Duke University Mobile Payment Acceptance Policy

Review Frequency: Annually
Updated: August 2022

Authority: Electronic Commerce Office

1. Purpose

The expanding capabilities of consumer electronic handheld devices (e.g., smartphones, tablets, PDAs, or collectively, "mobile devices") now includes payment card (credit and debit card) transaction capabilities. Mobile payment technologies introduce new risks to the security of cardholder data because they have limited security safeguards for payment.

The uniqueness and variety of mobile devices introduce challenges in securing that environment. General-purpose mobile devices do not provide the same level of security as expected with a traditional retail store system. Almost any mobile application could access account data stored in or passing through the mobile device. This poses a challenge for merchants to demonstrate adherence to the PCI Data Security Standard.

The Duke E-Commerce Office continually evaluates best practices and standards for Duke Merchants in regards to credit card processing in a mobile environment. Duke has developed the following policies for the use of mobile payment technologies.

2. Policy

Authorized Mobile Payment Technologies:

- Duke merchants must gain approval from the Duke E-Commerce Office to process credit cards at off-site, remote or "mobile" locations.
- The Duke E-Commerce Office has authorized the use of purpose-built, hand-held cellular (bank) terminals or P2PE devices for those merchants approved for mobile credit card processing. These dedicated terminals must be ordered through the Duke E-Commerce Office.
- Authorized cellular terminals may not be used to process transactions for more than one Duke merchant account.
- Authorized cellular terminals must be stored in a secure locked location when not in use.

Unauthorized Mobile Payment Technologies:

- Duke merchants must not transmit or process credit card data using ***any*** Wi-Fi network (IEEE 802.11).
- Duke merchants must not use mobile devices such as smart phones or tablets (e.g., iPhone, iPad, Android) for receiving, transmitting, processing, or storing credit card data.
- Duke employees are prohibited from using any personal mobile device for payment acceptance on Duke's behalf.
- Mobile device plug-in credit card readers such as Square, PayPal, etc. are prohibited.

3. Scope

This policy applies to all Duke employees, students or contractors that process credit card payments on behalf of Duke.

Supporting References:

- Duke University E-Commerce: https://finance.duke.edu/banking/ecommerce/reginfo.php
- PCI Security Standards Council: https://www.pcisecuritystandards.org/