



Tackle fraud by removing card holder data from call recordings and agent screens.

Why CallGuard On-Site?

- PCI DSS compliance from technology that's straightforward
- Simple to install, no time consuming integration
- No changes needed to call recording or phone systems, CRM platform, payment processes or provider
- Agent remains on the call and can speak to the caller throughout the entire process.

Contact center fraud and PCI compliance have been extensively covered in the media over the last few years.

Criminal gangs look for weaknesses in any payment acceptance and storage process - including payments taken over the phone by call center agents. Most call recordings store this data, which raises a whole host of security issues, especially in the eyes of the Payment Card Industry.

So how do you prevent the use of credit card data in recorded calls whilst retaining the benefits of your premised call recording system?

Part of the Secure Payments Suite, CallGuard On-Site eliminates sensitive card data from telephone conversations before they are recorded. It can also prevent your agents from seeing any card data on screen, which eliminates the potential for card data theft.

CallGuard is straightforward to explain, easy to implement and simple to use. It allows any organization using a premised call recording system to continue to do so without any implications to PCI DSS. So, everything stays running as normal.



How it works

At the heart of CallGuard On-Site are three components: the Filter, the ToneDevice and DataShield. Together, they allow your customers to relay payment card details using their telephone keypad, while continuing to talk with the agent throughout the call.

The Filter automatically detects and takes out the DTMF tones. This happens as the customer enters their card number using their phone keypad and before the call is captured by your call recording system. At the same time the ToneDevice detects the DTMF tones, and encrypts them into a

string which it types into the agent screen as if it was a keyboard.

DataShield, the third element, takes this encrypted string, decrypts it, and enters the card data into the payment page. DataShield obscures the card data with '****' asterisks and the agent cannot copy or paste the information. The caller has effectively typed their own card details securely into the agents screen. Payment data cannot be viewed, copied or compromised in any way, either in the payment application or elsewhere.

Extent of PCI DSS De-Scoping



CallGuard On-Site removes the following from PCI DSS scope:

- Call Recording
- Screen Recording
- Agents

CallGuard On-Site process

