Standards for Mobile Online Payment Transaction Processing
REF: NDSU Policy 509, Electronic Financial Transaction Policy
Final Version April 5, 2012

Using Mobile Online Payment Applications for
NDSU Financial Transactions (Credit and Debit Cards)

Definitions:

Mobile Online Payment (MOP) Systems – Those applications which can be downloaded and activated on an electronic mobile device such as a data phone, iPad, tablet, and/or laptop, and used to electronically process credit card transactions.

Device Specifications and Procedures:

1. The device and associated hardware such as the dongle and or card swipe device must be assigned to a specific, full-time, benefitted employee. This person will be responsible to ensure that all requirements, standards, and guidelines are met or exceeded for this device.
2. A list of wireless/data phone devices, along with who has authorized use must be maintained by the department.
3. All wireless/data phone devices that are used for online payment processing must be labeled with the owner and contact information.
4. The mobile device must be an NDSU-owned mobile device with a data plan used solely for the purpose of processing payments. Only the payment application and the operating system software are allowed on the device.
5. The phone number associated with the account must be "private" or unlisted. This is to prevent unwanted text messages or phone calls.
6. Currently, mobile devices are limited to specific data phones. Tablet devices such as the iPad and Android systems are not acceptable, because they are not approved by the Bank of North Dakota.
7. Only data phones that have a strict vetting process for approving and requesting downloadable applications will be acceptable for online payment use.
8. The device used must have the ability to be remotely wiped or "killed", in the event the phone is lost or stolen.
9. The device must be password-protected.
10. The device must have encryption capabilities.
11. The device must only use the secure Internet data connection through the NDSU cell phone data plan. Open (non-secure) wireless Internet connection is not permitted.
12. Bluetooth capabilities must be turned off or disabled.
13. Automatic search and connect to external wireless networks must be turned off or disabled.
14. The data phone used for mobile electronic credit card processing must only be used by those who have a need to use and are authorized by the owning department/college and have data confidentiality and PCI training
15. When the phone, dongle or card swipe device, and signature pad (if one is used) is not being used for online financial transactions, the phone must be powered off, and stored in a locked drawer, file cabinet or vault that only those who have a need have access to.

16. Applications or software not related to the operating system or to the online processing application must be approved by the Chief IT Security Officer.
17. The data phone's operating system and other approved software must be patched and updated in a timely manner to reduce vulnerabilities and enhance productivity.
18. If it is suspected that a data phone may be compromised or infected with malware, immediately stop using the phone for online payment processing; notify the supervisor, and contact the Chief IT Security Officer. Be sure to document the reason for suspecting the phone to be compromised or infected.

MOP Application procedures:

1. The MOP application used must be NDSU and Bank of North Dakota approved for processing electronic payments securely. Please contact Customer Account Services for list of approved mobile payment applications.
2. A card reader must be used and be approved by NDSU Customer Account Services and the Bank of North Dakota.
3. The application must require authentication and authorization (e.g., login and password). The application must have the capability to purge transaction data after the required 90 day period when a charge can be disputed by the customer.
4. If an email address is required for using the application, the email address used on the phone must be specific for payment-processing only. There will be one "owner" of this email account. The owner must be a full-time, benefitted NDSU employee. This email address and accompanying account must be requested through the Information Technology Division and approved by the NDSU Chief IT Security Officer.

Lost or Stolen Device Procedure:

1. Immediately activate the device to wipe or "Kill."
2. Notify the following:
    a. The manager or department chair
    b. The cell phone carrier and request the phone and associated services be cancelled and explain why.
    c. Payment vendor
    d. Customer Account Services
    e. Campus police
3. The manager/department chair must notify:
    a. VP or Dean of division/ college
    b. Chief IT Security Officer
    c. NDSU Telecomm