Straight Answers on PCI and EMV

Gray Consulting

November, 2015

Why We Are All Here

This presentation is an attempt to demystify the challenges faced by the car wash industry, in dealing with secure, electronic payments.

Before executing on any solution strategy, be sure to consider all factors carefully, ensure current market information, and check with Gray Consulting or your payment expert. All information is correct at the time of publication.

Liability

Breach

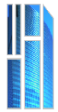
What happens when the bad guys take all your stored card numbers

For the typical car wash, less than one year's worth of cards-on-file could shut down your business

Vs.

EMV

Merchant is liable for counterfeit EMV cards, when the merchant does not use EMV-capable PoS



P2PE, or Not P2PE

PCI Compliant

E2EE
(Non-Validated)

Annual audit and/or complete SAQ C or D

Multiple policy documents

Segmented networks

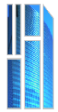
Vs

P2PE
(Validated)

Invest in a validated P2PE solution

Complete SAQ P2PE

Skip annual audit



Car Wash Industry Challenges

EMV is a mandate – *False*

There is no mandate for merchants to support EMV
Only impact is from counterfeit cards - merchant is liable without EMV capability at the PoS

Action -
Know your chargeback rate
Beware non-compliance fees
Stay tuned in to EMV

Car Wash Industry Challenges

E2EE (End to End Encryption) is a mandate - *False*

Only PCI compliance is mandated
A merchant or provider may validate without E2EE or P2PE

Action –
Encrypting vulnerable, valuable PAN data is still the point.
Devalue it on your network to minimize impact of breach

Car Wash Industry Challenges

Hackers are breaching millions of cards every week - *True*

Hackers are attacking virtually any merchant with an IP address, and many other vectors

Action –
PAN data represents tremendous value to the hacker. Devalue card data on your system!

Update Strategy

	Urgency	Description
1	Very High	Encrypt stored PANs with tokenization End Goal: No PANs on file
2	High	Implement E2EE – PoS upgrade End Goal: PAN-free network + PCI Compliance
3	Strategic Decision	Implement P2PE – industry-sponsored security End Goal: Zero Breach Liability + Low-Cost Compliance
4	ROI & Regs Decision	Implement EMV – Mitigate counterfeit fraud costs End Goal: Readiness for mandated EMV

PoS Unattended Hardware

Expect hardware shortages to continue for a year or more. Plan for P2PE as the end goal, but in the meantime:

- Delay hardware upgrades as long as possible, assuming no other driving factors
- Maintain PCI compliance
- Watch industry regulations & guidelines

Hot Off the Presses

Visa Announcement

Released 29 October 2015

Key Statements

- "Effective 31 March 2016, acquirers must require all newly boarded Level 4 merchants to use only Payment Card Industry (PCI)-certified QIR professionals"
- "Effective 31 January 2017, acquirers must ensure their Level 4 merchants validate full PCI DSS compliance annually."

Implications

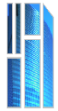
- Installers will need certification to install PoS hardware PCI QIR List
- Acquirer no longer sets the bar for validation for Level 4 merchants - some validation loopholes will disappear

The Bottom Lines

- Devaluing the PAN with encryption is the only practical strategy to mitigate the threat of a business-destroying breach

- Implement encryption across your entire network; expect trend towards P2PE as an industry standard to continue

- Defer EMV enablement as long as it makes business sense, while maintaining good future-proofing investment strategies.



Who is Gray Consulting?

- Independent perspective into the payments market
- Deep insight into EMV and PCI
- Staunch advocate of PAN-less payments

- 40+ cumulative years in technology and payments
- Clients throughout the acquiring, networking, security and technology sectors in payments
- 10+ years as independent consultants and merchant advocates

- *www.grayconsulting.com/contactus*