Payment Painkillers:

How to secure customer payment data in a complex world

Payments Network
THE PLACE FOR PAYMENT SECURITY ADVICE

Vodat INTERNATIONAL LTD.

A better way to secure payment data

There is a more secure, affordable, manageable and sustainable way for retailers to secure customers' payment data and it doesn't involve Point to Point Encryption (P2PE).

Vodat International has created this special report to help senior retail executives build an effective strategy for getting PCI compliance.

It starts with understanding the real cost to your business of poorly secured payment data.

Payment data is vulnerable and under continuous assault. In fact, it remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals. 74% of attacks on retail, accommodation and food services companies target payment card information .

A breach costs on average £95 per customer record lost, of which over half (£50) is due to indirect costs such as drops in turnover and customer churn.

> *cost of a breach is £2.21m, up 8% on 2013*

Per company, the average cost of a breach is £2.21m, up 8% on 2013 due mostly to increased customer churn, proving that consumers are becoming more aware of payment security and voting with their feet .

Where there is an obligation on the retailer to secure critical customer data – credit and debit card information – the response from many retailers has been both mixed and heavily delayed. According to a Government report on information security breaches, retailers spend the least on information security compared to other sectors in the UK.

> *74% of attacks on retail, accommodation and food services companies target payment card information .*

Retailers are still not effectively securing payment data

Payment Card Industry (PCI) compliance is mandated by the Card Schemes and the PCI Security Standards Council created the standards that retailers must attain, and yet companies are still not PCI compliant. A recent report into the payments landscape revealed:

- Only 38% of businesses are PCI compliant
- Only 27% of retailers fully understand the PCI requirements and how to gain compliance
- Only 19% are aware of the penalties for non-compliance

Confusion in some areas clearly reigns, further complicated by the advent of Point-to-Point Encryption (P2PE), promoted as the Holy Grail for PCI scope reduction, but which hides some uncomfortable truths.

The cost of implementing P2PE will almost certainly be higher than most retailers appreciate. Worse, it will not reduce the scope of PCI quite as much as has been suggested. The result might be that merchants ends up with two headaches: one for PCI and one for P2PE, both of them painful, expensive to remove, and likely to return unless carefully managed every day.

P2PE only covers the customer-present environment, so excludes both online and the call centre. In addition, some so-called P2PE offerings are not validated solutions, as listed on the PCI web site, running further risk that these recommendations will not be accepted by a QSA.

What's wrong with most P2PE services?

Inflexible – as the solution has been developed by commercial organisations, many of the P2PE solutions are developed for specific hardware, so there are limited integration capabilities

Complex – complicated managed environment to maintain compliance

Expensive – implementing P2PE involves extensive software and hardware changes for all transaction points

Counter-productive – P2PE designed to take data security responsibility away from retailers. P2PE compliance management shifts that responsibility back to the retailer

1 Verizon, Data Breach Investigations Report, 2013
2 IBM/Ponemon Institute, Cost of Data Breach Study: United Kingdom, 2014
3 Department for Business and Innovation Skills/PWC/Infosecurity Europe, Information Security Breaches Survey, 2014
4 Sage Pay, The Payments Landscape, 2014

A road less travelled

The claim that P2PE is the only option for reducing PCI scope is wrong. There is an alternative that is more secure, affordable, manageable and sustainable.

It involves removing sensitive card data from the merchant's network altogether, to the extent that 10 of the 12 PCI Data Security Standards (DSS) requirements are wholly delivered by a third party. Even for the remaining two, PCI compliance scope is reduced.

The end result is that the solution delivers the same benefits of scope reduction without the constraints of implementing P2PE.

This solution is Vodat's Unified Payment Service.

*The alternative to P2PE: **Remove sensitive card data altogether***

The Vodat solution in detail

Vodat's Unified Payment Service is an integrated in-store solution that provides retailers with a single, fast and secure interface for all card present EFT transactions. The service is managed totally by Vodat International through a secure, resilient network.

The solution consists of IP based Chip and PIN Entry Devices (PED) and a managed firewall. The firewall provides network isolation between the PEDs and the in-store network. All communications from the Point of Sale (PoS) to the PED and back are via the firewall into and out of the Vodat secure data centres. The PoS and PED are never connected and never communicate directly. Implementing payment solutions in this way reduces scope against the PCI DSS.

Highlights

- **All traffic to the PEDs from the merchant network is considered untrusted and blocked.**
- **The PEDs can only communicate with the Vodat Unified Payment Service data centres in order to process payment.**
- **Merchant personnel have no access to the firewall management interfaces.**

Vodat's managed firewall is configured with a number of additional security features that further assist in mitigating threats as well as in meeting PCI compliance requirements:

- Network Address Translation
- Intrusion Detection
- ARP Spoofing prevention (assists with man in the middle mitigation).

Unified Payment Service grew out of an industry oversight; the Special Interest Group (SIG) that worked on P2PE overlooked what was the simple option. A number of Chip and PIN terminal manufacturers already supported Transport Layer Security (TLS), which forms the basis of the Vodat Unified Payment Service, a Secure Alternative to P2PE, and a Level 1 PCI DSS compliant service.

Vodat further enhanced the solution using encryption, which occurs on the PED. All data remains encrypted until it's safely received in Vodat's secure data centres. Because Vodat operates the service this also reduces scope for users; there is no complex key management or rotation processes to implement and no central infrastructure scope.

PCI DSS Requirement (based on SAQ B-IP)*	Vodat Responsibility	Merchant Responsibility
Requirement 1	Wholly delivered by Vodat	
Requirement 2	Wholly delivered by Vodat	
Requirement 3	Wholly delivered by Vodat	
Requirement 4	Wholly delivered by Vodat	
Requirement 6	Wholly delivered by Vodat	
Requirement 7	Wholly delivered by Vodat	
Requirement 8	Wholly delivered by Vodat	
Requirement 9	Guidance provided by Vodat	Physical security responsibility of merchant
Requirement 11	Wholly delivered by Vodat	
Requirement 12	Guidance provided by Vodat	Reduced requirement in SAQ B-IP

* Requirement 10 (track and monitor all access to network resources and cardholder data) is not in this list because it is not required for SAQ B-IP.

Vodat's approach to payment data isolation has been validated and endorsed by a leading independent IT audit and compliance firm, Coalfire, and the global Thought Leaders on enhancing the security of vital data and communications resources, MWR InfoSecurity. The architecture and benefits of this approach are published in a white paper (LINK).

Why act now?

Merchants have been urged for nearly 10 years to ensure that their systems are fully PCI compliant, which explains the sense of fatigue many now experience at the constant barrage of vendor pressure.

However, the business imperatives are mounting as merchants recognise that their current legacy systems and PoS hardware are no longer able to serve the multi-channel consumer.

Worse, PCI PTS v1.x PIN Entry Devices must be replaced by 31st December 2017; although Vodat's Unified Payment Service ensures no

> *current legacy systems and PoS hardware are no longer able to serve the multi-channel consumer*

customer data reaches the Point of Sale, so replacement can focus on PEDs rather than the whole network and PoS operating system.

The urgency to act should be based on retailers' desire to secure customer data and avoid the financial and reputation resulting from breaches, regardless of whether it will be mandated or not.

> *"We recommend that organizations define, implement, and maintain a process to proactively manage the scope of compliance for each environment."*
>
> Government Report on Information Security Breaches

Where to start

As the leading provider of telecom solutions and private managed networks to retailers, Vodat recommend that we carry out a free review of your current network to determine where the vulnerabilities lie.

Click here for more details