Clarifying key facts about PCI DSS and call recording

The PCI DSS call recording guidelines are maturing. In parallel, conflicting and sometimes inaccurate interpretations of the directive are becoming more prevalent. The end customer, for whom the guidelines have been introduced, appears to being lost in the mix. For a business seeking to sort out their PCI DSS compliance needs, it is becoming a needlessly confusing place to be.

One of Eckoh's core values is to deliver straightforward technology which is easy to understand and use. We have been clocking the growing confusion around PCI DSS with concern as, in our opinion, it is unnecessary.

So with the objective of informing instead of confusing, we have laid out some key facts, explained in plain English, about PCI DSS and what it means for business taking payments by phone and recording calls.

PCI DSS and call recording - key facts

- The PCI DSS guidelines do apply to your business if it takes card payments by phone and records its calls.
- These guidelines have been put in place to protect your customers' card data and to reduce the risk of credit card fraud. It is a customer centric measure and of course, happy customers stick around,so ultimately, PCI DSS can be good for your business.
- The PCI DSS guidelines specify that after a payment has been authorised, the sensitive authentication data (i.e. the three- or four digit CV2 security number on the card) are not stored in any format. That means not in stored data files, not in recorded calls, not in a spreadsheet, not in an email and not scribbled down on paper whilst taking a call.
- If you store the PAN (that'sthe long number on the front of the card) then you need to ensure it's encrypted. However, encrypting the CV2 is not acceptable – you simply can't store it at all.
- The PCI DSS guidelines don't say that agents cannot be involved in taking a card payment over the phone. They do recommend that you should consider ways of preventing an agent who takes card payments by phone from being able to see sensitive card data on their screen.
- There is no approved method for making your business' call recordings PCI DSS compliant. There are several ways to meet the guidelines but you will need to choose what works best for your business. Compare these methods of making call recordings PCI DSS compliant at http://www.callguard.com/pci-dss/compare/.

So there you go: six uncomplicated key facts about PCI DSS and call recordings.

Find out more: Call: **08000 630 730** Click: **tellmemore@eckoh.com** Visit: **www.eckoh.com** Tweet: **@eckoh**