Prior to accepting credit/debit card transactions, UND departments must submit all requests to accept credit card transactions to the UND Treasury department and PCI Committee. PCI Committee approval must be obtained in advance of signing an agreement with a vendor for a product or software system with the functionality to store, process, and/or transmit cardholder data or are involved in the security of the cardholder data. The PCI Committee reviews for validated service providers, validated payment applications, network requirements, and determines if Bank of North Dakota (BND) approval is required due to the NDCC requiring all credit card processing be through BND.

When departments are completing the Contract Request form through Procurement Services, there is a question that asks whether the vendor/system accepts credit/debit cards. If the vendor/system has the functionality to store, process, and/or transmit cardholder data or are involved in the security of the cardholder data, this question should be answered as “YES”. If yes, Procurement forwards the information to UND Treasury/PCI Committee. As requests are submitted to the PCI Committee, the PCI Committee reviews and approves or denies the request. If additional information is requested by the PCI Committee, UND Treasury communicates to the department and assists the department in collecting the additional information.

Methods of acceptance includes:
- Credit card terminal, including analog or IP terminals, P2PE terminals and mobile terminals
- On-line payment site via Marketplace uStores or uPay
- Third Party system that accepts credit/debit card transactions

If the request is approved, UND Treasury works with the department:
- to obtain Bank of North Dakota approvals (if necessary)
- to purchase necessary equipment from Bank of North Dakota
- to perform testing with the new system to ensure transactions are posting correctly to the general ledger
- to provide credit card training to all departmental employees working with cardholder data
- to complete an SAQ prior to the department accepting credit/debit card transactions or shortly after implementation, and annually for compliance requirements.

In the near future, an electronic request process will be implemented. This new process will streamline the submission and approval process.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. A cardholder data environment (CDE) is a computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component/equipment that directly connects to or supports this network.

Although the PCI DSS requirements are developed and maintained by an industry standards body called the PCI Security Standards Council (SSC), the standards are enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data or are involved with the security of the cardholder information. It covers technical and operational system components/equipment included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

Cardholder data is defined as any sensitive data associated with the credit card account. This includes the primary account number, cardholder names, expiration date, and service code. The service code is a three-digit or four-digit value in the magnetic-stripe that follows the expiry date of the payment card on the track data.

The main purpose of the PCI DSS is to reduce the risk of debit and credit card data loss, such as a data breach or fraudulent transactions. In the credit card industry, data breaches occur when hackers obtain credit card information that could be used to commit fraud or identity theft. PCI DSS suggests how a data breach could be prevented, detected, and how to react if potential data breaches occur. It provides protection for both merchants and cardholders. It’s important that the University’s website or Point of Sale device is secure, which includes the hardware, software, and the established business procedures for processing credit/debit card transactions.
The PCI DSS is a set of twelve security standards/requirements designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, including network and firewall configuration to protect cardholder data.

Merchants ignoring the adoption of PCI DSS do so at their own risk:

1. Non-PCI compliant merchants and payment processors can face fines from $5,000 to $500,000, depending on a variety of factors.
2. Credit card companies may also revoke the right of a merchant to process credit card transactions.
3. Reputational damage, lost business and reduced consumer confidence and trust are just some of the after-effects of a data breach.

The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the PCI DSS. There are various types of SAQ's available, based on the method in which the transactions are processed. The various SAQ's are located at: https://www.pcisecuritystandards.org/document_library

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C-VT
- SAQ C
- SAQ P2PE
- SAQ D

Annually, or at any time the cardholder processing environment changes, the Bank of North Dakota (UND’s acquirer) requires UND to complete PCI DSS compliance reporting by submitting a Self-Assessment Questionnaire (SAQ) for each merchant account. SAQ's are required for all credit card processing methods (terminal, online payment sites, or third party systems). UND Treasury will complete the SAQ and AOC through an online portal for each department/merchant account. UND Treasury will then forward a copy of the SAQ and Attestation of Compliance (AOC) to each department head that accepts credit/debit cards. The department head is required to review the documents and confirm the accuracy of the reports by signing each document and returning them to UND Treasury.

If a merchant fails to validate that they are in compliance with PCI DSS security requirements for their business type, they are considered to be non-compliant. In addition, by adopting the PCI DSS operating guidelines, entities can mitigate many of the risks of a breach and potential costs and fines associated with a data breach.