Payment Security Today

Bart Lawyer, Duke University
John Diaz, Blackboard Transact
About Duke University

• Located in Durham, NC
• 14,500 students
  – 6,500 Undergraduates
  – 8,000 Graduate/Professional
• 35,000 employees
• Duke University Health System
  – North and South Hospitals
  – Duke Raleigh
  – Durham Regional
• Campuses:
  – Durham (East, West, Central)
  – Beaufort (Marine Lab)
Auxiliary Departments Accepting Payments

- Dining Services
- Retail Stores
- Office Products & Printing
- Parking & Transportation
- Athletics
- Postal Services
- Event Management
- Box Office
Credit Card Processing Analysis

<table>
<thead>
<tr>
<th>Summary of Credit Card Transactions</th>
<th>Year End 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># of Transactions</td>
</tr>
<tr>
<td>Auxiliaries</td>
<td>2,303,232</td>
</tr>
<tr>
<td>EDU</td>
<td>401,814</td>
</tr>
<tr>
<td>Health Systems</td>
<td>1,389,904</td>
</tr>
<tr>
<td>Totals</td>
<td>4,094,950</td>
</tr>
</tbody>
</table>

** Does not include Campus Card (DukeCard)

Reference:
Treasury & Cash Management, E-Commerce Office, Duke University
Duke E-Commerce and PCI-DSS Compliance Policies

• Merchants must adhere to PCI-DSS standards + Duke supporting policies
• No storage of credit cards at any time
• Service Providers must be PCI-DSS level 1 validated
• We do not accept Vendor self assessments – require AOC signed by QSA – if processing brings Duke Network into scope
• Duke owns the Merchant account, not the vendor
• We do not allow for WiFi Credit Card processing (Cellular is OK if bank provided)
Keeping up with Compliance

• Annual MANDATORY merchant training for all owners
• Established an internal PCI Board with senior leadership
• Contracted with an external QSA consultant
  – Evaluation of merchant environment, reduction of scope where possible, approval, design and planning of protected network
• Implemented Merchant specific networks using Cisco’s VRF and MPLS technologies and stood up a dedicated Active Directory for PCI merchants/users
• Currently asking all vendors to provide P2PE/E2EE solutions
Uses of Credit Card technology: (The bigger uses)

• POS with P2PE/E2EE payment terminals
• POS with no payment terminals (aka tabletop ordering)
• Hosted Order Pages for E-Commerce
• Parking Pay on Foot Stations
• Parking Pay at Lane
• Ingenico Cellular Terminals
• Dial-up Terminals
• Virtual Terminals

CyberSource®
the power of payment
Payment security at the POS devices

• Register swipes are deactivated and the only option is to swipe the credit card on the MX 915
• Card data is encrypted at the swipe using Verifone VSP
• Tokenization
• Self-swiping ensures that credit/debit card does not leave the customer’s hand/possession
• Positive feedback from:
  – Campus IT
  – Treasury & Cash Management
  – Merchants
  – Our Customers
Challenges as we look ahead to EMV

- How to support open check
- Collection of tips
- Mobile / wireless security
- Speed of Service
- P2PE/E2EE device failures/repair

“The PCI Council has specified that P2PE solutions must use a PCI-approved point-of-interaction device (POI), which has been evaluated and approved via the PCI PTS program. This means that the implementation guidelines for hardware are now more stringent.” - Verifone
Future Plans

• EMV Kickoff in 2017
  – Campus Stores & Dining Services
  – Verifone Point deployed in Dining and in progress for College Stores
  – Deploy EMV at other non-Blackboard merchants
• CampusCard HOP/HPP for online payments
• Adherence to new PCI DSS rules including v3.2
EMV Merchant Adoption Remains Sluggish a Year Later

1. Of card-accepting merchants have EMV terminals: 44%
2. Of card-accepting merchants can accept chip-based trans.: 29%

Top EMV Hurdles (% of Respondents)
- Processor Readiness: 47%
- Replacement POS Terminal Readiness: 47%
- Gateway Readiness: 45%

Expected EMV Acceptance:
- Current: 29%
- Oct. ’16: 32%
- Dec. ’16: 51%
- Mar. ’17: 62%
- Later Than Mar. ’17: 90+%
Updated US EMV Statistics

Six years to chip card saturation

- Percentage of cards expected to be chip-compliant
- Percentage of volume expected to be chip transactions
- Forecasted dollar volume of chip transactions (billions)

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage Cards</th>
<th>Percentage Volume</th>
<th>Forecasted Dollar Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>15%</td>
<td>48%</td>
<td>$259</td>
</tr>
<tr>
<td>2016</td>
<td>58%</td>
<td>48%</td>
<td>$890</td>
</tr>
<tr>
<td>2017</td>
<td>84%</td>
<td>73%</td>
<td>$1,465</td>
</tr>
<tr>
<td>2018</td>
<td>95%</td>
<td>85%</td>
<td>$1,825</td>
</tr>
<tr>
<td>2019</td>
<td>98%</td>
<td>91%</td>
<td>$2,087</td>
</tr>
<tr>
<td>2020</td>
<td>99%</td>
<td>95%</td>
<td>$2,354</td>
</tr>
<tr>
<td>2021</td>
<td>100%</td>
<td>100%</td>
<td>$2,623</td>
</tr>
</tbody>
</table>

Source: Mercator Advisory Group
CreditCards.com
EMV Timeline

Figure 1: Road Map for Introducing EMV into the U.S.: POS Terminals

- 10/2012: PCI Relief for Early Conversion
- 4/2013: Merchant Acquirer Requirement
- 10/2015: Merchant Fraud Liability Shift
- 10/2017: Fraud Liability Shift for Gasoline Retailers

Source: Mercator Advisory Group
Why did we do EMV?

• EMV was created in an effort to reduce fraud worldwide by 90%
• The Liability Shift makes whoever is not conforming to EMV standards liable for fraud
  • If all parties are conforming then whomever is supporting the least secure certification
  • The liability shift only affects counterfeit card and lost / stolen card fraud (in theory)
  • Can vary by card brand
Updated US EMV Statistics

Percentage of Card-Present Transactions that are EMV

- **Africa & The Middle East**
  - July 2014 - June 2015: 83.77%
  - July 2015 - June 2016: 89.94%
- **Asia**
  - July 2014 - June 2015: 33.55%
  - July 2015 - June 2016: 57.93%
- **Canada, Latin America, & The Caribbean**
  - July 2014 - June 2015: 86.95%
  - July 2015 - June 2016: 88.81%
- **Europe Zone 1**
  - July 2014 - June 2015: 96.94%
  - July 2015 - June 2016: 97.60%
- **Europe Zone 2**
  - July 2014 - June 2015: 65.41%
  - July 2015 - June 2016: 74.98%
- **The United States**
  - July 2014 - June 2015: 0.26%
  - July 2015 - June 2016: 7.20%

Figures represent the percentage of all card-present transactions processed by each member institution that are EMV transactions (Contact or Contactless). The reported data (blue bar) is from the twelve months of July 2014 through June 2015 and (green bar) the twelve months of July 2015 through June 2016; the data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa during this period. To qualify as an “EMV transaction” for the purpose of this methodology, both the card and terminal used during a transaction must be EMV-enabled. Data is reported from the acquirer perspective. These figures do not include offline transactions, “on us” transactions (defined as a transaction handled exclusively by another processor), and/or transactions processed by non-EMVCo-member institutions, such as local schemes.
Fraud Mutation Predictions

Pre-EMV
- Counterfeit: 45%
- Lost or stolen: 37%
- Card-not-present: 14%
- Other: 4%

2016
- Counterfeit: 67%
- Lost or stolen: 14%
- Card-not-present: 9%
- Other: 10%

Source: American Banker/Fiserv
CreditCards.com
EMV card fraud liability: Who's responsible?

This graphic is in relation to shifts for chip only and does not reflect any other changes to how disputes work today.

Graphic courtesy of Heartland Payment Systems.
EMV card fraud liability: Who's responsible?

<table>
<thead>
<tr>
<th>Fraud scenario:</th>
<th>Merchant/Acquirer</th>
<th>Card issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip card is stolen and swiped by fraudster in store not EMV-ready.</td>
<td>X (If the card is PIN-based and from American Express, Discover or Mastercard)</td>
<td>X (If the card is a Visa, Accel, China UnionPay, NYCE or STAR Network card)</td>
</tr>
<tr>
<td>Stolen card number is used online.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Chip card swiped at non-EMV compliant merchant, mag stripe data stolen and fraud occurs.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Chip card-less consumer gets hit by fraud because they couldn't dip a chip card at an EMV-ready retailer.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stolen/lost chip card dipped by fraudster at EMV-ready merchant.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mag stripe data copied from chip card onto counterfeit card and swiped by fraudster at non-EMV compliant merchant.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mag stripe data copied from chip card onto counterfeit card and swiped by fraudster at EMV compliant merchant.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Chip card dipped at EMV-compliant merchant.</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Source: CreditCards.com
Chip & Pin vs. Chip & Signature

“It's like locking the front door and leaving the back door open. It would be a shame to spend all that money for a half-baked solution.”

Mallory Duncan, Senior VP and General Counsel NRF

Chip and PIN
- Used in UK, France and Canada
- Inherently more secure

Chip & Signature
- Used in Mexico and Germany and now the United States
- Easier to integrate into existing environment
- More familiar to current customers
EMV Challenges

• Requires both EMV capable hardware and software
• New merchant accounts required for many processors
• If an EMV card is swiped at an EMV capable reader it will force the customer to ‘dip’ instead
• Card must stay with the reader until the transaction completes
• Customer learning curve
Quick-Chip to the Rescue?

How Quick Chip for EMV Works at the Point of Sale

1. Insert the card as prompted.
2. Remove card when prompted. Processing should take no more than 2 seconds.
3. Complete transaction. Follow prompts on screen to finalize transaction.

Remove Card Before Authorization Response
Generate the EMV cryptogram based on the final transaction amount, but allow the card to be removed before the authorization response.

Generate Cryptogram Without Final Sale Amount
Create the EMV cryptogram before the final transaction amount is known and prompt the cardholder to remove the card. The final amount will be included in the non-EMV transaction data.
EMV Alone is not Sufficient

Troy Leach, Chief Technology Officer of the PCI Security Standards Council, testifying before Congress:

"While EMV encrypts elements of EMV data to protect the authentication of the transaction, a very important point is that it does not encrypt the account data - not for transmission to the processor or for storage within a merchant's network. This means the PAN [primary account number] is in clear text."

Feb. 5, 2014
What do these retailers have in common?
Holistic Payment Security

You need all three:

• Tokenization
• EMV
  – But really need PIN or other multi-factor authentication
• Point-to-Point Encryption

But don’t forget PCI including physical and network security and proper card handling procedures!
Tokenization

Format preserving tokens: maintain the look and feel of original 16-digit payment card data. For example:

• Payment Card Number: 4111 1111 1111 1111
• Format Preserving Token: 4111 8765 2345 1111

Non-format preserving tokens: do not resemble the original data and could include both alpha and numeric characters. For example:

• Payment Card Number: 4111 1111 1111 1111
• Non-format Preserving Token: 25c92e17-80f6-415f-9d65-7395a32u0223
Point-to-Point Encryption

- Reduces Card Data Environment and thereby PCI DSS exposure
- Secures sensitive cardholder data at the card swipe and protects it throughout the transaction
- Card data decrypted either at Payment Gateway or Processor
  - Merchant and POS provider do not have keys to decrypt card data
- Strict requirements for Validated PCI P2PE solutions
Point-to-Point Encryption Solution

A **validated** PCI P2PE **solution** must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE-validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage
P2PE Challenges

- Key injection and activation required for P2PE units
- Chain of custody requirements
- The P2PE device may encrypt your campus card

Co-Branded Campus Cards

- Alternate swipes
- White Lists
- Non-ISO card numbers
P2PE Approved Listings

• Regulations were far too tight initially for complex deployments to make it through
  – After 3 years, only 6 vendors were able to obtain certification
  – Most were not in the US
• Version 2.0 divided P2PE solution certification into domains and vendors are now able to be assessed based on the portions they contribute
• P2PE 2.0 now available – Today:
  – 64 P2PE Validated Applications
  – 28 P2PE Validated Solutions
## PCI P2PE Validation & DSS 3.2 SAQ Changes

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Description</th>
<th># Req. v3.1</th>
<th># Req. v3.2</th>
<th>PCI DSS Security Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card not present merchant: all payment processes have been outsourced, no electronic storage of cardholder data</td>
<td>14</td>
<td>21 (+7)</td>
<td>No</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-commerce merchant: direct POST or elements embedded into payment page (iFrame or redirect), no electronic storage of cardholder data</td>
<td>143</td>
<td>182 (+39)</td>
<td>Yes</td>
</tr>
<tr>
<td>B</td>
<td>Merchant uses imprint machines or standalone terminals with dial-out connection via phone line: no e-commerce, no electronic storage of cardholder data</td>
<td>41</td>
<td>41 (+/- 0)</td>
<td>No</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchant uses IP-connected standalone terminals: no e-commerce, no electronic storage of cardholder data</td>
<td>87</td>
<td>87 (+/- 0)</td>
<td>Yes*</td>
</tr>
<tr>
<td>C</td>
<td>Merchant uses payment applications that are connected to the internet: no e-commerce, no electronic storage of cardholder data</td>
<td>144</td>
<td>161 (+17)</td>
<td>Yes*</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchant uses web based virtual payment terminal: no e-commerce, no electronic storage of cardholder data</td>
<td>78</td>
<td>84 (+6)</td>
<td>Yes*</td>
</tr>
<tr>
<td>P2PE</td>
<td>Merchant uses terminals with certified PCI P2PE solution: no e-commerce, no electronic storage of cardholder data</td>
<td>35</td>
<td>33 (-2)</td>
<td>No</td>
</tr>
<tr>
<td>D-Mer</td>
<td>All other merchants</td>
<td>332</td>
<td>332</td>
<td>Yes*</td>
</tr>
</tbody>
</table>

*If systems are reachable from the internet

©usd AG
Resources

PCI Security Standards Council
• https://www.pcisecuritystandards.org

EMVCo
• http://www.emvco.com/

Smart Card Alliance
• http://www.smartcardalliance.org/

Your Financial Partners
• Acquirer / Acquiring Processor
• Payment Gateway Vendor
• POS Provider
Questions
Contact Information

Bart Lawyer
Assistant Director
Office of Information Technology
Duke University
Tel: 919-660-3755
E-mail: barton.lawyer@duke.edu

John Diaz
VP – Product Management
Blackboard Transact
Tel: 919-805-3525
E-mail: john.diaz@blackboard.com
Thank You!!!