Spire PAYMENTS

Transaction. Interaction. Convergence.™

Are your point of sale devices secure?

Any merchant taking card payments must ensure their equipment meets the necessary security standards. This is of paramount importance to ensure cardholder data is protected and to minimise merchant liability for any payment fraud undertaken on their system.

These security standards are mandated by the major card schemes and are defined in a wide ranging set of standards published and maintained by the Payment Card Industry Security Standards Council (PCI SSC). The best known of these standards is the Payment Card Industry Data Security Standard (PCI DSS). The scope of PCI DSS is broad as it covers all equipment processing, transmitting or storing cardholder data, but of particular note here is the need for all point of sale devices which accept cardholder personal identification numbers (PINs) to be certified as secure.

What makes the situation more complex is the need to continually develop these security standards to counter the ever more elaborate attacks made by criminals on global payment systems. As such, PCI PTS continually evolves and any new point of sale device brought to market must meet the latest standards. The standard version, sometimes referred to as a certification level, is defined by a two digit number. The first digit is most relevant with the current PCI PED standard being referred to as PCI PTS 5.x, published in September 2016 and replacing its predecessor PCI PTS 4.x.

Understandably, as these standards develop, deployed devices start to fall behind current PCI requirements. To ensure the integrity of the global payments system is maintained dates are published by the major card schemes to indicate when devices with older versions of PCI PED compliance firstly can no longer be deployed, and secondly should be removed from use (referred to as retirement or sunset dates).

Who's responsible?

It is the merchant's responsibility to ensure deployed point of sale devices are not in service after the retirement date. Non-compliance may result in merchants facing fines and be potentially liable for fraud on their payment system.

The table below shows the VISA Europe retirement dates:

PCI PTS Level	Device type	No new deployments after	Retirement date
1.x	Attended	April 2014	December 2017
1.x	Unattended	April 2014	December 2020
2.x	Attended	April 2017	December 2020
2.x	Unattended	April 2017	Not yet defined

Who's responsible?

It is the merchant's responsibility to ensure deployed point of sale devices are not in service after the retirement date.

How does a merchant find out the PCI PTS level of deployed devices?

The simplest way of identifying the PCI PTS compliance version for a payment device is to refer to the lists published online by the PCI SSC. The council maintains separate listing for expired devices (PTS 1.x and PTS 2.x) and another one for non-expired ones (version 3.x onwards).

Devices compliant with versions 4.x or later also include a public Security Policy document to facilitate the identification of valid devices. For older devices (3.x) it is also recommended to contact the hardware provider.

What to do next?

If payment devices are deployed beyond their retirement date they must be replaced immediately. However, if deployed devices are within two years of their retirement, a succession strategy should be put in place to avoid non-compliance in the future.

It's not all bad news

Investment in upgrading payment systems can be a hard pill to swallow but the underlying benefits are numerous. Apart from minimising the risk of fraud, associated fines, brand damage and bad press, the deployment of new point of sale devices ensure a merchant can increase profitability by exploiting the latest technologies:

Increase sales
Exploiting the power of the latest point of sale devices reduces transaction times which in turn reduces queues and minimises the risk of shoppers deciding not to purchase goods due to long waiting times to pay.

Never turn a customer away
Shoppers are demanding merchants accept a wider range of payment methods such as contactless cards and mobile phone applications such as Apple Pay, Android Pay etc. The latest point of sale devices support these as standard.

Reduce the risk of not being able to take card payment
New devices are more reliable due to the fact they are new and also exploit the latest technologies. This reduces the risk of failure and not be able to accept card payments until a replacement terminal is provided.

Increase customer loyalty
The ability to support loyalty schemes on the latest point of sale device is becoming more common, which in turn promotes customer retention.

Additional revenue
Revenue can be earned by allowing third parties to advertise on the screen on your point of sale device thanks to large colour displays.

Increased protection for your customers
Newer payment devices implement additional physical and logical protections against theft, including card data encryption capabilities known as SRED.

How Spire Payments can assist

Spire Payments can not only provide a complete range of payment solutions (including mPOS) accredited to PCI 4.x and PCI 5.x, but can also manage the upgrade of complete estates, from remote deployment, merchant training and 24/7 help desk support. If this is of interest please visit www.spirepayments.com or contact merchantelite@spirepayments.com.