

# Mobile Payment Solutions and the EMV/PCI Impact

Steve Woods  
Director of Student Accounts  
Cal Lutheran University

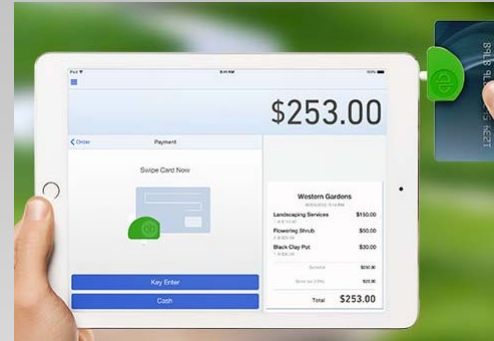
Matt Camino  
Director of eCommerce  
University of the Pacific




- So you're ready to take your payment acceptance mobile? What do you need to know:
  - Software Platforms
  - Hardware
  - EMV
  - PCI

## **Accepting Mobile Payments**

- A few of the many options



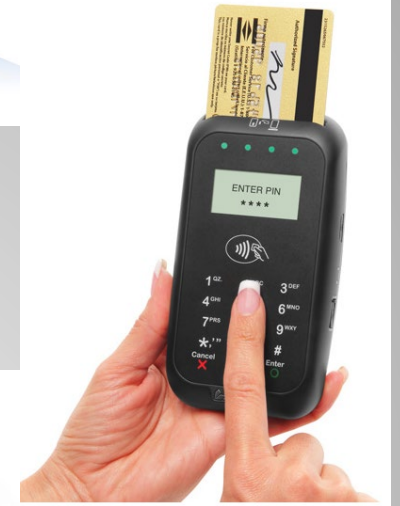
## Software Platforms & Hardware

- 
- So you're ready to take your payment acceptance mobile? What do you need to know:

- ~~Software Platforms~~
- ~~Hardware~~
- EMV ←
- PCI

# Accepting Mobile Payments

- October 1<sup>st</sup>, 2015
- Chip + Pin or Chip + Sig
- New hardware required



**EMV (Europay, Mastercard, Visa)**

# Dual Interface Chip Cards

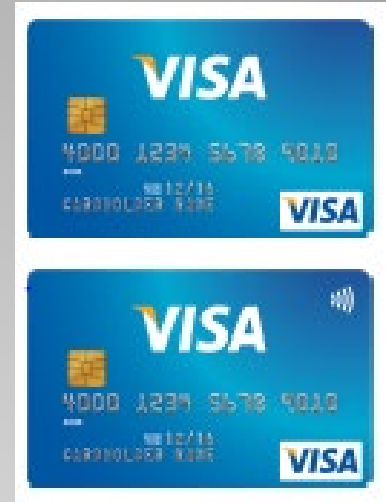
- Contact Cards

Traditional magnetic swipe cards and new chip encrypted cards


- Contactless Cards

Communicate via radio frequency (RF), also referred to as NFC (Near Field Communication), i.e., Apple Pay

- Dual interface chip cards combine both technologies and can communicate either way. You can purchase hardware that will process all three types of payments



**EMV (Europay, Mastercard, Visa)**

- 
- So you're ready to take your payment acceptance mobile? What do you need to know:

- ~~Software Platforms~~
- ~~Hardware~~
- ~~EMV~~
- PCI ←

# Accepting Mobile Payments

## PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network and Systems</b>	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
<b>Protect Cardholder Data</b>	<ol style="list-style-type: none"><li>3. Protect stored cardholder data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"><li>5. Protect all systems against malware and regularly update anti-virus software or programs</li><li>6. Develop and maintain secure systems and applications</li></ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"><li>7. Restrict access to cardholder data by business need to know</li><li>8. Identify and authenticate access to system components</li><li>9. Restrict physical access to cardholder data</li></ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
<b>Maintain an Information Security Policy</b>	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security for all personnel</li></ol>

Source: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf)

# PCI DSS



**Mobile Payment Acceptance Application Category 1** – Payment application operates only on a PTS-approved mobile device.

**Mobile Payment Acceptance Application Category 2** – Payment application meets all of the following criteria:

- i. Payment application is only provided as a complete solution “bundled” with a specific mobile device by the vendor;
- ii. Underlying mobile device is purpose-built (by design or by constraint) with a single function of performing payment acceptance; and
- iii. Payment application, when installed on the “bundled” mobile device (as assessed by the Payment Application Qualified Security Assessor (PA-QSA) and explicitly documented in the payment application’s Report on Validation (ROV), provides an environment which allows the merchant to meet and maintain PCI DSS compliance.

**Note:** “Bundled” solutions are defined as the approved payment application being provided to the customer together with specific version(s) of both the mobile device and the device’s operating system/firmware.

**Mobile Payment Acceptance Application Category 3** – Payment application operates on any consumer electronic handheld device (e.g., smart phone, tablet, or PDA) that is not solely dedicated to payment acceptance for transaction processing.

Source: [https://www.pcisecuritystandards.org/documents/pa-dss\\_mobile\\_apps-faqs.pdf](https://www.pcisecuritystandards.org/documents/pa-dss_mobile_apps-faqs.pdf)

# PCI Mobile Categories

- Category 1:



- Category 2:



- Category 3:



# PCI Mobile Category Hardware

- CASHNet Mobile Payments
- Category 2 & 3 for PCI purpose
- Existing CASHNet eMarket users
- Started with 4 iPad's (2 AT&T, 2 Verizon)
- Stored in locked Ergotron wall mount
- IDTECH Shuttle reader
- Check out form



**Mobile at Pacific**

- Over 50 online stores with many now adding mobile versions
- De-centralized management, 60+ users
- PCI DSS Requirement 9.9 will become much more difficult

**LAWN BOX SITE MAP**

Each box is an 8' x 8' space marked on the lawn.  
Each space has room for only 4-6 adults.

To reserve an available lawn box click on the 'next step' button or call 805-493-3014.  
Be sure to bring your own blanket and/or a low-back low-profile lawn or beach chair.  
Chairs that are normal chair height will not be permitted in the lawn boxes.

● -\$110  
● -\$90  
● -\$75  
 (Each Box)

	Aisle	1	2	3	4	5	6	Aisle			
Aisle		25	7	8	9	10	11	12	30	Aisle	
		26	13	14	15	16	17	18	31	32	
		28	29	19	20	21	22	23	24	33	34

\*Designated area for regular sized chairs for patrons with special needs

K. S. t

HOME » [MEASURE FOR MEASURE - JUNE 26TH](#)

Box 6 - June 26th	\$110.00
Box 7 - June 26th	\$90.00
Box 8 - June 26th	\$90.00

iPad 9:45 AM 41%

Favorites KSCM - KSC - Mobile Pay

★ Box Seat \$0.00

Enter Amount Done

Enter Amount \$0.00

Required fields appear in bold type

Box Number

Box Number *Enter Here*

Add

Subtotal \$0.00

# Mobile at Cal Lutheran

- EMV Readiness Guide:

<http://usa.visa.com/download/merchants/visa-merchant-chip-acceptance-readiness-guide.pdf>

- PTS Approved Devices (Category 1 Mobile):

[https://www.pcisecuritystandards.org/approved\\_companies\\_providers/approved\\_pin\\_transaction\\_security.php](https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php)

**More Resources**