UNIVERSITY OF NORTH DAKOTA
TREASURY DEPARTMENT

SUMMARY OF PCI DSS COMPLIANCE
02.01.2021

If you are a merchant (UND department) who accepts or processes payment cards, you must comply with the Payment Card Industry Data Security Standards (PCI DSS). These guidelines assist entities to mitigate many of the risks of a breach and potential costs and fines associated with a data breach or fraudulent transactions. If a merchant fails to validate that they are in compliance with PCI DSS requirements for their business type, they are considered to be non-compliant.

The PCI DSS is a set of requirements intended to ensure that all companies that process, store, transmit, or are involved in the security of credit card information, maintain a cardholder data 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 is a set of twelve security standards/requirements designed to ensure all merchants maintain a secure environment, including network and firewall configuration, to protect cardholder data, and applies to all entities that:

- store cardholder data
- process cardholder data
- transmit cardholder data
- involved with the security of the cardholder information

Additional information for the twelve security standards requirements can be reviewed at:
https://www.pcisecuritystandards.org/document_library (PCI DSS Quick Reference Guide).

PCI DSS compliance includes:

- technical and operational system components
- equipment included in or connected to cardholder data

Cardholder data is defined as any sensitive data associated with the credit card account. This includes:

- Primary account number
- Cardholder names,
- Expiration date
- Service code (three-digit or four-digit value)

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 compliance provides protection for both merchants and cardholders.

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

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

Summary of SAQ Reporting

The PCI DSS 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.

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 an SAQ for each merchant account. SAQ's are required for all credit card processing methods (terminal, online payment sites, or third party systems).

Annually, the PCI Committee will complete the SAQ and an Attestation of Compliance (AOC) through an online portal for each department/merchant account. UND Treasury will then forward a copy of the SAQ and AOC to each department head. 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.