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

Why CallGuard On-Site?

- A major step to PCI DSS compliance from technology that's straightforward
- Payment is PCI DSS compliant
- 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 centre fraud and PCI DSS 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 centre 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 presence of payment card data in recorded calls whilst retaining the benefits of your premised call recording system?

Part of Eckoh's 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, or hearing any card details, which minimises the potential for card data theft.

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

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

pci WINNER Awards for Excellence 2019
2019, 2018 & 2017

PAYMENTS AWARDS 2017 SHORTLISTED

Retail Systems awards 2016 WINNER

FStech awards 2018 SHORTLISTED

CREDIT & COLLECTIONS TECHNOLOGY AWARDS 2018 FINALIST

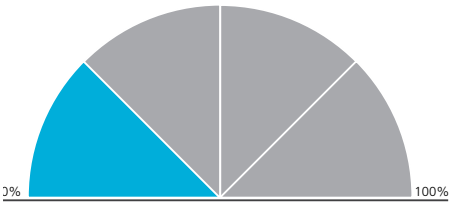
How it works

At the heart of CallGuard On-Site are three components: the Filter, the ToneDevice and DataShield. Together, they allow your customers to enter 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 agent's 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

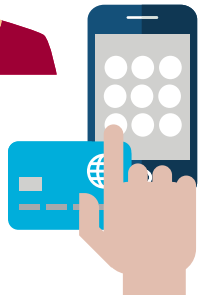


CallGuard On-Site removes the following from PCI DSS scope:

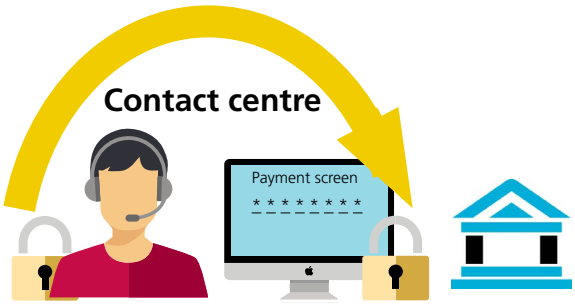
- Call Recording
- Screen Recording
- Agents

CallGuard On-Site process

1 Caller rings the contact centre to make a purchase.



2 Using their telephone keypad, the caller types card data which is captured by CallGuard.



3 CallGuard instantly replaces the actual card data with asterisks which are automatically entered into the payment screen. Agent sees no data.

4 Asterisks are converted back to real card data and sent to Payment Service Provider. Agent is notified of payment approval or rejection.

Our solutions are delivered via the Eckoh Experience Portal.
Works well with ChatGuard and Chatbot