must still be provided to the customer and supplied by the merchant. If the merchant would like to accept card transactions at the event, they must request through eCO the rental of an approved POS device (see: EC : POS Terminal Order Form) or the use of a laptop or desktop computer as a virtual terminal. The completion and submission of the *EC-Request for Virtual Terminal for Card Processing* form will be required for laptop use.

VII. Outsourcing/Third party Contract Requirements

A. Any unit that wishes to utilize third party software that includes card processing functions or the outsourcing of its credit card transaction processing must request approval to do so in writing to eCommerce@uncc.edu. The vendor selected by the campus entity must be approved through eCO and meet current requirements. Contracts and associated documentation must address these elements:

1. Compliance with all appropriate PCI SSC requirements (Payment Card Industry Data Security Standards (PCI DDS), the Payment Application Data Security Standard (PA-DSS), and the Pin Transaction Security Requirement (PCI- PTS)).

2. Compliance with NC Daily Deposit Act (NC G.S. 147-77)
3. Statements clarifying where CHD is captured; specifically, detailed information regarding integration with the designated gateway provider and linkage type must be disclosed.
4. If CHD is captured on the vendor's network, they must:
   a. Provide proof of PCI validation and/or PA-DSS validation. It is preferred that any third party that captures CHD be a validated Level 1 Service Provider.
   b. Specify the elements of the PCI DSS for which they will be responsible and those for which the University must be responsible.
   c. Provide documentation which clearly details the flow of CHD and specifies any outside entities' applications or servers utilized.
5. Service level agreements
6. Remote access and use of Multi Factor Authentication
7. Personally Identifiable Information (PII)
8. Data retention and destruction
9. Liability
10. Business continuity

B. All contracts must be submitted to eCO for review and revision, as necessary, before they are executed. ITS, The Office of Legal Affairs, and Materials Management will be integral in the review process. ITS will oversee the final approval, signature, and execution of contracts that involve ITS resources.

C. Any third party agreement that involves ITS resources must comply with IT Governance processes. A review of those may be located at IT Governance.

D. A final copy of the executed contract must be submitted to eCommerce.

VIII. Review Process for Processing Request

A. Requests for card processing must be submitted to eCommerce@uncc.edu using the *EC-Application to Process Payment Cards (EC-APP) (path: S:\Campus Merchants\eCommerce Forms\ EC-APP - Application to Process Payment Cards)* form. The application includes requirements to:

1. Document the business need for accepting credit card transactions in a new unit or location.
2. Document anticipated transaction volume and mechanism for card acceptance.
3. Agree to basic rules for card processing.
4. Obtain approval of the business manager.

B. The eCO will review submitted requests and confer with ITS as needed. Requests will be reviewed for feasibility, functionality, compliance, and business operations.

C. Third party contracts associated with the request must be submitted to eCO and will be reviewed by eCommerce, ITS, Legal, and Materials Management as needed. All contracts meet federal, state, PCI DSS, and University contractual requirements.

IX. Incident Response

A. Report any suspected or known security incident to:

   a. Your supervisor and/or primary merchant contact for your area.

   b. ITS. See the following resources below:

      i. Guideline for Reporting Information Security Incidents: https://itservices.uncc.edu/iso/guideline-reporting-information-security-incidents

      ii. FAQ: How do I report an IT security incident? https://spaces.uncc.edu/pages/viewpage.action?pageId=11928016

B. Note: If the potential information security incident involves a compromised computer system:

   a. Leave the computer system on and as-is, with all current computer programs running and current state of network access.

   b. Do not shut down the computer, restart the computer, or remove the computer from the network until/unless directed to do by the ITS incident response team.

C. If the incident involves criminal activity, report it immediately to the UNC Charlotte Police and Public Safety Office.

D. Notify the Data Security Officer (DSO) or Information Security Liaison (ISL) for your college or department. Designated DSOs and ISLs are listed at: https://itservices.uncc.edu/security.

E. ITS and the eCommerce Office will co-ordinate review for any incident which involves CHD and escalate if deemed incident is valid and meets threshold for escalation.

F. All merchant/departmental entities involved are expected to cooperate fully and in a timely manner with any investigation.

X. Exceptions to Regulation

A. Any request for an exception to the UNC Charlotte Payment (Credit/Debit) Card Processing Standard or UNC Charlotte Payment (Credit/Debit) Card Processing Procedures should be made in writing to the VCBA and CIO and include the following::

   1. Reason for the exception request.
   2. Steps that will be taken to ensure compliance with the standard.
   3. Date the need for the exception will be no longer needed.

B. The eCO in conjunction with University ITS will work with the VCBA and the CIO to review the request for exception. Following a review of the request, the final approval or denial will be made by the VCBA.

Related Resources

Legal References:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Payment Card Industry Security Standards Council (PCI SSC)
- North Carolina State Laws and Regulations
    - NC G.S. 147-77 (Daily Deposit Act)
    - NC Session Law 99-434
    - NC OSC Policy 500.1 (Maximization of Electronic Payment)
    - NC OSC Policy 500.2 (Master Services Agreements for Electronic Payments)
    - NC OSC Policy 500.10 (Merchant Cards Security Incident Plan)
    - NC OSC Policy 500.11 (Compliance with PCI Data Security Standards)
    - NC OSC Policy 500.13 (NC Security and Privacy of Data)

Other References:

- American Express Merchant Regulations
- ECommerce Glossary
- MasterCard Merchant Acceptance Guide
- UNC Charlotte Guideline for Data Handling
- UNC Charlotte Guideline for Reporting Information Security Incidents
- UNC Charlotte Payment (Credit/Debit) Card Processing Standard
- UNC Charlotte Policy 101.23, Employment-Related Background Checks and Criminal Activity Reporting
- UNC Charlotte Policy 307 Responsible Use of University Computing and Electronic Communication Resources
- UNC Charlotte Policy 311 Information Security
- UNC Charlotte Policy 602.4, Handling Cash, Checks, and Other Monetary Receipts
- UNC Charlotte Standard for Information Classification
- UNC Charlotte Standard for Managing Information Security Incidents
- Visa - Card Acceptance Guidelines

Please note: eCommerce forms may be located on the campus S drive at: S:\Campus Merchants\eCommerce Forms

Revision History:

Initially approved October 5, 2006

Revised: 4/30/2015, 8/15/2016, 4/30/2018