Eckoh

What your de-scoping vendor fixed.

What they missed.

What threats are hiding under the surface of your PCI DSS strategy?

Titanic differences in de-scoping vendors.

It's easy to spot the iceberg floating in the ocean. But it's impossible to know just how massive it is without diving deep into the water.

The same can be said for new vendors entering the PCI DSS market. They may offer to secure your payments and give you broad promises about de-scoping, but their solutions only tackle surface-level threats and often rely on compensating controls. And that's just the tip of the iceberg. The real dangers to your contact centre lurk deep beneath the surface, in the areas most vendors are incapable of protecting.

In other words, you paid for de-scoping, but got stuck with de-risking.

The dangers of de-risking.

By using a de-risking strategy for the sake of PCI DSS compliance, which often includes a number of compensating controls, you allow data to continue to flow through crucial parts of your contact centre.

Only by completely removing the data from your environment (deep de-scoping) can you be sure that your contact centre is as safe as possible.

The difference between de-risking and de-scoping can have significant cost implications for merchants. These implications aren't always clear when you choose an approach.

On average, UK contact centres use three different PCI DSS solutions to maintain compliance.

A multi-solution approach offers some form of de-risking, but not fully de-scoping. You might be investing time, money and effort on an unreliable system that still leaves you exposed. These ineffective solutions include:

- **Pause and resume**
- **Mid-call**
- **Appliance at the desktop and call recorder**
- **Appliance within your data centre**

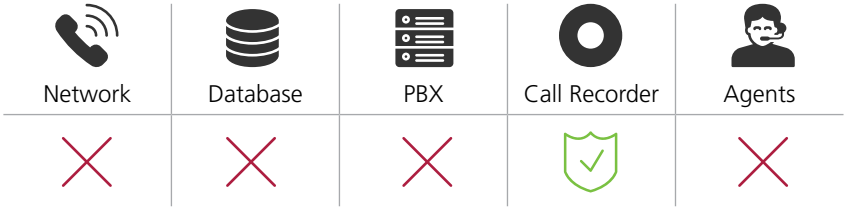
Discover the risks of each.

Pause and resume.

How it can capsize your system.

Pause and resume presents several risks to your call recording system. For example:

- Agents can still hear card details being read aloud and could choose to copy them down
- Agents can pause the recording and have an unmonitored conversation with the caller in secret
- Agents can simply forget to pause and accidentally record sensitive card data
- Your PBX, applications, CRM and agents are still in scope.



What is it?

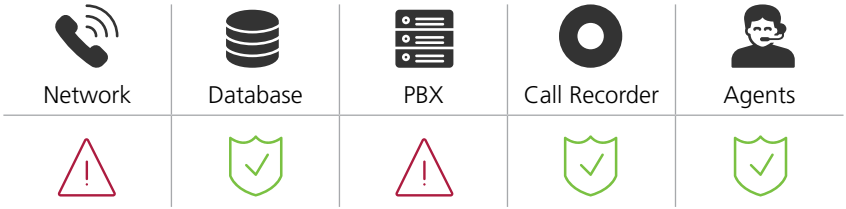
Pause and resume is when the agent manually pauses the call recording system while the customer reads their credit card information aloud over the phone, then resumes recording afterward.

Mid-call.

The collision of timing and human error.

With just a mid-call solution, you're prone to problems such as:

- Calls that are only directed through the DTMF masking service at the time of payment, so the PBX database and telephony network are still in PCI DSS compliance scope
- Agent is responsible for beginning the DTMF masking process.



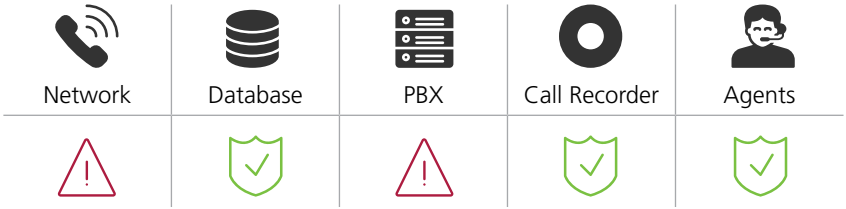
What is it?

A mid-call solution relies on the agent to turn on a DTMF masking service at the time of payment on a call. Once initiated, the customer can securely enter their credit card information using their phone keypad. The agent can still see payment progress indicators on screen, but not the actual card number. The entire call can be recorded, but payment data is not stored in your database.

Appliance at the desktop and call recorder.

The problems with appliance at the desktop and call recorder.

- DTMF needs to get to the agent's phone to be entered into the payment form
- The card details are present in the agent's PC, telephony and networks
- Sensitive data is exposed and open to fraud in a number of ways
- Requires other controls to achieve PCI DSS compliant.



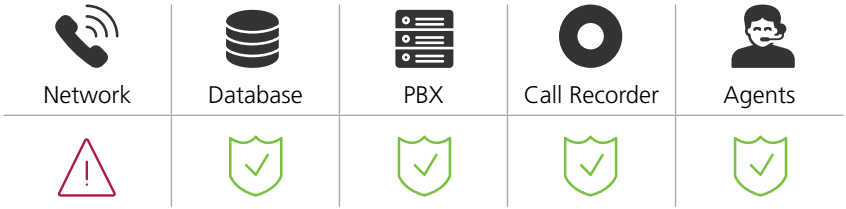
What is it?

Data is screened locally – at the agent's workstation or desktop, and at the call recording devices. It relies on the caller/customer entering their card data using DTMF key-presses on their phone keypad.

Appliance within your data centre.

The problems with appliance within your data centre.

- You're still bringing card data into your environment
- You are still open to fraud and data breaches
- Even if using a third party contact centre - you are still responsible.



What is it?

This involves moving the DTMF masking to a comms room or data centre, removing the DTMF from your environment so you avoid it reaching your agents. DTMF must be verified and processed by an appliance and progress indicators sent to the agent so they can follow data entry.

Don’t let de-risking sink your contact centre.

There’s only one solution that truly de-scopes the contact centre environment from the scope of PCI DSS compliance. You need a hosted DTMF solution like CallGuard from Eckoh to check all the boxes and consistently protect customer credit card data.

	Network	Database	PBX	Call Recorder	Agents
Pause & resume	⚠	⚠	⚠	✓	⚠
Mid-call	⚠	✓	⚠	✓	✓
Appliance at desktop and call recorder	⚠	✓	⚠	✓	✓
Appliance within your data centre	⚠	✓	✓	✓	✓
De-scoping using CallGuard	✓	✓	✓	✓	✓

It’s not just voice calls.

There are many new ways to pay, like chat and other channels. Remember that customers expect security from whichever payment channel they choose.

The CallGuard experience.

Card Data Input

When the customer is ready to make a payment over the phone, the agent simply asks them to enter their payment card data on their phone keypad.

Agent Experience

The agent NEVER hears the DTMF tones, or sees a card number or CVV. In addition, no card data will be captured on screen, in call recordings or enter any part of your network.

Customer Experience

The customer and agent are in constant contact throughout the call, making for a great customer experience and reduced handling time.

Future Proof

CallGuard doesn't tie your hands to any existing systems or payment processes. You're free to make changes at any time.

Light Touch

Eckoh does all of the heavy lifting, greatly reducing the burden on your IT staff. There are no APIs to write to and no integration necessary with existing systems.

Secure

Not only are you compliant, more importantly, you're secure because the card data never enters your environment.

Go with CallGuard and ensure your contact centre stays afloat.

Call 08000 630 730, email tellmemore@eckoh.com
or visit www.eckoh.com to learn more.