White Paper

VERIFONE IN UK AND IRELAND

Payment fraud threatens retail business

P2PE helps you fight back

Foregenix

Verifone®

Every day there are new 'headlines' relating to data breaches. Globally and locally, criminals are targeting organisations that store or transmit customers' Personally Identifying Information (PII) and payment data.

A staggering 82% of financial institutions now say payment card fraud is the most common form of fraud[1]. In 2016, fraud losses on UK-issued cards alone totaled £618.0 million, an increase of 9% on 2015[2]. That means that card fraud as a proportion of card purchases now equates to 8.3p for every £100 spent[1].

Criminals are targeting retail checkouts

Retailers are one of the most popular targets for cybercriminals, experiencing nearly three times as many attacks as elsewhere in the financial services sector[3]. In fact, loss of personal information from merchants more than doubled from 2014 to 2016[4]. On top of that, 64% of retail data disclosure breaches were caused by point of sale (POS) intrusions[5].

'Fraud losses of £618m on UK-issued cards alone'

This cost of fraud is high

The annual bill for UK retail crime soared to £613m last year. And up to 36% of this was retail cyber-crime[6]. While some incidents are isolated, many are symptoms of bigger underlying issues. If card fraud occurs, unless merchants can prove that they were fully Payment Card Industry Data Security Standard (PCI DSS) compliant, they can be held liable not just for the cost of the fraud but other costs too such as the cost of an investigation to determine how the fraud occurred and remedial costs to become compliant. In addition, the introduction of the new EU General Data Protection Regulation (GDPR) in May 2018, will usher in non-compliance fines of €20 million or 4% of turnover (whichever is greater) per breach.

Merchants must also bear the often larger cost of reputational damage and loss of customer confidence, which can linger for years. A recent study shows that 75% of adults in the UK would stop doing business with an organisation if it was hacked.[7]

Despite safeguards, data is still compromised

The depth and breadth of anti-fraud solutions has helped reduce risk. Today, retail IT professionals feel they are more prepared for handling breaches than they were two years ago. They are increasingly confident in their ability to discover data breaches, with 90% now claiming they can detect one within a week, compared to 70% in 2014[4].

'80% of breaches investigated are UK based'

Despite this, in the past 12 months Foregenix, the global leaders in data forensics and information security, has seen their case load multiplying nearly 8 fold from 2013 levels. It reveals that 80% of breaches investigated are UK based and 44% involve hospitality, retail or financial services. Within these, Foregenix's team of experts has identified the top three attack types as: Targeted Malware; Application Vulnerability Exploits; Structured Query Language (SQL) Injection.

As the US rolls out EMV, the subsequent tightening of security standards has shifted the emphasis for fraudsters. They are responding with ever increasingly sophisticated attack methods. There is now a major skills mismatch between criminals and retail IT professionals, who are finding it increasingly difficult to keep up with a new generation of hackers with extensive IT skills.

'75% of adults in the UK would stop doing business with an organisation if it was hacked'

Even with PCI there are still challenges

PCI DSS Compliance helps keep a high proportion of transactions safe from base level attacks and provides much needed accountability for those delivering retail services. However, it presents a number of challenges for retailers:

- **Disparate legacy systems**
  These often have flat networks resulting in data spread across many locations.
- **Financial burden**
  PCI costs are high, which leaves IT departments with reduced budgets to invest in new technology.
- **Skills base**
  Reliance on best practice to implement, which in turn calls for specific in-house skills/knowledge.
- **Education effort**
  Everyone must be aware of the PCI process from senior management to till operators.

Locking down the payment chain

Built on a solid reputation of trust and reliability, Foregenix are forerunners in information security; helping to simplify compliance and secure payment environments. Verifone are the global leaders in secure payment services and solutions and also sit on the PCI Security Standards Council (SSC). Together, they work with some of the world's leading retail brands and are responsible for securing millions of transactions daily.

Both agree that, for PCI to be effective, the network environment – as well as devices – needs to be properly secured in order to lock down retailers' systems from hackers and malware. Together they support Point-To-Point Encryption (P2PE) as the most logical route to achieving this – addressing fraud while creating minimal effort for the retailer.

This is backed by PCI assessor companies, who also confirm that a well-architected, properly deployed PCI P2PE solution can virtually eliminate the current risk of credit card data compromise for retail environments and provide a clear and dramatic reduction of PCI compliance scope which, in turn, reduces the cost of PCI compliance assessment and validation.

How PCI P2PE works

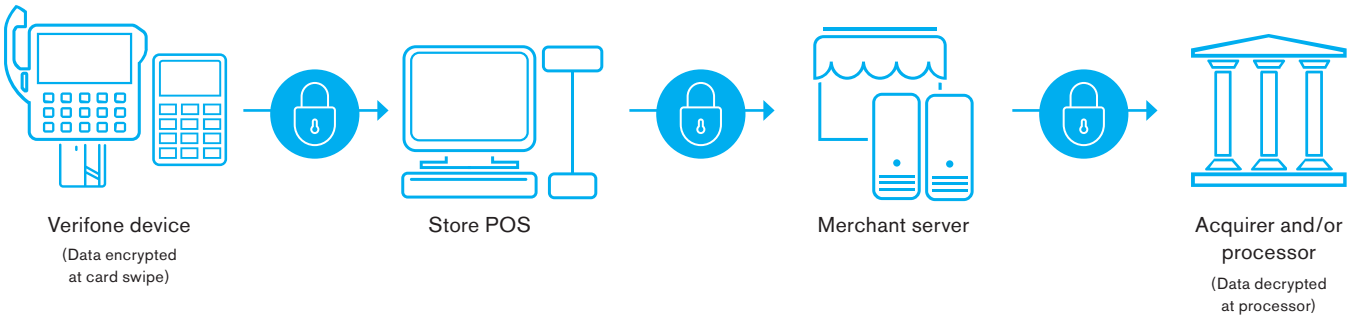
PCI P2PE is the ultimate 'gold standard' for merchant security. It works by addressing the risk of unauthorised interception associated with cardholder data-in-motion during the transmission from the POS terminal to the payment processor.

It also encourages best practice in terms of managing PIN Entry Device (PED) life cycles and operations. All of this helps to prevent criminals from accessing card data at the point of sale.

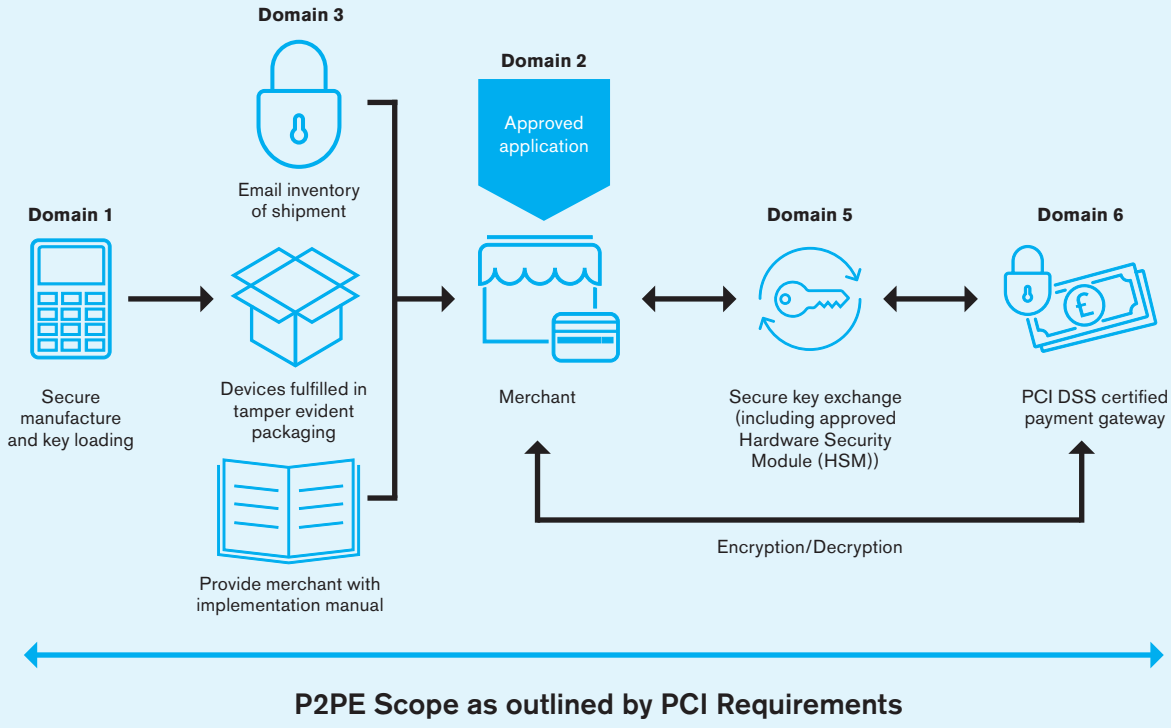
PCI P2PE protects credit card data as it travels through a merchant's local network and across the internet before it reaches the payment processing system.

With PCI P2PE all card data is encrypted on the secure card reader itself and decrypted in a trusted PCI certified gateway. Card data is never decrypted in the merchant's own systems. This effectively locks down the payment chain. If a criminal gets into the system, any data extracted is useless to them without access to the relevant encryption keys.

Importantly, PCI P2PE does not have any negative impact on the user experience or journey. There is no change to the way card payments are accepted – no loss of speed or service. All the encryption is managed by the terminal invisible to the cardholder.



Merchants who adopt certified P2PE solutions and processes can dramatically reduce their PCI scope



P2PE cuts fraud & delivers retail advantage

If PCI P2PE is properly applied, it can **eliminate skimming devices by more than 95%** as terminals are securely delivered to the stores. It also **reduces data compromise risk and liability by more than 80%**, as the cardholder data is encrypted thus eliminated from the stores.

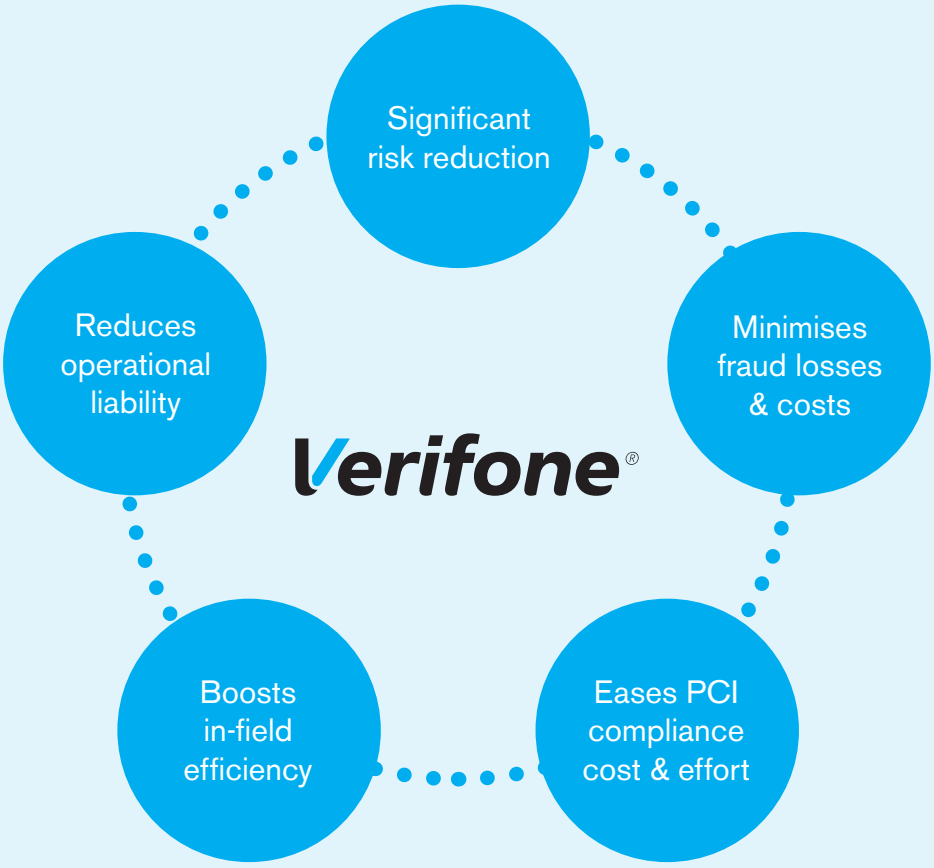
'PCI P2PE can eliminate skimming devices by more than 95%'

PCI P2PE not only **reduces fraud but also boosts operational efficiency by more than 25%**, because the payment solution provider can manage activity remotely on behalf of the retailer. Implementing a PCI P2PE solution has shown to **reduce cost and complexity of PCI DSS compliance for merchants by more than 50%.**

'Implementing a PCI P2PE solution has shown to reduce cost and complexity of PCI DSS compliance for merchants by more than 50%'

Many UK retailers are already realising the advantages of PCI P2PE using Verifone Payment as a Service, an end-to-end solution that makes it easy to manage payments and compliance – and to achieve security best practice every step of the way. **Over 200,000 Verifone Secure Reading and Exchange of Data (SRED) devices are connected to leading third party platforms supporting PCI P2PE.**

The benefits of Verifone PCI P2PE Payment Solutions



Does PCI P2PE impact customer tracking and Customer Relationship Management (CRM)?

PCI P2PE does not impact customer tracking and CRM if it is used in tandem with tokenisation, which is supplied as standard on all Verifone PCI P2PE solutions. Software-based, tokenisation replaces the cardholder's Primary Account Number (PAN) with a randomly-generated proxy alphanumeric number ("token") that cannot be mathematically reversed. This is used for long-term storage or as a transaction identifier.

For merchants, it is ideal for recurring payments as the card number is only on the merchant's network 'in flight' during the initial transaction – which can be encrypted and protected using P2PE. Beyond that, the merchant uses the token that represents the original card, for subsequent payments or to track customer transactions for marketing purposes. This allows personalised marketing programmes to be developed and targeted using cardholder purchase history data.

Using the right tools

Only PCI PIN Transaction Security (PTS) certified payment devices with SRED and OP approvals – such as Verifone's VX, MX, UX and E-series devices – can be used in an approved PCI P2PE environment. All payment devices in a PCI P2PE environment must also be handled according to the P2PE Implementation Manual (PIM) document and be traceable from birth to death of the device.

Merchants can only use 'non P2PE certified devices' in a P2PE environment if they choose to opt out of PCI P2PE at the chosen payment location. With PCI P2PE all card data is encrypted on the secure card reader itself and decrypted in a trusted PCI certified gateway. In this case, card data is never decrypted in the merchant's own systems.

Using PCI certified P2PE solutions and following the PIM guidelines, merchants' operations can be taken out of scope. This means retailers only have to complete a simple self-assessment form – in the same way that small and micro merchants do – instead of having to submit their entire operations to expensive and time consuming PCI audits.

This can potentially save large scale retailers millions in audit fees. This cost saving alone is enough to persuade major retailers to switch to PCI P2PE certified solutions, as they take advantage of an opportunity to cut their expenditure.

'Using PCI certified P2PE solutions can potentially save large scale retailers millions in audit fees – enough to persuade major retailers to switch to PCI P2PE certified solutions'

For service providers & integrators

PCI P2PE made easy

Given the benefits to retailers, it makes sense for service providers to migrate to PCI P2PE based solutions. To make it easier for them to do this, Verifone has developed a PCI P2PE toolkit.

Eliminating unnecessary development and costs, it includes everything a third party service provider needs to create their own certified PCI P2PE payment solutions.

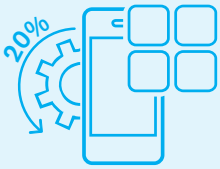
This includes PCI PTS Card Acceptance Devices, SRED Operating Systems, Key Management & Authentication, Documentation, PIM and Integration and Test Tools as well as easy to use Verifone Integrated Payment Architecture Application Programming Interface (VIPA API) or Software Developer Kit (SDK) for effortless integration.

Open and agnostic, the Verifone PCI P2PE Toolkit can be used by any system integrator and third party provider to develop pre-certified P2PE solutions and validated processes for any merchant type, size and channel.

In the UK, Verifone PCI P2PE Toolkit is already being used by leading integrators and service providers.

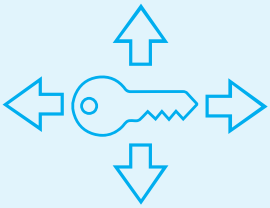
Protecting more than 200,000 terminals nationwide, it has been shown to:

Reduce cost, time and complexity of PCI P2PE by more than **60%**



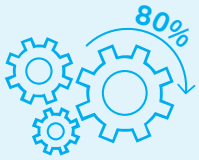
Reduce integration, application development cost by **20%**

Shrinks `lead times' by **20%**

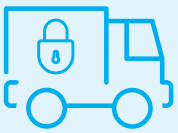


Ease management and in-field distribution of **encryption keys**

Deliver **effortless P2PE** across even the largest estates



Reduce configuration costs by more than **80%**



Minimise risk of tampering during transit

Ensure best practice and skills by delivering full consultancy, support and training

Summary

Both Foregenix and Verifone believe that PCI P2PE is a positive way for the industry to unite and clamp down on retail fraud. By providing expert guidance, comprehensive tools and encouraging P2PE best practice among providers and merchants, they are championing higher standards of security in order to reduce risk to their customers and improve the safety of consumers. At the same time, officially reducing PCI scope – and thereby costs – for retailers.

In order to do this, however, PCI P2PE solutions must use validated devices and processes as well as secure encryption methodologies and cryptographic key operations – including key generation, distribution, loading/injection, administration and usage. They must also utilise approved best practice while managing end of life devices.

Properly applied PCI P2PE can benefit retailers by:

- reducing scope, complexity and burden of PCI DSS compliance
- ensuring greater protection for cardholder data – from swipe through processing to settlement
- decreasing security compliance costs
- reducing threat of non-compliance and financial liability
- decreasing risk of cardholder data fraud and increase data protection
- reducing software development cost
- simplifying payment processing architecture
- allowing easy integration with current infrastructure, across multiple physical locations, using simple SDKs.

About Verifone

As a PCI P2PE validated solution provider, PCI P2PE validated P2PE application provider and PCI PTS SRED approved terminal supplier, Verifone is uniquely positioned in the market to offer end-to-end PCI P2PE payment solutions for retailers. It is also the only vendor to offer a full PCI P2PE Toolkit to service providers and partners.

‘Verifone is the only vendor to offer a full PCI P2PE Toolkit to service providers and partners’

About Foregenix

Foregenix was the first assessor in the world to be accredited by the Payment Card Industry Security Standards Council (PCI SSC) to guide and assess payment applications against its P2PE standards. Foregenix P2PE Certification services are delivered by one of the industry’s leading Qualified Security Assessor (QSA) teams with substantial experience and skills in assisting P2PE Solution Providers in securing their solutions.

‘Foregenix was the first assessor in the world to be accredited by the PCI SCC’

References

1 ISMG 'Faces of Fraud: The 2016 Agenda'

2 Financial Fraud Action UK Year-end 2016 Fraud Update

3 NTT Group 2016

4 Tripwire 2016

5 Verizon 2016 Data Breach Investigation Report

6 British Retail Consortium Annual Retail Crime Survey, published February 2016

7 Centrify June 2016

Abbreviations

API	Application Programming Interface
CRM	Customer Relationship Management
EMV	Is a global standard for credit and debit payment cards based on chip card technology" taking its name from the card schemes Europay, MasterCard, and Visa – the original card schemes that developed it
HSM	Hardware Security Module
ICO	Information Commissioner's Office
P2PE	Point-to-Point Encryption
PAN	Primary Account Number
PCI	Payment Card Industry
PCI DSS	The Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PED	PIN Entry Device
PII	Personally Identifying Information
PIM	P2PE Implementation Manual
POS	Point Of Sale
QSA	Qualified Security Assessor
SDK	Software Developer Kit
SRED	Secure Reading and Exchange of Data
VIPA	Verifone Integrated Payment Architecture

Verifone can help with PCI P2PE solutions for retailers and service providers. Find out more:


www.verifone.co.uk


info-emea@verifone.com


@Verifone_EMEA

Find out more about Foregenix digital forensics and PCI P2PE compliance services:

www.foregenix.com