PCI DSS: De-scoping your contact centre -

What some vendors won't tell you *(but you need to know)*

How many customer payment channels do you have today? Securing all of them to PCI DSS standards can sometimes prove tricky. SSL is good for online security, and Chip & Pin is ideal for face-to-face sales. Most businesses have taken steps to make these channels more secure. But what about Card not Present MoTo transactions made over the phone to your contact centre? Fraud in the sector is set to reach £680m by 2021[1] as criminals target this softer underbelly.

So, it's vital when considering how to protect your business you understand exactly what you are protecting. It's complicated by new vendors are entering the PCI DSS market offering to secure payments, making broad promises about "descoping", but to what degree?? SAQ A or SAQ D. These promises can be thin, and or even misleading. In many cases it is not descoping but really de-risking.

Here's where life can get murky, confusing and risky. However, this at-a-glance guide will help you to know exactly what you're protecting — so you can avoid costly and embarrassing mistakes.

De-scoping the contact centre: How deep do you want to go?

If you're a customer service director, contact centre manager, chief security officer or head of compliance then you'll have a special interest in contact centre security for three good reasons:

#1 Staying secure

Losses from Card-Not-Present (CNP) fraud in the UK stand at over £400m each year. A security breach can cost companies dearly in terms of fines, customers and lost reputations.

#2 Keeping compliant

You'll also want to maintain PCI DSS compliance to achieve industry standards — and pass those regular audits that keep you on the right side of the major card schemes.

#3 Being cost effective

UK contact centres use an average of 3 different PCI DSS solutions to maintain compliance. The challenge with these 'sticking plaster' solutions is that they are difficult to manage and it's hard to understand the real cost.

But here's the health warning ...

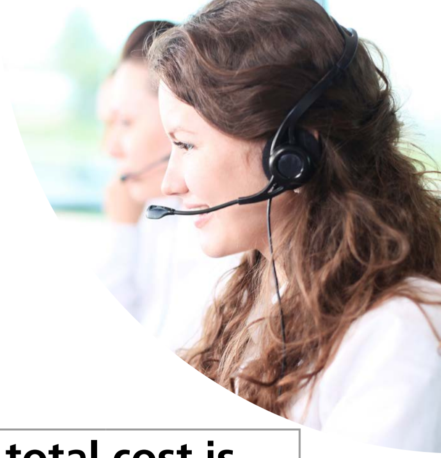
The method you use to achieve these goals is up to you. But worryingly, some companies may believe they are secure, compliant and cost effective — only to discover they were wrong when there's a data breach or they fail an audit. Why? Because they didn't ask critical questions early on.

Choosing the right PCI DSS solution … with your eyes open

Dozens of companies promise to provide PCI DSS security for contact centres. They may pitch for exactly the same contract and say almost identical things — but the offering is very different.

Here are 5 solutions you're likely to come across:

Once you lift the lid and look closely, the outcomes can be radically different …



Solution type and what's secured						**Where the total cost is actually borne**		
	PBX-Telephony	Database	Applications/ CRM	Call Recordings	Contact Centre Agents	Price of solution	Work left for you	Overall value
#1 Pause & Resume during call	✗	✗	✗	✓	✓	↓	😬	👎
#2 Mid Call - agent asks caller to key in numbers	✗	✓	✗	✓	✓	↓	😬	👎
#3 Appliance at desktop and call recorder	✗	✓	✗	✓	✓	→	🙄	👉
#4 Appliance within your data centre	✗	✓	✓	✓	✓	→	🙄	👍
#5 De-scoping using hosted DTMF solution	✓	✓	✓	✓	✓	↑	😂	👍👍

Eckoh

What are we being sold — de-scoping or de-risking?

On closer examination, what becomes clear is that solutions #1-4 are actually de-risking, not descoping.

You could be left with some serious costs, and work to complete, that will include putting a series of expensive mitigating measures in place that you then need to manage. These may include overseeing 'clean rooms', expert vetting of employees, extra system security, and energy-sapping complications every time your technology changes. It all adds up to extra time, cost, hassle and continuing risk.

If you joined your organisation to spend much of your time managing an intensive security operation, then fair enough. But few people signed up for this. It's a huge and never-ending task, fraught with problems.

In contrast, only a hosted DTMF solution provides true descoping. Here, all sensitive data goes directly to a trusted third -party provider, such as Eckoh, who manages the majority of PCI DSS compliance on your behalf. And with no card holder data at all within your contact centre environment, there's nothing for anyone to steal. Simple.

Should you choose de-risking or de-scoping?

If you want more time to focus on your customers, get greater peace of mind, and get the certainty of predictable costs, then only a hosted DTMF solution will do.

Discover more

To find out more download our handy eGuide 'The Definitive Guide to PCI DSS Compliance for Contact Centres' for all the answers in one place.

Eckoh

A jargon-free guide to compliance for forward thinking organisations

The Definitive Guide to...
PCI DSS Compliance

Alternatively, if you'd like to talk to us about Secure Payment solutions or PCI DSS compliance just drop us an email tellmemore@eckoh.com or simply call 08000 630 730.

[1] National Audit Office