CIVICA

# Civica MidCall

## Safe, compliant payments by phone - no matter where your agents are.

How can your organisation stay PCI DSS compliant if your agents aren't based in the office? MidCall, powered by payment security experts PCI Pal, helps protect you and your customers against fraud. Phone payments are collected safely and efficiently, even when staff are working remotely.

### What is MidCall?

With MidCall, the agent doesn't hear or see customer card details, but maintains contact throughout the call. Not only does this make the call PCI DSS compliant, it helps encourage customers to complete the payment.

### Complying with PCI DSS

Most organisations have a large number of operators spread over the council network – or working remotely – who need to take payments over the phone. Without any form of secure ATP system, these telephone payments can bring the council's network and agents into scope for PCI DSS for the following reasons:

- By hearing them, agents are by default exposed to the debit/credit card details
- Networked workstations and laptops used to input the card details bring the PC, local environment and connected network into scope
- Many councils use VoIP calls which are not encrypted. This means that card details can be passed unencrypted across the council's internal network. One call brings the entire internal network into scope for PCI DSS

### How does MidCall work?

1. A citizen contacts the council by telephone to make a payment.

2. The agent uses Civica Income Management to enter the transaction details. When payment is required, the agent opens MidCall to secure the call.

3. When prompted the citizen enters their card details using their telephone keypad.

4. Asterisks are displayed to the agent with card details validated in real time. Card data does not reach the agent or their environment.

5. The agent and customer remain on the call throughout the process, so help can be given if required.

6. The agent hits the 'process card' button, which completes the transaction.

This process means that the card details are never exposed to the agent, and the payment data is stored at our PCI DSS Level One secure data processing centre - protecting both the council and customer from risk of fraud.

### Key benefits:

- Agents are not exposed to card numbers and details, de-scoping them from PCI DSS considerations.
- The council internal network does not carry or transmit card data either from the workstation processing for transaction or from VoIP telephone call, thus de-scoping the council's network from PCI DSS.
- MidCall allows agents to collect secure payments while working remotely.
- Any member of staff can potentially take a card payment over the phone without PCI DSS repercussions.
- Maintaining a voice call with the citizen allows the agent to support the caller, encouraging payment and avoiding incomplete transactions.

# £556.3m

was lost to UK credit, debit and other payment card fraud in 2022.