The Changing Face of Payment Security
Securing Your Campus Payment Environment
FreedomPay makes payments faster, simpler, safer and smarter

A multi-patented, award winning, fin-tech company focused on providing the payments infrastructure required in today’s rapidly changing processing environment.

- 17 years old and based out of Philadelphia, Pennsylvania
- Rapidly expanding North American footprint, launching internationally (UK, EU, JAPAC)
- Leading markets - Retail, Restaurant, Lodging, Food Service, eCommerce, Theme Parks and Stadiums:
  - World’s Top 5 Food Service Providers
  - World’s Top 4 of 5 Global Gaming Providers
  - The Third Largest Bank in the U.S. (11th Globally)
  - World’s Fourth Largest eCommerce Retailer
  - World’s Largest Unattended Solution Provider
  - World’s Second Largest Shipping Company
- Global connectivity across payments ecosystem:
  - Seamless integration to Oracle Payment Interface
  - EMV certification with all major payment processors
  - PCI certified P2PE payment devices with Ingenico and Equinox
Effective October 2015, merchants that update infrastructure to accept EMV payments will not be held financially liable for fraudulent charges.
Assessment of EMV Capabilities

Advantages

• Validates card information to prevent fraudulent charges
• Aligns US merchants with European security standards
• Benefits merchants who have upgraded POS devices by 2015 Liability Shift deadline

Disadvantages

• Leaves cardholder information exposed during transactions
• Fails to protect data on magnetic swipe terminals, online commerce, or mobile transactions
• Does not equate to PCI compliance
EMV + P2PE = True Security

What EMV Does:
- Identifies and validates consumer has a genuine card
- Provides real-time negotiation between chip, terminal and back-end acquirer/issuer network

What EMV Does Not Do:
- Provide data encryption
- Provide tokenization
- Provide security for card-not-present transactions
Encryption + Tokenization

Encryption and Tokenization address the security gaps of EMV and vulnerabilities of clear-text data

- **Encryption**
  - POI Devices injected with cryptographic key
  - Card data encrypted immediately upon contact

- **Tokenization**
  - Card information replaced with proxy data
  - Transactions referenced without exposing data
PCI Validated P2PE

The gold standard for card security

_PCI Validated Point-to-Point Encryption (P2PE) is an extensive set of security requirements set forth by the PCI Security Council_

_Encrypts and protects data from the point of interaction, throughout transport and in storage_
Listed vs. Non-Listed P2PE

<table>
<thead>
<tr>
<th>PTS Device Dependencies</th>
<th>Expiry Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingenico, IPP310, IPP320, IPP350 (4-20184)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, ISMP (4.20183)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, ICMP (4.20235)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, ISC250 (4.30062)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, ISC Touch 480 (4.30098)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, IUC160 (4.30100)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, IUP250 (4.30075)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, IVL220, IVL250 (4-20181)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>Ingenico, IPP310, IPP320, IPP350 (4-20142)</td>
<td>30 Apr 2017</td>
</tr>
<tr>
<td>ID Tech, SREDKey (4.10156)</td>
<td>30 Apr 2020</td>
</tr>
<tr>
<td>ID Tech, SecuriRED (4-10144)</td>
<td>30 Apr 2020</td>
</tr>
</tbody>
</table>

Other Dependencies
- Ingenico, Retail Based Application (RBA) v10.0.12

---

“Official PCI Validation for a P2PE solution means that merchants can significantly reduce their scope for PCI DSS compliance”

- Matt Getzelman
  National PCI Practice Director
  Coalfire Systems Inc.
Scope Reduction

PCI DSS Compliance

- Merchants must comply with the PCI Security Standards to accept credit cards for all transactions
- SAQ P2PE-HW reduces time, cost and complexity of PCI compliance
- 300 controls to approximately 30
Campus Payment Ecosystem

Reduce PCI Scope Across Campus

1. Bursar’s Office
2. Dining Hall
3. Football Stadium
4. Campus Hotel
5. Development Office
6. Food Trucks
Accept credit card payments outside of the network through a hosted payment page or with a merchant portal connected to secure payment devices.
Dining Hall

- Enable credit, PIN-debit, EMV and NFC transactions with a payment terminal integrated with the point-of-sale.
Football Stadium

➢ Sell concessions, tickets and apparel with secure credit card terminals that integrate with the point-of-sale and support EMV and NFC transactions.
Accept online reservations and retain cardholder information with tokenized payment data. Provide Pay at Table devices for EMV cards.
Accept donations at events and over the phone with secure payment terminals and PIN pads connected to a website.
Food Trucks

- Process transactions securely, even when the workstation is offline, with mobile payment devices.
EMV, NFC and swipe-capable P2PE payment terminals that do not require a cashier.
P2PE Payment Terminals

Ingenico iPP320  Ingenico iPP350  Ingenico iSMP  Ingenico iCMP
Ingenico iSelf-Service  Ingenico iSC250  Ingenico iSC480  Ingenico iWL250
Payment Processing

First Data
Elavon
CHASE Paymentech
Heartland
vantiv
WorldPay
T|SYS
MERCURY
global payments
Thank you

Paul Guidone
Vice President, Sales Solutions
Paul.guidone@freedompay.com