NDSU Incident Response Plan for Suspected or Confirmed Credit Card Security Breach

In the event of a suspected credit card security breach, the affected department must follow the following procedures:

1. Department representative must notify the following individuals:

a. Department head/chair.

b. Customer Account Services - who will alert:

i. Bank of North Dakota - Bank of North Dakota will notify Trustwave (our compliance vendor) and Chase Paymentech (our processor). Chase Paymentech will notify the card brands.

ii. Vice President of Finance and Administration.

iii. Campus Police.

iv. Other campus departments (if the breach affects or could affect multiple areas of credit card processing).

c. Information Security Office.

i. Information Security Office will follow their protocols for data security breaches.

2. The Department may continue business operations, excluding credit card acceptance, until notified by Customer Account Services that they may resume credit card processing activities.

a. In the event the breach occurs at a department with multiple credit card processing methods (ecommerce, registers, etc.), the credit card processing activity for each method must be suspended until the notification is received from Customer Account Services that a method may be resumed.

b. If the breach is not isolated to a single department's processing environment, all credit card processing activity across campus is subject to suspension until Customer Account Services notifies each department that it is acceptable to resume operations.