PCI: Life after P2PE

Crissy Sampier, Longwood University
Edward Ko, CampusGuard
Agenda

• Background
• Longwood’s PCI DSS Journey
• E2EE vs. P2PE
• Life After P2PE
• Skimming
• Q & A
About Longwood

• Located in Farmville, VA
• About 5,000 students (~1,100 Freshmen)
• SAQ C for the University
• PCI Mission: Reduce Scope
Longwood’s Credit Card Locations

- **Lancer Card Center** – in person and online
- **Dining locations** – FreedomPay readers
- **Athletics** – in person, online and over the phone
- **Theater Box Office** – in person and online
- **University Foundation** – in person, over the phone, online giving and phone-a-thon
- **Bed & Breakfast** – in person, online and over the phone
- **Cashier’s Office** - kiosk
What have we done?

• Dining locations:
  – Upgraded registers to Simphony
  – Using FreedomPay’s P2PE devices at each register

• Other locations:
  – Set up a PCI Network
  – Use Third Party Software online
  – Utilize a Proxy Server (phone-a-thon & kiosk)

• University-wide:
  – Created and Updated Policies
  – Payment Card Information website
    • [http://solomon.longwood.edu/offices--departments/cashiering--student-accounts/payment-card-information/](http://solomon.longwood.edu/offices--departments/cashiering--student-accounts/payment-card-information/)
Happening Now...

- **Dining** – Added standalone P2PE readers
  - iWL252 (Bluetooth/Ethernet) – Catering, etc.
  - iWL255 (cellular) – Food Truck & Concessions

- **University Tickets/FreedomPay integration**
  - All credit card ticket sales processed through University tickets software (online & in person)
  - P2PE device used with PC to offer in-person solution
    - SREDKey PCI Key Pad with Encrypted MagStripe Reader
      - Eliminate phone/network line and VeriFone
      - Eliminate additional steps
Big Rocks

• Reduce scope
• SAQ P2PE
• FreedomPay Integrations?
  – Ruffalo Noel Levitz
  – Blackbaud – Raiser’s Edge
  – TouchNet
  – CBORD – GET or WebManager
  – Reservation Nexxus
• Mobile P2PE readers for campus use
  – Departments (Foundation, Alumni, etc.)
  – Student Use?
Why FreedomPay Integration?

- Reduce Scope
- SAQ P2PE
- Campus solution
- Ease of reporting and reconciliation
- Offers validated solutions
- Save $$
  - Eliminate VeriFone terminals
  - Eliminate analog phone lines in these areas
  - Eliminate separate PCI network
  - Eliminate Proxy
E2EE vs. P2PE

• Only PCI-listed P2PE can reduce scope
• Only PCI-listed P2PE can use SAQ P2PE
• New guidance for Non-listed Encryption Solutions (December 2016)
What’s Left after P2PE

• Protect CHD (3.x)
• Tamper/Substitution Checking (9.9)
• Policies/Procedures (12.1)
• Training (12.6)
• Self-Assessment Questionnaire (P2PE)
Daily Device Inspections and Security

Longwood University

Credit Card Device Inspection Checklist

<table>
<thead>
<tr>
<th>Date</th>
<th>Verify Model/Serial #</th>
<th>Verify device seams are secure (no evidence of tampering)</th>
<th>Verify no skimmers or other devices have been attached</th>
<th>Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Merchants are responsible for securing their credit card devices. Devices are to be examined to ensure that the device has not been replaced, that no attachments have been installed, and that no tampering has occurred. Devices are to be examined daily prior to transaction processing.
Skimming
Skimming
Smarter Skimmers
Annual Credit Card Security Awareness Training

- Annual training for anyone processing credit cards
  - Includes student workers
- Maintain training logs

Longwood University
Credit Card Security Awareness Training

<table>
<thead>
<tr>
<th>Merchant/Department Name:</th>
<th>Lancer Card Center</th>
</tr>
</thead>
</table>

As required by Payment Card Industry Data Security Standards (PCI DSS) and Longwood policy, all individuals involved in credit card processing activities must complete credit card security awareness training upon hire and at least annually.

Individuals within Lancer Card Center (department) completed training as indicated below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Securing the Human</th>
<th>PCI Compliance Training</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date Completed</td>
<td>Date Completed</td>
</tr>
</tbody>
</table>
# Annual Credit Card Merchant Assessment

<table>
<thead>
<tr>
<th>Merchant Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Fiscal Contact</td>
<td>Phone Number</td>
</tr>
<tr>
<td>Merchant Number(s)</td>
<td></td>
</tr>
<tr>
<td>Credit Card Brands Accepted</td>
<td>Visa</td>
</tr>
<tr>
<td>SAQ Level</td>
<td>Last Attestation Date</td>
</tr>
</tbody>
</table>

1. **By what method(s) do you accept credit cards?**
   - ☐ In person
   - ☐ Mail
   - ☐ Fax
   - ☐ Phone
   - ☐ Email
   - ☐ Online
   - ☐ Other

2. **If you accept credit cards in person, do you have a point-of-sale (POS) terminal to accept credit card payments?**
   - ☐ Yes – POS terminal connected to internet
   - ☐ Yes – POS dial-out terminal via analog phone line
   - ☐ N/A

2.1 **Is the credit card number truncated on both the customer’s and merchant’s printed receipt? (last four recommended)**
   - ☐ Yes
   - ☐ No

2.2 **Who is responsible for daily batch settlement?**
   - Name:
   - Title:

2.3 **What type of information is available on the daily batch settlement printed from the POS terminal?**
   - ☐ Itemized sales by customer with full 16 digit credit card number listed
   - ☐ Itemized sales by customer but credit card number is not listed or is truncated
   - ☐ Summarized sales for the batch but sales are not itemized by credit card number/customer
   - ☐ Other

2.4 **Where is the daily batch settlement and merchant copy of receipts stored?**
   - ☐ Unlocked filing cabinet/desk
   - ☐ Locked filing cabinet/desk
   - ☐ Other, specify:

3. **If you accept credit cards in person through a swipe device, please provide:**
   - Manufacturer:
   - Model Number:

4. **Is credit card data entered via computer terminal into a 3rd party website on behalf of the consumer?**
   - ☐ Yes
   - ☐ No

4.1 **If yes, please provide:**
   - Terminal Type:
   - Longwood Tag Number:

4.2 **Is the computer terminal connected to any other system?**
   - ☐ Yes
   - ☐ No
<table>
<thead>
<tr>
<th>PCI DSS Question</th>
<th>Expected Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9</td>
<td></td>
</tr>
<tr>
<td>(a) Are devices that capture payment card data via direct physical interaction with the card protected against theft or loss?</td>
<td>Yes</td>
</tr>
<tr>
<td>(b) Are policies and procedures in place that require the devices to be stored securely at all times?</td>
<td></td>
</tr>
<tr>
<td>(c) Are devices that capture payment card data via direct physical interaction with the card protected against theft or loss?</td>
<td></td>
</tr>
</tbody>
</table>

- **Only 33 questions**
- **No IT-related questions**
- **Still must protect CHD**
- **Still must have policies/procedures**
- **Still must have annual security awareness training**