Interview with Graham Thompson, GDPR, PCI & Data Security Advisor

Director DataDivider Inc.

The travel industry must protect itself against €20M plus fines

Why?

All travel businesses need to get serious about true compliance to the ten year old global PCI DSS (Payment Card Industry Data Security Standard) because of the introduction of the new EU General Data Protection Regulation (GDPR) which will become pan European law on 21 April this year (2016) and will become enforced in early 2018. The GDPR fines (the larger of 4% of global annual turnover or €20M) will not only supersede the PCI DSS fines but more importantly the GDPR will enforce public reporting of any PCI DSS breach potentially forcing business closure. The PR nightmare from such a publication could well outstrip the cost of the GDPR fines.

Who is affected?

All sectors of the industry taking credit card face-to-face, internet, phone, fax or email payments are impacted.

What is PCI DSS?

PCI DSS is a prescriptive security standard with some three hundred security controls which needs to be adhered to, audited and reported upon annually. All businesses that process credit card payments have to be compliant to the standard. The standard, now in its third version, is defined by the PCI Council on behalf of the five credit card schemes (Visa, MasterCard, American Express, Discover and JCB) and enforced by your credit card acquirer (WorldPay, Barclaycard, Elavon, Lloyds Cardnet, Global Payments, etc.) again on behalf of the schemes. To date enforcement has been very light handed as the merchant (business taking credit card payments i.e. you in your travel business) is the customer of the acquirer. Policing customers always proves problematic as if the merchant doesn't like the policing they can move to one of the acquirer's competitors. However, with the new GDPR that is all about to change.

So what are the real challenges for the travel industry?

The travel industry has a number of challenges when attempting to comply with PCI DSS. The most challenging environment is that of the hotel reception and the high street travel agent where staff have to multi-task in terms of taking payments by phone, fax, email, mail and face-to-face.

Concepts such as a paperless environment to stop an employee writing down a credit card number are just impractical and unworkable. It is therefore important to minimize the exposure of credit card details to staff and have strong security policies forbidding the writing down of credit card details onto paper.

So how can a travel trade business minimize exposure to credit card details?

Let's first look at telephone payments.

It is important not only to keep these details from being written down but ensuring that these are protected against hackers getting access to this sensitive data. The most cost effective protection to secure phone based payments is to use a SaaS (Software as a Service) security service that affords the ability to capture the card details without exposing them to the local machine or network. Rather than employees typing card details using their keyboard they are presented with the Virtual Keypad (see figure 1). Using their mouse they click on the rotary keypad entering each credit card digit. As the digit 0 is initially placed in a random position it is not possible to correlate any mouse click coordinate to a specific digit. As the SaaS security service prevents a hacker getting access to any screen images it is impossible to reverse engineering (reconstruct) the mouse click coordinates back to the credit card number. The Virtual Keypad although accessed locally actually runs remotely in a highly secured PCI Certified hosted environment. Here the secured credit card details can either be used to process the payment or stored for subsequent payment. In the latter case a unique identifier with the same first six digits (the BIN representing the issuing bank of the credit card) and the last four digits is generated and commonly referred to as a token. This "Token", which has no value to a hacker, can be returned back to your business to process future credit card transactions. Keeping the first six and last four digits is very helpful as you can ask your customer would they like to use, for example, their Barclaycard ending in 1234.

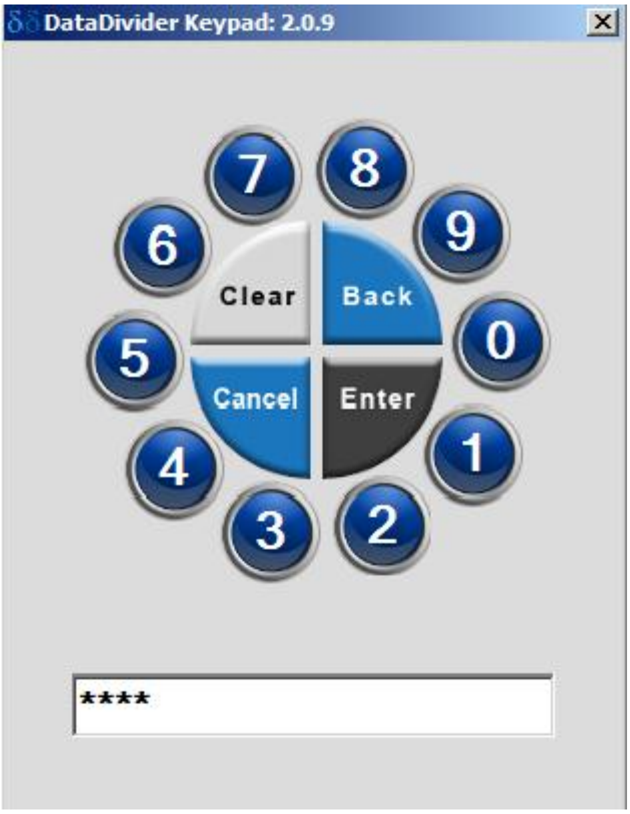

Figure 1 : Virtual Keypad

In effect, by ensuring the credit card details are not exposed to the desktop or its local network it has been possible to de-scope these environments from PCI DSS negating the significant cost and risk of securing this data locally. This is the same philosophy as adopted by most merchants in their brick and mortar businesses and ecommerce where they have adopted P2PE (Point to Point Encryption) and Tokenization respectively to again ensure their businesses are never exposed to credit card details.

Is this also possible for email, mail and fax based payments?

Yes - For each of these communications which include credit card details there are PCI certified service providers who have the capability of intercepting these communications and substituting card details with tokens. Images or texts are then provided with these tokens which are out of scope from PCI DSS. At the point of requiring the processing of a payment the token can be used. These hosted PCI services simply reverses out the token for the original credit card number.

Is there any way of circumventing compliance?

NO! - The EU GDPR is going to make the total compliance of the PCI DSS essential for all travel businesses processing credit card payments by the start of 2018. Travel businesses need to adopt PCI de-scoping strategies ensuring the minimal exposure to credit card data to eliminate the risk of any breach which, from 2018, will have business critical consequences.

For further information or h-res photography please contact:

Alison Cryer: alison@representationplus.co.uk, 07831 555 106

If using all or any part of the above copy please quote: **Graham Thompson, Director DataDivider Inc.**