SECTION 509: Payment Card and Electronic Funds Transfer (EFT) Procedures

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

It is the University's responsibility to protect the privacy of its customers and ensure that all payment card transactions 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: Payment Card and Electronic Funds Transfer (EFT) Policy.

All individuals who participate in payment card processing on behalf of NDSU, or use NDSU equipment or facilities, hereafter referred to as a "merchant", must be compliant with the above.

Failure to be compliant in any areas may result in the revocation of authorization to accept payment card and/or EFT transactions and the merchant will be responsible for paying all related penalties.

Payment Card/EFT Usage

- North Dakota State University accepts Visa, MasterCard, Discover Card and American Express payment cards, or EFT payments for university business. Merchants may have the option to accept any or all of the aforementioned payment types. North Dakota State University permits payment card or EFT transactions ONLY via telephone, in person, or through an approved online portal. Departments must receive approval from the Vice President of Finance and Administration, or their designee in order to request payment card or EFT transactions through the mail.

Online Application

- The NDSU official online payment system is provided by TouchNet. All merchants wishing to accept online payment card transactions must use TouchNet's Marketplace product, unless an exception is granted to the merchant by the Vice President of Finance and Administration or their designee and the Vice President of Information Technology or their designee.

- To request a Marketplace website, the "Departmental Request for TouchNet Marketplace" must be completed and submitted to NDSU Customer Account Services.

- If a merchant has a specific business operational need that TouchNet's Marketplace product cannot meet, the merchant can apply for an exception. Merchants initiate the exception request by submitting the "Departmental Request for Other 3rd Party/Online Processor", along with written justification to the Vice President of Finance and Administration and the Vice President of Information Technology that explains their need and why Marketplace cannot adequately support the operation. Exception requests are evaluated on a case-by-case basis. As part of the exception process, Customer Account Services and the IT Security Office will conduct a full evaluation of proposed equipment, network structure and remote access privilege use.

    - In addition, merchants applying for an exception, must achieve and maintain full compliance with North Dakota State University Policy 509, legal, and industry regulations. Any merchant granted an exception is responsible for the fiscal costs associated with payment card security as detailed in the NDSU Policy 509, and this document.

Acceptable Technology

- Dial-up and cellular terminals for processing payment cards are available for purchase through the Bank of North Dakota. To request a dial-up or cellular terminal, the "Departmental Request for Dial-up Credit Card Machine" must be completed and submitted to NDSU Customer Account Services.

- If a department has a need to utilize a POS terminal that utilizes an Internet connection, they must complete a "Department Request for Other 3rd Party/Online Processor". The terminal must be approved by the Vice President for Finance & Administration, or their designee and the Vice President for Information Technology, or their designee. The terminal(s) payment card reader(s) must utilize Point to Point Encryption (P2PE) technology. The P2PE hardware must be on the PCI Security Standards Council list as a validated solution in order to be considered.

- Terminal usage for each processing environment is evaluated on a case-by-case basis. North Dakota State University merchants authorized to accept payment card transactions MUST supply Customer Account Services with an inventory of all equipment to be used in the processing environment prior to authorization and assignment of merchant account. The inventory shall include a description of the device, the model number, operating system or firmware information and a DNS/IP address, if applicable. Merchants must notify Customer Account Services within 7 days of any changes in processing equipment.

User Access to Processing Environments

- Merchants authorized to accept payment card transactions will have one or more payment card merchant accounts established by Customer Account Services with the Bank of North Dakota. All payment card transactions for the merchant will flow through this account. As a condition of merchant account assignment, all requirements detailed in the Payment Card and Electronic Funds Transfer (EFT) Policy must be met.

- For departments utilizing a POS terminal, access to the Cardholder Data Environment will be restricted by job duties of each individual. Every user must be assigned a unique User ID and password to access the Cardholder Data Environment. Passwords for users MUST be changed every 90 days. User accounts must also be locked after a maximum of 3 failed login attempts. Accounts inactive for at least 90 days must be removed or locked.

- NDSU employees are prohibited from using Remote Desktop Protocol (RDP) or any Terminal Services application to remote into their POS terminal from another computer to complete a payment card transaction. All terminal services must be disabled while the workstation is used within the payment card processing environment.

Payment Card Security

- The Division of Finance and Administration and the Division of Information Technology are responsible for campus compliance with payment card processing and security regulations. These Divisions are granted authority to take appropriate action to ensure conformity and compliance with University policies and procedures. Appropriate action up to and including suspension or termination of payment card processing activities will be imposed for an NDSU merchant that violates NDSU Policy 509.

- The purpose of this section is to establish procedures for the security of payment card transaction data, so that NDSU can seek to ensure that sensitive account and personally identifiable information (PII) that customers provide is protected against theft and/or improper usage. Additionally, the procedure seeks to ensure that the University complies with credit and banking industry security regulations related to credit card processing and reporting, including PCI DSS. This policy applies to all NDSU merchants, employees (including temporary and student workers), contractors and consultants. Affiliated merchants are encouraged to comply.

Reporting and Monitoring Responsibilities

- Customer Account Services and the Office of Information Security will perform regular internal assessment of systems, security procedures, policies and controls related to University payment card processing. Additionally, merchants will complete a compliance questionnaire annually. The compliance questionnaires report the status of campus compliance with NDSU Policies and Procedures and PCI DSS requirements. These questionnaires are made available to the Bank of North Dakota.

Sanctions

- Merchants that do not comply with requirements of NDSU Policy and Procedure 509, or other supplemental documents related to those policies and procedures must take necessary action to become compliant or be subject to sanctions up to and including immediate suspension or termination of payment card processing privileges.

- Customer Account Services, and/or the Office of Information Security, will notify merchants when remedial action is necessary to achieve compliance with campus and industry requirements. If compliance is not achieved in a time deemed reasonable by the Division of Finance and Administration and the Division of Information Technology, payment processing privileges will be suspended and the merchant will no longer be an authorized payment card merchant. Within the institution, merchants engaged in payment card processing are responsible for any financial loss incurred by the University resulting from inadequate controls or insufficient adherence to the PCI DSS and other industry security requirements. Any appeal of actions taken by the Division of Finance and Administration and the Division of Information Technology regarding suspensions or cost recovery will be considered by the Vice President for Finance and Administration.

Merchant Responsibilities

- All merchants engaged in any form of payment card/EFT processing must comply with the General Procedures listed below. Additional procedures may be required for merchants that have been granted an exception to use an alternate processing system, outside of the Bank of North Dakota.

General Procedures

- Each merchant engaged in payment card processing shall maintain formal, written operational procedures that demonstrate compliance with NDSU Policy 509 and the PCI DSS. Operational procedures must include transaction processing methods, refund policies, and reconciling procedures. Customer Account Services will review the documentation and upon approval, a copy of the approval will be placed in the merchant's file. Merchants must evaluate procedures annually and update with Customer Account Services as necessary.

- Physical and electronic storage of sensitive PII associated with payment card transactions is prohibited. The definition of PII may be revised for payment card policies as legal and industry regulations change. Examples of PII for which retention is prohibited are: Primary Account Number (PAN), security code (CVV) or contents of magnetic track data from a payment card.

- Each merchant engaged in payment card processing shall ensure that all employees who have access to customer PII associated with payment card transactions annually complete the NDSU Credit Card Training, or the PCI Training for Managers. Additional training may be required, depending on the processing method used by the merchant. Only persons who have completed all required training will be permitted to handle payment card data on behalf of North Dakota State University.

- Each merchant engaged in payment card processing must be in compliance with University policies regarding employee background checks, in accordance with NDUS Procedure 602.3.

- Each merchant engaged in payment card processing must establish segregation of duties among payment card processing, the processing of refunds, and reconciliation of revenue to the extent possible. Each such merchant shall immediately notify Customer Account Services of any staff changes related to payment card data-handling positions.

- Acceptable methods of payment card acceptance include: walk-in (face-to-face), telephone, or customer-initiated online payment (via Marketplace or other approved online payment system). Phone payments should be processed while the customer is on the line. Making note of a customer's payment card number to process at a later time is strongly discouraged. If it is necessary to write down a customer's information, it must be stored in a secure location until processed. Upon processing, the information must be destroyed via cross-cut shredder. Accepting payment card data via email, fax or any end-user messaging technology is prohibited. Tuition/Fee payments are accepted only as customer-initiated through the TouchNet module linked to Campus Connection. Soliciting payment information through the mail is generally prohibited, an exception may be granted by submitting written justification to Customer Account Services.

- All refund transactions must have sufficient documentation, and should be performed by a separate individual that does not normally process transactions OR perform reconciliations. Excessive refund activity may be investigated by Customer Account Services and may result in a mandatory change in business operations.

- Customer PII associated with payment card transactions, especially account numbers, shall not be transmitted via any insecure method, especially e-mail, fax, cell phone, vocally in a public location, or any end-user messaging technology.

- All devices within a merchant's cardholder data environment should be secured to the extent possible. Machines that are left unattended must be locked or logged-off. Non-computer devices should never be left unattended in an area where customers or visitors may have access to the device. Customer Account Services will provide additional guidance to merchants based on their specific needs.

- In accordance with PCI DSS requirements, devices within a merchant's cardholder data environment should be periodically inspected for evidence of tampering. Employees at each merchant should be trained by their supervisors to spot possible signs of tampering.

- All workstations used in processing must run any Anti-Malware programs required by Information Security and have the computer name registered with Customer Account Services and Information Security. In addition, each workstation will be subject to quarterly PCI DSS compliance scans. All workstations used in processing must be turned on during scanning. Quarterly scans are scheduled by the merchant PCI contact.

- Each merchant engaged in payment card processing must complete all security enhancements to processing systems as required by Customer Account Services and Information Security. All vendor supplied security patches to systems must be applied within one month of issue date.

- All merchants engaged in payment card processing must cooperate with all reporting and audits required by Customer Account Services, including full compliance with PCI DSS and all other industry security requirements, or be subject to the Sanctions detailed above.

- All merchants must complete an annual Self-Assessment Questionnaire (SAQ) in accordance with the PCI DSS and Bank of North Dakota requirements.

- All merchants who engage with any type of 3rd party service provider, must request annual certification from that vendor, of PCI DSS (or PA DSS) compliance.

- Any changes to the processing environment, including any software/hardware additions MUST be approved by the Vice President for Finance and Administration, or their designee and the Vice President for Information Technology, or their designee prior to purchase. If this provision is violated, the merchant will be subject to the Sanctions detailed above.

Additional procedures for Merchants Granted Exception

- Merchants that have been granted an exception to process outside of the University banking and accounting environment, MUST abide by all regulations set forth in the 509 policy series, and additional requirements not detailed above.

- Approval (on an annual basis) by the Vice President for Finance and Administration and the Vice President for Information Technology; as well as the Bank of North Dakota, is required for all third party processing agreements/contracts.

- All contracts and contract renewals for payment card processing MUST be approved by the Vice President for Finance and Administration and the Vice President for Information Technology prior to execution. All contracts MUST contain PCI DSS contract language determined by the Vice President for Finance and Administration, or their designee and the Vice President for Information Technology, or their designee.

Vendors

- NDSU is not required to provide internet services to vendors doing business on campus to access credit card payment processors; it is the vendor's responsibility to specifically request such services through the Vice President for Finance and Administration, and the Vice President for Information Technology Services, or their designee. Vendors on campus can use the Vendor Request to Process Credit Card and Electronic Fund Transactions Utilizing (Outside) Third Party Online Processor form.

Reconciliation Procedures

Payment Card Fees

- Each merchant is responsible for any hardware, software, setup and/or maintenance costs to maintain the processing environment, including the cost of security scans. Merchants may also be required to pay for background checks as required by NDSU Policies and Procedures.

- The University is charged fees on all payment 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 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 merchant's fund via journal entry/import on a monthly basis by Customer Account Services or the Accounting Office.

- As merchants are developing rates (fees for goods or services) they should recognize the payment card merchant fee as a cost of doing business. Should the merchant choose to recover the fee, they must build it into the overall rate structure. They may generally not impose any surcharge on over the counter payment card transactions. It may be permissible, however, to offer a discount for cash transactions, provided that the offer is clearly disclosed to customers and the cash price is presented as a discount from the standard price charged for all other forms of payment. Surcharging is generally prohibited by ND State Law, however, exceptions can be granted by appealing to Bank of North Dakota. Contact Customer Account Services to file this appeal. Adding a surcharge to payment card transactions can result in loss of business from disappointed customers. Always consider all angles when preparing to surcharge.

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 merchant by Customer Account Services. The merchant 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 merchant being charged for the transaction in question and the merchant cannot appeal the chargeback.

Recording and Reconciling Credit Card Transactions

- Merchants utilizing TouchNet Marketplace are required to submit the "Monthly Marketplace Sales Report" within the first 5 business days of the next month. Electronic check (ACH, EFT) sales should be reported separately from payment card sales in order to facilitate proper charging of credit card fees.

- Merchants using credit card machines, POS terminals, or online provider other than TouchNet Marketplace must 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 3rd business day of the next month. If the end of the month falls mid-week, that week should be split for reporting purposes.

- When submitting weekly reports to Customer Account Services, the credit card report form should be submitted with the Daily Totals or Daily Settlement 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 Customer Account Services, and one copy is to be retained by the merchant). Merchants should transmit and settle their batches daily.