POLICY SECTION 509: Electronic Financial Transaction Procedures

Source: NDSU President
NDSU VP for Finance and Administration
NDSU VP for Information Technology

A. Purpose / Rationale
Many NDSU departments 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 and ensure that all electronic financial transactions and payments of North Dakota State University will be compliant with

- Payment Card Industry Data Security Standards (PCI DSS);
- All applicable federal and state laws and mandates; and
- North Dakota University System and North Dakota State University (NDSU) policies and procedures, most notably: NDSU Policy, Section 509: Electronic Financial Transactions

B. Scope
These procedures apply to all North Dakota State University (NDSU) faculty, staff, students, organizations, and individuals who on behalf of the University handle electronic financial transactions and payments such as credit/debit card transactions, and electronic fund transactions (EFT). This includes any electronic financial transactions conducted at all North Dakota State University campuses and locations.

Failure to be compliant in all areas may result in the revocation of authorization to accept electronic-based financial transactions and the department will be responsible for paying all related penalties.

C. Procedures for Obtaining a Service or System for Electronic Online Payments

1. All electronic financial transaction activities and payment technologies of NDSU must comply with the Payment Card Industry Data Security Standards (PCI DSS) as described in NDSU Policy, Section 509. No activity or technology may obstruct compliance with these standards.

2. NDSU departments (divisions, colleges, departments, groups, organizations) must have approval from NDSU Customer Accounts Services before accepting electronic-based financial transactions. To request approval, one of the forms listed below which best fits your needs must be completed and submitted to the NDSU Customer Accounts Services department. A Touchnet Marketplace uPay or uStore site is the preferred choice for credit card online transactions.
   a. Departmental Request to Process Credit Card Transactions utilizing a Dial-up Credit Card Machine
   b. Departmental Request for Touchnet Marketplace
   c. Departmental Request for Other 3rd Party Online Processor

3. If a department has not obtained approval to accept and process credit card payments, they cannot accept and/or store credit card information.

4. The acceptable methods for processing credit card transactions are
a. In person;
b. By telephone;
c. An online TouchNet Marketplace uPay or uStores site or other NDSU approved third-party vendor.

5. 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 VP for Finance and Administration and the VP for Information Technology.

6. Credit card types that NDSU departments may request to be accepted within their department or their TouchNet Marketplace site for goods and services include MasterCard, VISA, Discover, and American Express (AMEX). There is additional setup involved for AMEX.

7. 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 account fee is charged. Merchant fees assessed to the University are charged to the funding source and the revenue is credited to the entity at the time of the transaction. Fees will be charged to the department fund via a journal entry/import on a monthly basis by NDSU Customer Account Services.
   a. As departments are determining rates (fees for goods and or services) they should recognize the credit card merchant fee as a cost of doing business. If the entity wishes to recover the fee, they must build it into the overall rate structure.
   b. 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.
   c. Discounts for using a payment method, other than credit cards, are not allowed (i.e., discount for paying by cash/check).

8. Prior to entering into a contract with a third-party vendor, the third-party vendor must have a secure Web site and must provide certification and attestation that they are PCI compliant, their payment application is PA-DSS compliant and will remain compliant during the business relationship. These requirements must be obtained from the third-party vendor and submitted to Customer Account Services for verification. Certification and attestation must be provided on an annual basis, or as requested.

9. The University will contractually require all third party vendors with access to cardholder data to adhere to PCI DSS. The contracts will clearly define information security responsibilities for the vendors. The NDSU General Counsel will review and approve such contracts as required by NDSU Policy 712 and NDUS Policy and Procedure 840. Third party vendors will provide documentation of compliance to NDSU. This documentation will be provided in a timely manner according to the level of certification.

10. Once approved, NDSU Customer Account Services will assist the department in obtaining the required information and/or equipment such as a merchant ID number, TouchNet Marketplace uStore or uPay site, and/or credit card processing machine.
D. Credit Card Data Transmission, Storage and Retention Procedures

1. Departments are considered to be the originating entity and should retain receipts processed with a Tender Type of Credit card.

2. If accepting credit card transactions via telephone, and the credit card or account number, expiration date and CVV code is required to complete the transaction:
   a. The credit card data must be destroyed after the transaction is processed. It cannot be saved and stored electronically or in paper format.
   b. If the transaction is for merchandise to be sent to the recipient, the address must be verified;
   c. The NDSU entity may choose to have a return receipt to confirm delivery of the goods.
   d. If credit card data must be retained after purchase has been made for the purpose of refunds or other,
      i. Only the truncated last four digits of the credit card number;
      ii. The name on the credit card, and the address can be retained;
      iii. This data can only be kept according to standards established by the NDSU Data Records Retention Policy 713;
      iv. The data must be kept in a locked file cabinet in a secure, locked area that only those who have a need to have access have entry to.

3. It is prohibited for those departments using an online payment system with a third-party payment Website (including, but not limited to Touchnet Marketplace)
   a. To enter credit card information on behalf of the customer by department personnel;
   b. Work computers (those computers provided for general business related to the department and the duties of the person to whom it is assigned) may not be used to enter credit card payments online on behalf of the customer.
   c. To provide a computer or device in their offices or place of business specifically for customers to use for submitting online credit card payments;
   d. Customers, when in the presence of employees and in the office or place of business, and preferring to submit a payment online via a Website, must be instructed to make that type of payment from their personal computer or other personally owned device;
   e. Departments wishing to use electronic smart phones, tablets, and other mobile devices to online payments must request and obtain permission from Customer Account Services.
   f. Payment terminals with a swipe device must be segregated and dedicated solely for the use of processing electronic payments.

4. Credit card information must not be requested or sent electronically (i.e., email, instant messaging, texting, phone, voice mail, etc.). If the cardholder sends information electronically, departments may NOT process the transaction, but must securely delete the card information and contact the card holder to inform them that the method they chose is not a secure means of sending credit card data and to collect their card information via phone.

5. NDSU departments must not store or transfer any credit card information, including CVV codes or PIN numbers, in a customer database, electronic spreadsheet, or paper format. All documents containing credit card information must be cross-shredded or incinerated.
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, or CVV2 data, or PIN data after transaction authorization on any electronic systems. The only elements of track data that may be retained are a truncated (last 4 digits only) account number, expiration date and name.

6. All paper and electronic media that contain cardholder data that is required to be retained must be physically and electronically secure and classified as confidential. All cardholder data will be disposed of according to NDSU Records Retention Policy 713 and PCI Data Security Standards. Paper documents must be cross-shredded or incinerated so that cardholder data or financial information cannot be reconstructed.

E. Refunds and Disputed Charges Procedures

1. When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the credit card from which the purchase was made. Exceptions need to be approved by the department head/manager on a case-by-case basis. Refunds needed through Touchnet Marketplace are to be processed by Customer Account Services.

2. Occasionally, the Bank of North Dakota will send a notification to the University indicating a disputed charge. A copy of this chargeback notification will be forwarded to the appropriate department by Customer 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.

F. Recording and Reconciling Credit Card Transactions Procedures

1. Customer Account Services will assist in providing the entity with procedures for processing credit card deposits and daily reconciliation.

2. Departments using Touchnet Marketplace are required to submit the “Monthly Marketplace Sales Report” within the first five business days of the next month. eCheck sales must be reported separately from credit card sales in order to facilitate proper charging of credit card sales.

3. Departments using credit card machines or third-party online vendor for processing credit card transactions need to submit reports on a weekly basis. Reports are due by Wednesday for the week prior. Reports for the final week/days of the month are due by the third business day of the next month. If the end of the month falls mid-week, that week should be split for reporting purposes.

4. When submitting weekly reports to Customer Account Services, the credit card report form should be submitted with

   a. Daily Totals or Daily Settlement Report – this includes only the totals for MasterCard, VISA, Discover, and AMEX. No credit card numbers are included.
      i. This report should be printed twice (one copy for Customer Account Services, and one copy is to be retained by the department).
      ii. It is required that departments transmit and settle their batches daily.
G. Network Scans for PCI Compliance
1. Departments using networked servers and computers for credit card transactions must have quarterly network vulnerability scans performed 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 vulnerability scans are the responsibility of the individual department.

H. PCI Self-Assessment Questionnaire
1. Departments are required to complete a PCI Self-Assessment Survey on an annual basis and submit it to Customer Account Services. Departments are required to submit a revised survey if there have been any changes since the last survey and before the next survey is due or if requested by the Bank of North Dakota or by Customer Account Services.

I. Department and Employee Responsibilities
1. To minimize the risk of compromise and misuse from internal sources, all NDSU employees who work with electronic financial transactions and the personal data associated with it will:
   a. Have completed criminal background checks;
   b. Have completed data privacy training;
   c. Have signed the Employee Credit Card Security Agreement.

2. Departments are responsible for providing their employees with policies and procedures to ensure compliance with PCI Data Security Standards and NDSU policies and procedures.

3. Departments using financial transaction processing systems and applications will
   a. Administer user accounts, including additions, deletions and modifications.
   b. Monitor and control all access to data.
   c. Remove access to all systems and services when an employee leaves or transfers to another campus department.

4. NDSU college or department heads or their designees will
   a. Ensure that all of their employees and business processes comply with this policy and related procedures.
   b. Be responsible for protection of protected data provided by the customer.
   c. Identify positions that require access to cardholder data and allow access as appropriate on a need to know basis.
   d. Ensure their employees are aware of the importance of electronic financial transaction information security.

5. NDSU Customer Account Services and the NDSU IT Security Office will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions. Both will conduct an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.

6. For those departments that want to perform credit card transactions from a wireless mobile device, please follow the procedures outlined in the document, “Accepting Credit Card Payments via Mobile Devices.”
J. Exceptions
1. Exceptions to this procedure may be granted only after a written request from the unit have been reviewed and approved by the Vice President for Finance and Administration and the Vice President for Information Technology Services or their designees.

K. Contacts
1. General questions about this document can be answered by your department’s administrative office. Specific questions should be directed to the appropriate area listed below.

<table>
<thead>
<tr>
<th>Policy/Procedure Content</th>
<th>Customer Account Services or IT Security Officer</th>
<th>(701)-231-7545</th>
<th>(701)-231-5870</th>
<th><a href="mailto:Carrie.a.petersen@ndsu.edu">Carrie.a.petersen@ndsu.edu</a> or <a href="mailto:Theresa.semmens@ndsu.edu">Theresa.semmens@ndsu.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Request to process Credit Cards</td>
<td>Customer Account Services</td>
<td>(701)-231-7545</td>
<td><a href="mailto:Carrie.a.petersen@ndsu.edu">Carrie.a.petersen@ndsu.edu</a></td>
<td></td>
</tr>
<tr>
<td>Assessment of Credit Card Fees</td>
<td>Customer Account Services or Accounting</td>
<td>(701)-231-7545</td>
<td><a href="mailto:Carrie.a.petersen@ndsu.edu">Carrie.a.petersen@ndsu.edu</a> or <a href="mailto:Jill.unruh@ndsu.edu">Jill.unruh@ndsu.edu</a></td>
<td></td>
</tr>
<tr>
<td>Recording &amp; Reconciling Transactions</td>
<td>Customer Account Services</td>
<td>(701)-231-7545</td>
<td><a href="mailto:Carrie.a.petersen@ndsu.edu">Carrie.a.petersen@ndsu.edu</a></td>
<td></td>
</tr>
<tr>
<td>Equipment problems</td>
<td>Bank of North Dakota</td>
<td>(800) 472-2166</td>
<td><a href="mailto:bndmerchantcard@nd.gov">bndmerchantcard@nd.gov</a></td>
<td></td>
</tr>
<tr>
<td>IT Network Security and Network Scanning</td>
<td>Chief IT Security Officer</td>
<td>(701) 231-5870</td>
<td><a href="mailto:Theresa.Semmens@ndsu.edu">Theresa.Semmens@ndsu.edu</a></td>
<td></td>
</tr>
</tbody>
</table>

L. Definitions
Credit Card Processing Machine: A machine or device used to process credit card transactions. *Examples may include: Omni3200SE, Verifone Vx570, Hypercom M4230, etc.*

Department: An NDSU entity which can be a division, college, department, group or organization that accepts credit cards in the course of its business.

Electronic Funds Transaction: 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).

Payment Card Industry (PCI) Standards: A multi-faceted 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 [https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

Payment Card Industry Self-Assessment Questionnaire: Departments accepting credit card transactions must complete a Payment Card Industry Standard Assessment questionnaire on an annual basis, or as requested. This survey assesses whether the department is in compliance with the required PCI standards. Customer Account Services will distribute the questionnaire annually to departments, and/or at the time the department is approved to accept credit cards. Departments utilizing Touchnet Marketplace will not need to complete the survey; compliance is certified by Customer Account Services.

Touchnet Marketplace uPay & uStore Site: 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. Marketplace is the North Dakota
University System application for processing online payments. Marketplace is intended for customer use only. Departments are not authorized to enter credit card information into their Marketplace sites on behalf of customers, thus turning their computer into a payment terminal.

**CAV2, CVC2, CID, or CVV2:** 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:** The personal identification number entered by cardholder during a card-present transaction

**M. History**
03/26/2008
Revised and Amended 5/28/13

**N. Authors**
Carrie Petersen, Customer Account Services
Theresa Semmens, Division of Information Technology