

**UNIVERSITY OF NORTH DAKOTA  
FINANCE & OPERATIONS POLICY LIBRARY**

**ACCEPTING CREDIT CARDS AND ELECTRONIC CHECKS  
TO CONDUCT UNIVERSITY BUSINESS**

*Interim Policy*

Section 2, Finance

Policy 2.3, Accepting Credit Cards and Electronic  
Checks to Conduct University Business

Responsible Executive: VP Finance & Operations

Responsible Office: Student Account Services

Issued: June 19, 2009

Latest Review / Revision:



---

## POLICY STATEMENT

All University of North Dakota departments and colleges that conduct electronic-based financial transactions for the University, which include credit/debit card or electronic check (eCheck) transactions, must be compliant with: Payment Card Data Industry Standards (PCI DSS), all applicable laws and mandates, and North Dakota University System and UND policies and procedures.

---

## REASON FOR POLICY

The University recognizes that accepting credit cards as payment for goods or services has become a common practice that improves customer service, brings certain efficiencies to UND's cash collection process, and may increase the sales volume of some types of transactions. In addition, the use of technology, such as the World Wide Web, provides easy access for many, and the use of credit cards is essential when sales are conducted electronically.

---

## SCOPE OF POLICY

This policy applies to all members of the University community and should be read by:

- |                                       |   |
|---------------------------------------|---|
| ✓ President                           | ✓ Staff   |
| ✓ Vice Presidents                     | ✓ Students  |
| ✓ Deans, Directors & Department Heads | ✓ Others: all those handling electronic fund transactions |
| ✓ Area Managers & Supervisors         |   |
| ✓ Faculty                             |   |

---

## WEB SITE REFERENCES

This policy: <http://www.und.edu/dept/policyoffice/html/finance.html#bus>

Policy Office: <http://www.und.edu/dept/policyoffice>

Vice President for Finance & Operations: [www.und.edu/dept/vpfo](http://www.und.edu/dept/vpfo)

Student Account Services: <http://www.und.edu/dept/studentaccounts/>

## CONTENTS

<b>Policy Statement</b> .....	<b>1</b>
<b>Reason for Policy</b> .....	<b>1</b>
<b>Scope of Policy</b> .....	<b>1</b>
<b>Web Site References</b> .....	<b>1</b>
<b>Related Information</b> .....	<b>3</b>
<b>Contacts</b> .....	<b>3</b>
<b>Definitions</b> .....	<b>4</b>
<b>Principles</b> (overview) .....	<b>5</b>
<b>Procedures</b> .....	<b>7</b>
Obtaining Authorization to Accept Credit Card Payments .....	7
Methods of Processing Transactions .....	7
Refunds .....	8
Disputed Charges/Chargebacks .....	8
Recording and Reconciling Credit Card Transactions .....	8
Retention Periods .....	8
Network Scans .....	9
PCI Self Assessment Questionnaire .....	9
<b>Responsibilities</b> .....	<b>10</b>
<b>Forms</b> .....	<b>11</b>
<b>Revision Record</b> .....	<b>11</b>

RELATED INFORMATION

<b>Gramm Leach Bliley Act</b>	<a href="http://www.ftc.gov/privacy/privacyinitiatives/glbact.html">http://www.ftc.gov/privacy/privacyinitiatives/glbact.html</a>
<b>Payment Card Industry Standards</b>	<a href="https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml">https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml</a> <a href="http://www.discovernetwork.com/fraudsecurity/disc.html">http://www.discovernetwork.com/fraudsecurity/disc.html</a> <a href="http://www.mastercard.com/us/merchant/index.html">http://www.mastercard.com/us/merchant/index.html</a> <a href="http://usa.visa.com/merchants/risk_management/cisp_merchants.html">http://usa.visa.com/merchants/risk_management/cisp_merchants.html</a> <a href="https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&amp;page=processingMain&amp;us_nu=subtab">https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&amp;page=processingMain&amp;us_nu=subtab</a>
<b>NDUS 1912.1 Information Security Procedures</b>	<a href="http://www.ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2586">http://www.ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2586</a>
<b>Incident Response Policy</b>	<a href="http://itsecurity.und.edu/policy">http://itsecurity.und.edu/policy</a>
<b>SBHE 802.7 Identity Theft Prevention</b>	<a href="http://www.ndus.nodak.edu/Uploads/proposedpolicies/9/802.7.PDF">http://www.ndus.nodak.edu/Uploads/proposedpolicies/9/802.7.PDF</a>
<b>UND Identity Theft Prevention Program</b>	Under review
<b>"What To Do If Compromised" VISA USA Fraud Investigations and Incident Management Procedures</b>	<a href="http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html">http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html</a>

CONTACTS

General questions about this policy can be answered by your department’s administrative office. Specific questions should be directed to the following:

<b>Subject</b>	<b>Contact</b>	<b>Telephone</b>	<b>E-Mail / Web Address</b>
Policy Content	Student Account Services	(701) 777-2967	<a href="mailto:emilygoodoien@mail.und.nodak.edu">emilygoodoien@mail.und.nodak.edu</a>
Authorization to Accept Credit Cards	Student Account Services	(701) 777-2967	<a href="mailto:emilygoodoien@mail.und.nodak.edu">emilygoodoien@mail.und.nodak.edu</a>
Authorization to establish Touchnet Marketplace uPay or uStores site	Student Account Services	(701) 777-2967 (701) 777-4131	<a href="mailto:emilygoodoien@mail.und.nodak.edu">emilygoodoien@mail.und.nodak.edu</a> <a href="mailto:lisaheher@mail.und.nodak.edu">lisaheher@mail.und.nodak.edu</a>
Credit Card Fees	Student Account Services	(701) 777-2967	<a href="mailto:emilygoodoien@mail.und.nodak.edu">emilygoodoien@mail.und.nodak.edu</a>
Disputed Charges	Bank of North Dakota	(800) 472-2166 Ext. 85630	<a href="mailto:dwblumhagen@nd.gov">dwblumhagen@nd.gov</a>
Equipment Problems	Bank of North Dakota	800) 472-2166 Ext. 85630	<a href="mailto:dwblumhagen@nd.gov">dwblumhagen@nd.gov</a>
Recording & Reconciling Transactions	Student Account Services	(701) 777-2967	<a href="mailto:emilygoodoien@mail.und.nodak.edu">emilygoodoien@mail.und.nodak.edu</a>

**DEFINITIONS**

<b>Credit Card Processing Machine</b>	A machine or device used to process credit card transactions. <i>Examples may include: Trans330, Trans380, Trans460, Omni3200SE.</i>
<b>Department</b>	A UND department that accepts credit cards to conduct business.
<b>Electronic Funds Transaction</b>	The term is used for a number of different concepts, such as cardholder-initiated transactions, where a cardholder makes use of a payment card (e.g., credit or debit card); electronic payments by businesses, individuals, or students, using electronic check clearing (banking information).
<b>Gramm Leach Bliley Act</b>	Key rules under the Act govern the collection and disclosure of customers' personal financial information.
<b>Payment Card Industry (PCI) Standards</b>	A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. For more information, visit <a href="https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml">https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml</a>
<b>Payment Card Industry Assessment Survey</b>	Departments accepting credit card transactions must complete a Payment Card Industry Standard Assessment survey on an annual basis, or as requested. This survey assesses whether the department is in compliance with the required PCI standards. The Assistant Controller will distribute the survey annually to departments, or at the time the department is approved to accept credit cards.
<b>Touchnet Marketplace uPay &amp; uStore site</b>	Third party vendor and software that enables University departments to build and operate secure web-based shopping cart applications and online payment pages. It uses Touchnet Payment Gateway for electronic payment processing.
<b>Touchnet Paypath</b>	Third party vendor and software for campus online billing and payment processing which follow applicable PCI DSS standards and guidelines. This includes payments for student accounts on Campus Connection.

## PRINCIPLES

**OVERVIEW** – Many departments on campus process credit card transactions, either infrequently or in the course of daily business. It is the University's responsibility to protect the privacy of its customers, as well as maintain compliance with the Gramm Leach Bliley (GLB) Act and Payment Card Industry (PCI) Standards.

All University of North Dakota departments and colleges that conduct electronic-based financial transactions for the University, which include credit/debit card or electronic checks (eChecks) transactions, must be compliant with: Payment Card Industry Data Security Standards (PCI DSS), all applicable laws and mandates, and North Dakota University System and UND policies and procedures. Failure to be compliant in all areas may result in the revocation of departmental authorization to accept electronic-based financial transactions and departmental responsibility for paying all related penalties. Currently, PCI DSS only applies to credit card transactions.

Departments must obtain prior approval to accept electronic-based financial transactions. Requests should be submitted to the Assistant Controller and should request one of the following:

1. Credit card machines approved through Student Account Services
2. TouchNet PayPath or Touchnet Marketplace uPay or uStores
3. UND approved third party vendor

Exceptions to this policy may be granted only after a written request from the department has been reviewed and approved by the Controller, or designee.

Credit cards for student accounts receivable payments are only accepted online via Campus Connection via Touchnet Paypath. Currently, VISA is not an accepted online payment option via Campus Connection for accounts receivable payments. Exceptions may be made for payments made by federal agencies and processed by Student Account Services, as determined by the Controller or Assistant Controller.

**ACCEPTABLE CREDIT CARDS** – The University is required to process credit card transactions through the Bank of North Dakota. Any exceptions must be approved, in writing, by the Bank of North Dakota. All requests to contract with a processor other than the Bank of North Dakota must be approved in advance by the Assistant Controller.

Credit card types that departments may request to be accepted within the department or via their Touchnet Marketplace site for goods and services include MasterCard, VISA, Discover, and American Express. Departments must request approval from Student Account Services to accept electronic payments, such as eChecks and credit cards.

**CREDIT CARD FEES** – The University is charged fees on all credit card transactions. The fees vary and are based on the card type accepted and the method of acceptance (swiped versus manually entered). In addition to a percentage on the amount of the transaction, a “per transaction” fee and a monthly merchant account fee is charged. Merchant fees for credit card transactions for student accounts receivable payments via Campus Connection are not assessed to the university, but instead, a convenience fee is assessed to the student at the time of the transaction.

Merchant fees assessed to the university are generally charged to the funding source that the revenue is credited to at the time of the transaction. Fees will be charged to the departmental fund via journal entry/import on a monthly basis by Student Account Services.

As departments are developing rates (fees for goods or services) they should recognize the credit card merchant fee as a cost of doing business. Should the department choose to recover the fee, they must build it into the overall rate structure. In other words, departments processing transactions on a credit card machine or through Touchnet Marketplace cannot assess a convenience fee or any other additional fee to the customer if the customer pays via a credit card. Discounts for using a payment method, other than credit cards, are not allowed (i.e. discount for paying by cash/check).

## PRINCIPLES, *Continued*

**SECURITY** – Departments must remain compliant with Payment Card Industry Data Security Standards (PCI DSS), all applicable laws and mandates, and North Dakota University System and UND policy and procedures.

If a department suspects that credit card records may have been compromised in any way, whether through malicious intent or due to a weakness in the handling and processing of credit card transactions, they are to notify the Controller or Assistant Controller immediately.

All security incidents will follow the [UND Incident Response Policy](#). “[What to do if Compromised](#)”, VISA USA Fraud Investigations and Incident Management Procedures will be utilized as a reference for any security incident.

In order to accept credit cards online for goods or services, departments must first consider establishing a Touchnet Marketplace uPay or uStores site. If a department feels that Touchnet Marketplace will not serve their needs, approval to contract with a third party vendor must be obtained in advance from the Assistant Controller. This written request should include justification as to the reasons Touchnet Marketplace would not serve their needs. In addition, prior to entering into a contract with a third party vendor, the department and the third party vendor must have a secured website and must provide certification that the internet site/provider is PCI compliant and will remain compliant. This certification should be obtained from the internet provider and submitted to the Assistant Controller. Certification must be provided on an annual basis, or as requested.

**NOTE:** *UND is currently developing policies and procedures for employee background checks. Once the policy is finalized, it will be incorporated into the credit card policy. Departments must adhere to NDUS and UND policy and procedures regarding background checks for employees having access to electronic payment information.*

## PROCEDURES

### Obtaining Authorization to Accept Credit Card Payments

Departments must obtain prior approval from Student Account Services to accept and/or process electronic check payments or credit card transactions (via credit card machine, online via Touchnet Marketplace, or processed through any other third party vendor). Requests should be made via email to the Assistant Controller. If approved, Student Account Services will assist the department in obtaining the required information or equipment, such as a merchant ID number or credit card processing machine. Student Account Services will also assist in providing the department with procedures for processing credit card deposits and reconciling on a daily basis. If a department has not obtained approval to accept and process credit card payments, they should not be accepting credit card information.

Departments must ensure that procedures are followed and PCI Data Security Standards are met. Access to system components, banking information, and cardholder data should be limited to only those individuals whose jobs require such access. Departments are responsible for providing their employees with policies and procedures to ensure compliance with PCI Data Security Standards and UND policies and procedures.

All paper and electronic media that contain cardholder data should be physically secure and confidential. All cardholder data should be disposed of according to records retention policy and PCI Data Security Standards. Documents should be cross-cut shredded or incinerated so that cardholder data or financial information cannot be reconstructed.

### Methods of Processing Transactions

The acceptable methods for processing credit card transactions include:

1. In person.
2. By telephone – if the CVV code is obtained from the back of the card, it must be destroyed after the transaction is processed; must verify the address if sending merchandise; may choose to have return receipt to confirm delivery of goods.
3. By fax – only if fax machine is in a secure, limited access location, accessible only by authorized personnel.
4. By mail – this is not the preferred method. All documents containing cardholder data must be secure and disposed of according to records retention and PCI Data Security Standards. No storage of magnetic stripe data, CVV, PIN, or other similar information may be retained.
5. Touchnet Marketplace uPay or uStores site – must obtain advance approval to establish a uPay or uStores site.

Credit card information must not be requested or sent electronically (i.e. email, instant messaging). If the cardholder sends credit card information electronically, departments may still process the transaction, but should reply to the cardholder with the following verbiage:

*"It is important that UND protects the privacy of our customers, and therefore, does not accept credit card information electronically, as the email system is not a secured site. Please discontinue sending credit card information electronically. Please contact the department providing the goods or services to request available payment options."*

Departments should attach a copy of the response to the merchant copy of the transaction being processed and retain in accordance with the records retention policy.

When issuing credits to customers, the credit should be processed in the same payment method as the original charge. Exceptions should be approved by the departmental head/manager on a case-by case basis.

## PROCEDURES, *Continued*

**Departments must not store any credit card information, including CVV codes or PIN numbers, in a customer database or electronic spreadsheet. All CVV codes, PIN numbers, and other documents containing credit card information, must be shredded immediately after the transaction has been processed. It is in violation with PCI Data Security Standards to store magnetic stripe (i.e. track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data after transaction authorization on any systems.**

- Magnetic strip data is data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.
- CAV2, CVC2, CID, or CVV2 data are the three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.
- PIN data is the personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transactions message.

### Refunds

When an item or service is purchased using a credit card, and a refund is necessary, the refund should be credited to the credit card from which the purchase was made. Exceptions should be approved by the departmental head/manager on a case-by case basis.

### Disputed Charges / Chargebacks

Occasionally, the Bank of North Dakota will send notification to the University indicating a disputed charge. A copy of this chargeback notification will be forwarded to the appropriate department by Student Account Services. The department is required to provide all requested information in response to the notification by the due date indicated. Failure to provide requested information in a timely manner will result in the department being charged for the transaction in question and the department cannot appeal the chargeback.

### Recording and Reconciling Credit Card Transactions

When submitting deposits to Student Account Services, the credit card deposit form should be submitted with:

1. Daily Totals Report - this includes only the totals for MasterCard, VISA, Discover, and American Express; no credit card numbers are included.
  - This report should be printed twice (one copy for Student Account Services, and one copy is to be retained by the department)
2. Daily Settlement Report - this indicates the amount settled successfully; no credit card numbers are included.
  - Departments should transmit and settle their batches daily.

### Retention Periods

Documents supporting the credit card transaction must be retained by the department according to the University's Records Retention Policy, the Payment Card Industry (PCI) Data Security Standards, and this policy.

Departments are considered to be the originating department and should retain the following documents for receipts processed with a Tender Type of Credit Card:

1. The merchant copy of the sales slip, which includes the signature, should only include the last four digits of the credit card number. The Primary Account Number (PAN) should be masked.
  - Retention period is current fiscal year plus two prior fiscal years.
2. Daily Totals Report - includes only the totals for each card type (MasterCard, VISA, Discover, and American Express); no credit card numbers are included.
  - Retention period is current fiscal year plus two prior fiscal years.

## PROCEDURES, *Continued*

3. Daily Detail Report - this includes the entire credit card number for all transactions.
  - Retention period is current fiscal year plus two prior fiscal years.

Student Account Services retains the following documents for receipts processed with a Tender Type of Credit Card:

1. Daily Totals Report - includes only the totals for each card type (MasterCard, VISA, Discover, and American Express); no credit card numbers are included.
  - Retention period is current fiscal year plus two prior fiscal years.
2. Daily Settlement Report – this indicates the amount settled successfully; no credit card numbers are included.
  - Retention period is current fiscal year plus two prior fiscal years.

For Touchnet Marketplace transactions, departments should retain the following:

1. Merchant Revenue Report
  - Retention period is current fiscal year plus two prior fiscal years
2. uPay Revenue Report
  - Retention period is current fiscal year plus two prior fiscal years

All transaction documents, as stated above, must be secured by the department, for example, in a locked cabinet/room with limited access.

### Network Scans

Departments using networks or servers for credit cards transactions should have quarterly network scans by an approved vendor. These scans may also be requested by the Bank of North Dakota on a periodic basis. All fees associated with the network scans are the responsibility of the individual department.

### PCI Self Assessment Questionnaire

Departments are required to complete a PCI Self Assessment Survey on an annual basis and submit to the Assistant Controller. Departments are required to submit a revised survey if there have been any changes since the last survey or if requested by the Bank of North Dakota or by Student Account Services.

## RESPONSIBILITIES

<b>Department Accepting Credit Cards for Goods or Services</b>	<ul style="list-style-type: none"><li>▪ Request/obtain prior approval from Student Account Services to accept and/or process eChecks and credit card transactions or to establish a Touchnet Marketplace uPay or uStores site.</li><li>▪ Must adhere to all university policies and procedures addressing electronic check and credit card transactions.</li><li>▪ Submit an annual PCI Assessment Survey or a revised survey if there have been any changes since the last survey or if requested by the Bank of North Dakota or by Student Account Services.</li><li>▪ Must be in compliance with PCI Data Security Standards regarding credit card transactions.</li><li>▪ Notify Student Account Services immediately if there is a suspicion that credit card records may have been compromised in any way.</li><li>▪ Follow UND Incident Response Policy and VISA’s “What To Do If Compromised” procedures.</li><li>▪ Obtain approval in advance if accepting eChecks or credit card information over the internet from a third party vendor.</li><li>▪ Must provide training and applicable information to all employees that are associated with processing credit card transactions to ensure department remains compliant with PCI Data Security Standards and university policies and procedures regarding electronic check and credit card transactions.</li><li>▪ Should take merchant fees and network scans into consideration when determining rates for goods and services.</li><li>▪ Must follow the procedures for processing credit card deposits.</li><li>▪ <b>Departments must not store any credit card information, including CVV codes or PIN numbers, in a customer database or electronic spreadsheet. All CVV codes, PIN numbers, and other documents containing credit card information, must be shredded immediately after the transaction has been processed. It is in violation with PCI Data Security Standards to store magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data after transaction authorization on any systems.</b></li><li>▪ Reconcile and transmit credit card transactions on a daily basis.</li><li>▪ Retain required electronic payment information, including credit card documents in a secured location according to the Records Retention policy, PCI Data Security Standards, and this policy.</li><li>▪ Do not request electronic payment information, including credit card information, via email. When this information is received by the department via email, departments are required to notify the sender to discontinue sending credit card information via email, as it is not a secured location. This notification should be attached to the merchant copy of the transaction for credit card transactions.</li><li>▪ When disposing of credit card or electronic check information, all documents must be shredded according to Records Retention and PCI Data Security Standards.</li></ul>
<b>Student Account Services</b>	<ul style="list-style-type: none"><li>▪ Grant authorization to departments to accept and process credit card or electronic check transactions or to establish a Touchnet Marketplace uPay or uStores site.</li><li>▪ Assist in developing departmental procedures for daily reconciling of electronic payments (eChecks and credit card transactions).</li><li>▪ Retain documents supporting credit card transactions, as required.</li></ul>

## FORMS

---

<b>Deposit Form</b>
---------------------

<a href="http://www.und.edu/dept/studentaccounts/html/employeeforms.htm">http://www.und.edu/dept/studentaccounts/html/employeeforms.htm</a>
---

---

## REVISION RECORD

06.19.09 – Policy Implementation with Interim status