Zoom Contact Center
Speak to Pay

Contents

1   Introduction

1.1   Zoom

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. Founded in 2011, Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Zoom is headquartered in San Jose, California.

This solution is in partnership with PCI Pal, enabling companies to take payments from their customers over the phone.

This document will take the company Agent through the payment journey with their customers focusing Speech Recognition to enter in their card details.

2   Zoom Contact Center – PCI Pal Speech Recognition

In order to be able to take payments via the Speak to Pay Payment Journey, you will need to be on an engagement with your customer via Voice (Phone Call)

2.1   Application Details

Once the App has been installed for each company Agent, the PCI Pal App is shown on the right hand side of the Zoom client.
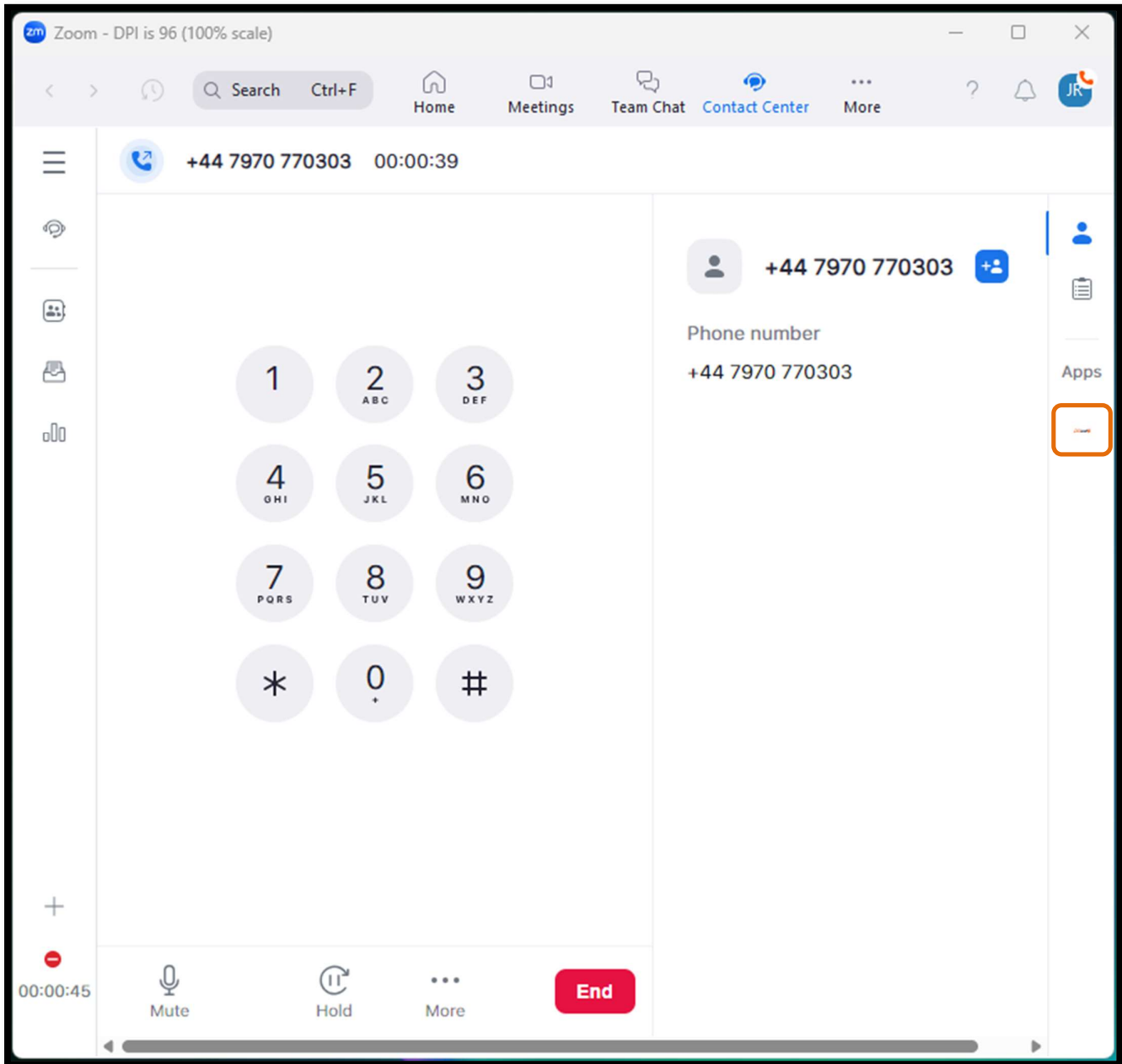
3   Speech Payment Journey

The Company Agent will be talking to their consumer via an inbound or outbound phone call.

The Agent will call or answer as normal, and go through any standard company processes.

During the call, the Agent will determine that a payment is required.

3.1   Launching the Zoom App – Authentication

When the Agent has determined that a payment from the Customer on the call is required, they will launch the PCI Pal App from within their Zoom Phone Client on their Computer.

1.   The Agent will need to click on the 'Launch' button to trigger the payment collection.
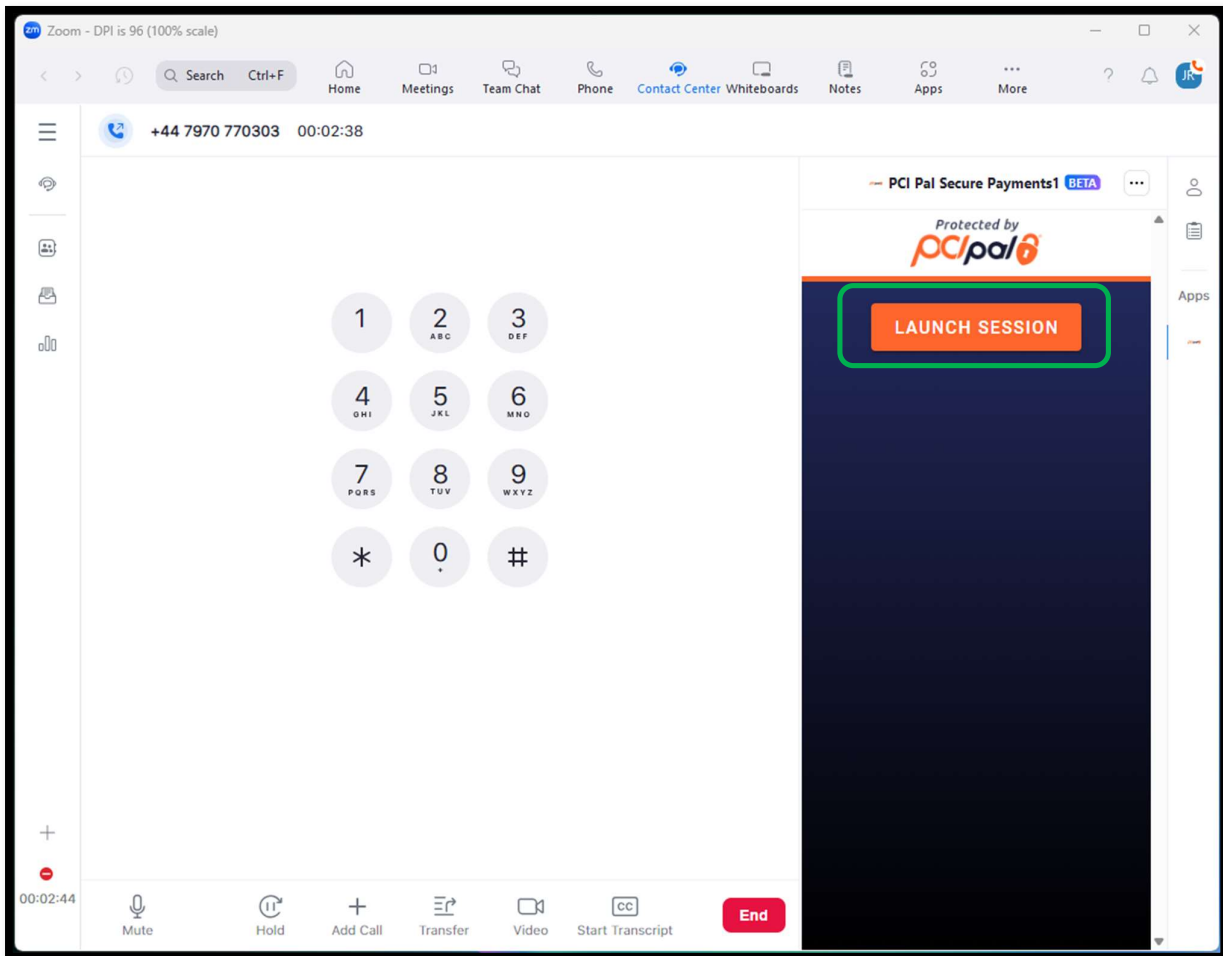
3.2   Splash Page

The Agent will be provided with up to 3 payment journey choices from a Splash Page.
- Key to Pay – Customer pay by card using their phone keypad
- Click to Pay – Customers will pay by card via a live payment link
- Speak to Pay– Customers pay by card speaking their card details

The choices shown will be determined by the order placed via Zoom for the PCI Pal Payments solution.

For the purposes of this document, the Agent will choose Speak to Pay

2. The Agent will select 'Speak to Pay'.
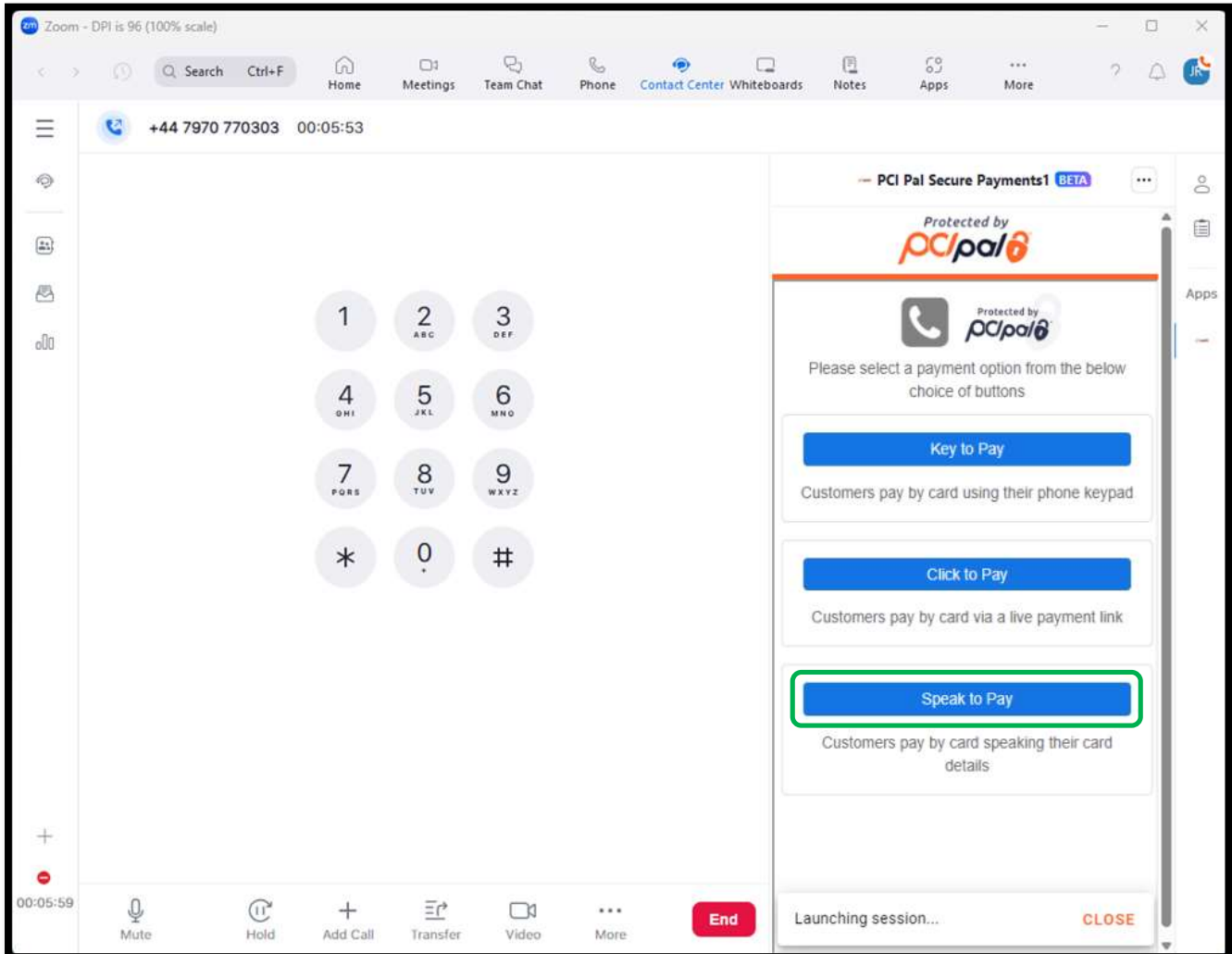
3.3   Order Data Capture

i.   Secured Call

After selecting Speak to Pay, PCI Pal and Zoom will be securing the call in the background. Providing the session is secured successfully the icons at the top of the app will change.
The Phone icon will go green, and the PCI Pal logo will go orange.

Unsecure: Secure:
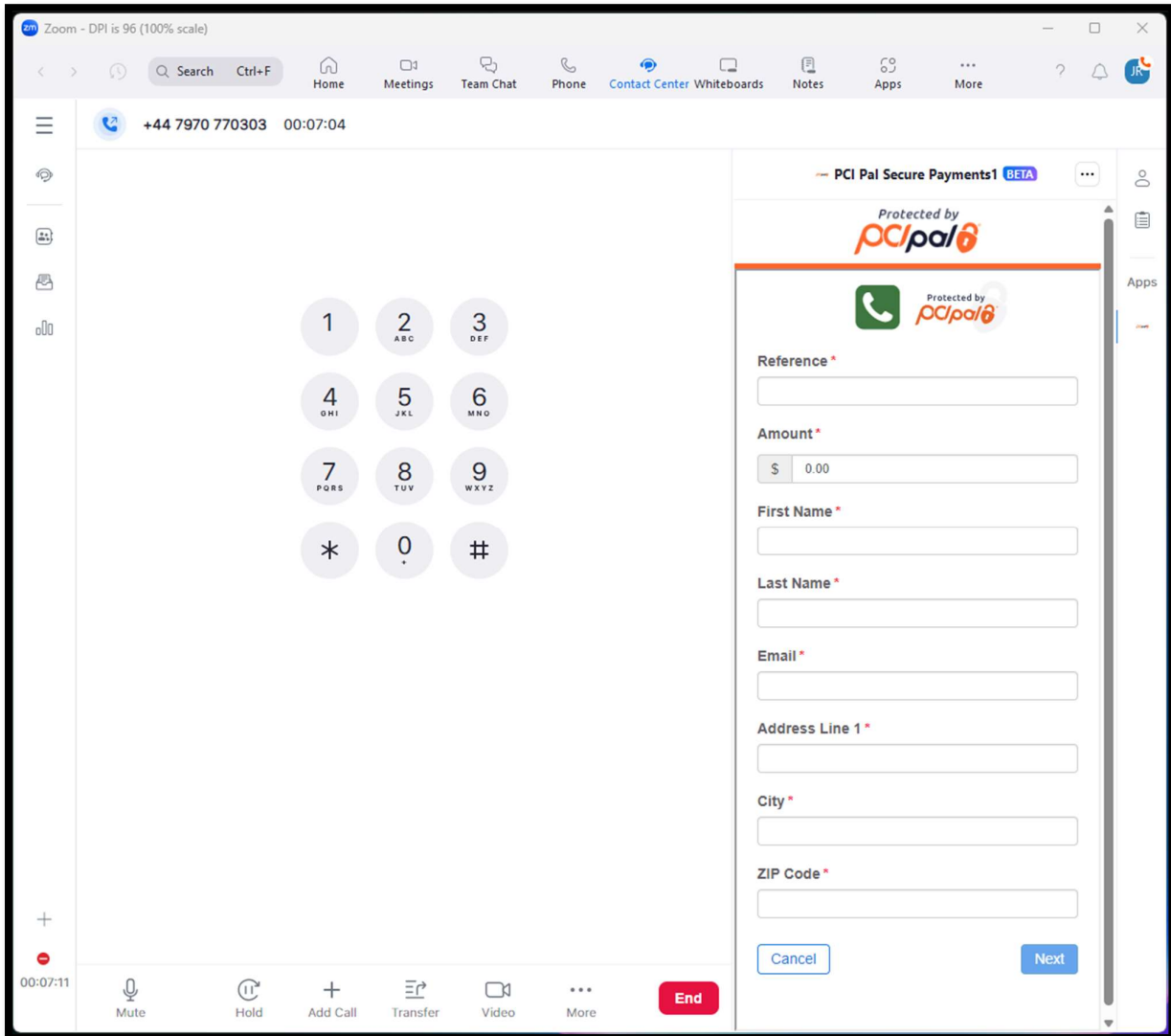

ii.   Order Details

The Agent will also progress to the Order Details page.

Below is an *example* of the Order Details page the Agent will need to manually populate for each payment.
The fields for completion will differ for each company. This will be confirmed during the PCI Pal Onboarding project.

Data entered;

3.4 Card Collection

iii. Card Collection - PAN

After clicking 'Next' they will proceed to the Card Collection Page.
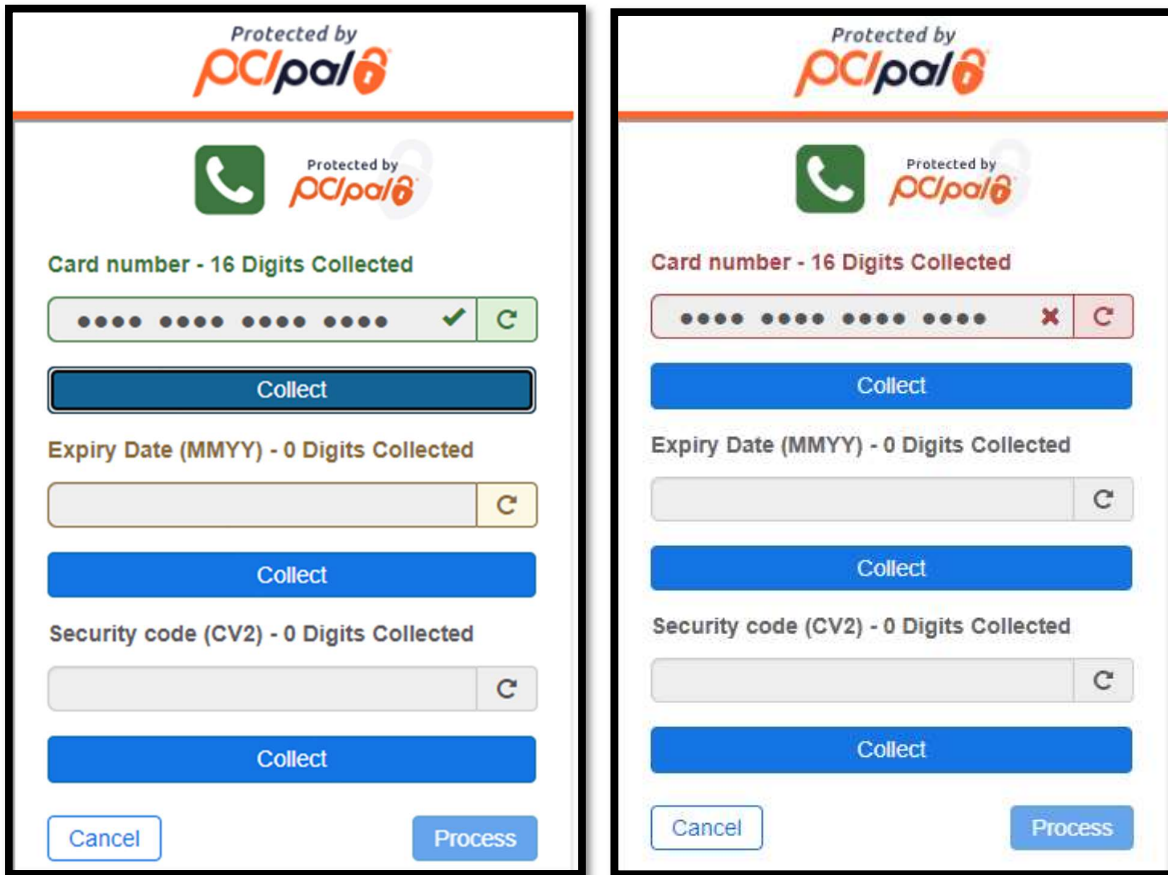With the 'Card Number' enabled in gold.
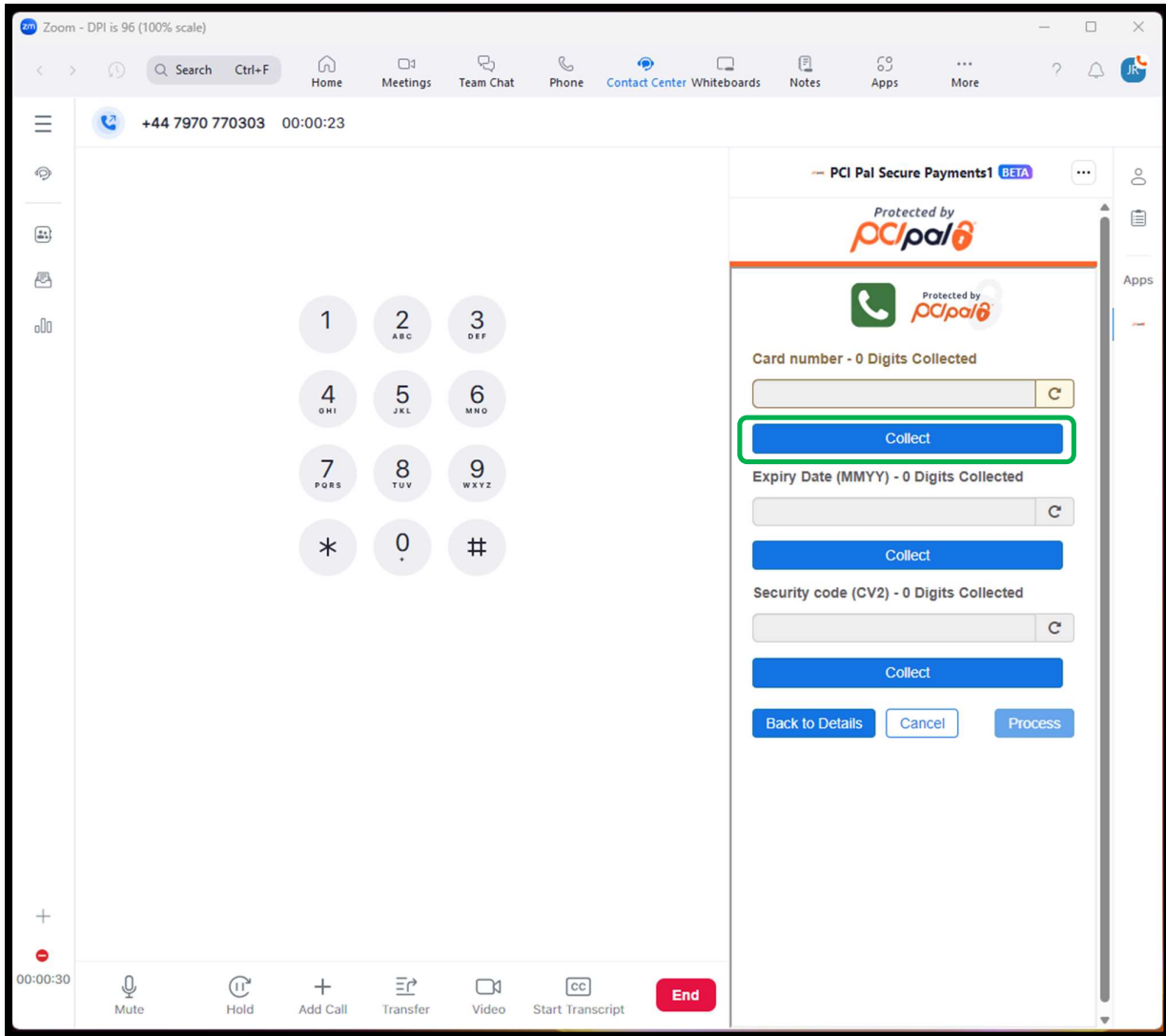
The Agent will ask click the Collect button. At which point the Agent and Customer are muted from one another. The system will then ask the Customer to read out their long card number via their phone keypad.

During this the Agent will not be able to hear the data entry, however they will see dots in place of the card numbers on the screen.

Once complete with the 16-digits (15-digits for AMEX) the user interface will show a Green "valid" tick and can show you the non-compliant data (Specific to each Customer's settings).

If the Card details are invalid, the user interface will show you a Red 'invalid' cross.

To be classed as a Valid card, it will pass the BIN Check and the Luhn Check.

If the field is not showing as valid after 16-digits has been entered, or is showing the red cross, the Agent can click the 'Card Number' bar or refresh icon to reset and ask the Customer to try again.

This button can be pressed at any time. Meaning if the Customer mentions they entered an incorrect digit, the Agent can clear the field and allow them to start again.

iv. Card Collection - Expiry

Once the details are correct, the solution will automatically enable the Expiry field. Should this not happen, the Agent can click the 'Expiry' bar to enable.

The Agent will click the 'Collect' button. At which point the Agent and Customer are muted from one another. The system will then ask the Customer to read out their expiry in the 4-digit format as shown on the card (MMYY).

As before, during this the Agent will not be able to hear the data entry, however they will see dots in place of the card numbers on the screen.

The system will either show a Green "valid" tick or a Red 'invalid' cross. The Agent again can re-set the relevant field by clicking on the bar or refresh icon.

As long as this is a date in the future this will be valid. If in the past, it will be invalid. The Payment Gateway trigger the checks to ensure the date is correct for that specific card.
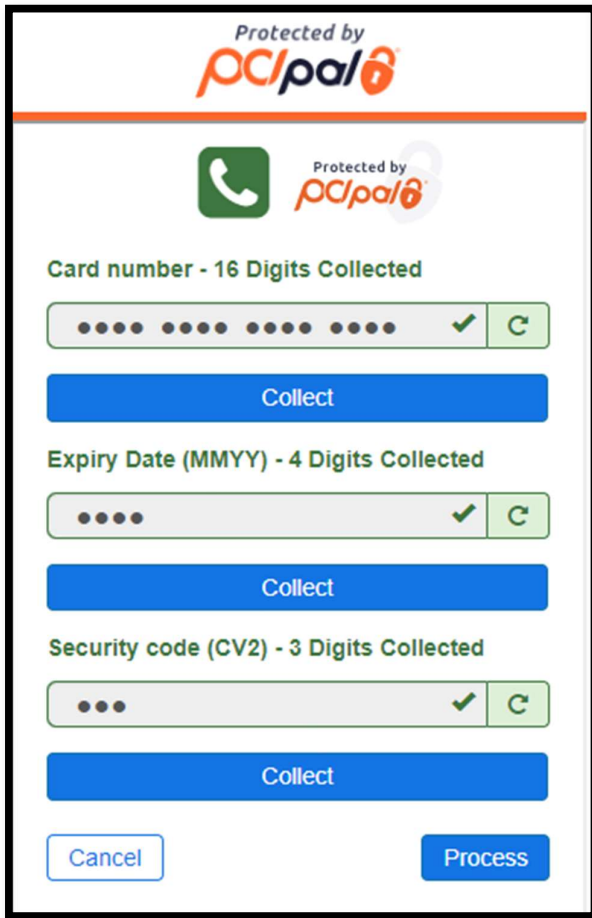
v. Card Collection - CVV

Once the details are correct, the solution will automatically enable the 'Card Security Code' field (CVV). Should this not happen, the Agent can click the 'Card Security Code' bar to enable.

The Agent will click the 'Collect' button. At which point the Agent and Customer are muted from one another. The system will then ask the Customer to read out their 3-digit digit security code (4-digit for Amex) from the card.

As before, during this the Agent will not be able to hear the data entry, however they will see dots in place of the card numbers on the screen.

This will always succeed, as the verification is done by the Payment Provider at the next stage.

3.5   Payment Process

Once all the card collection fields are complete, the call is un-muted from one another and the Agent will need to click on the 'Process' button.

PCI Pal encrypts the data and securely sends this to the Company's Payment Gateway. The Payment Gateway also encrypt this and send the details to the Acquiring Bank linked to the account (for example Stripe).

The Acquiring Bank forwards the data to the Issuing Bank (the End Customer's bank, for example Chase) for Verification and Authorisation.

During this process the various Banks are running through all of their checks. This may include some of the following:
- Address Verification
- Fraud Checking
- Confirm PAN, Expiry and CVV are correct for that card
- Confirm that the Name is correct for the card
- Does the End Customer have enough funds for the transaction

Once all of these processes are complete, the results of the transaction are sent back up the chain to PCI Pal.

PCI Pal will display the results to the Agent in the UI. This will include whether or not the transaction was successful or failed/declined.
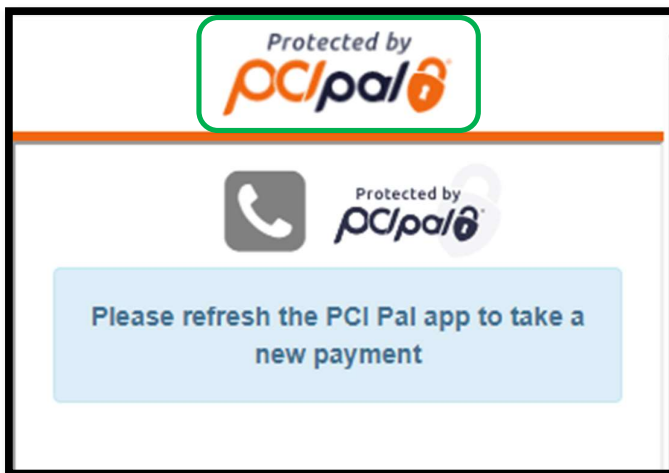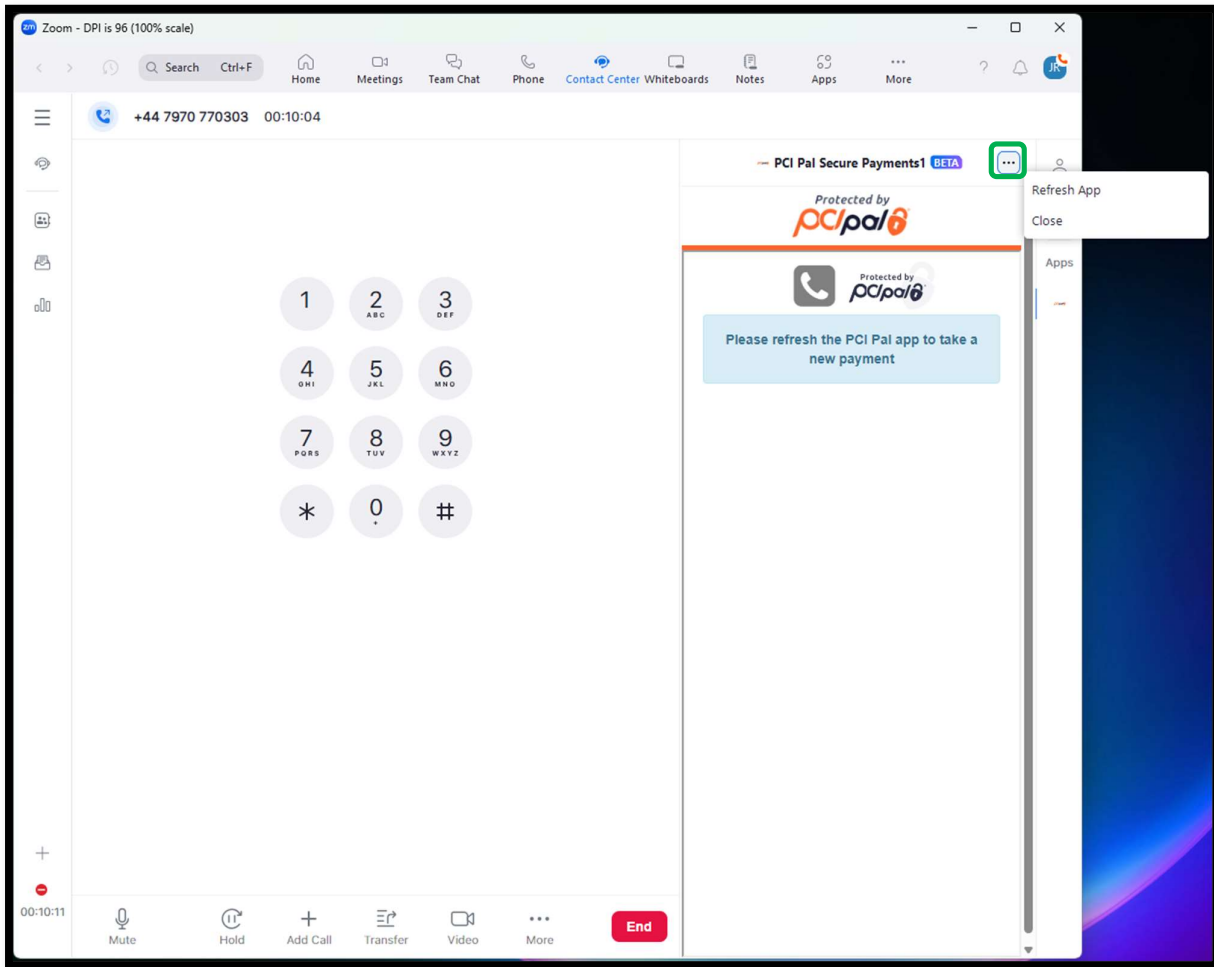
Connection with PCI Pal is complete.
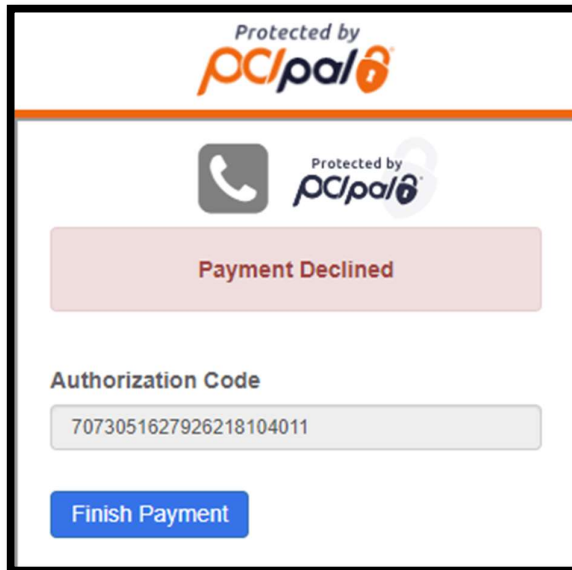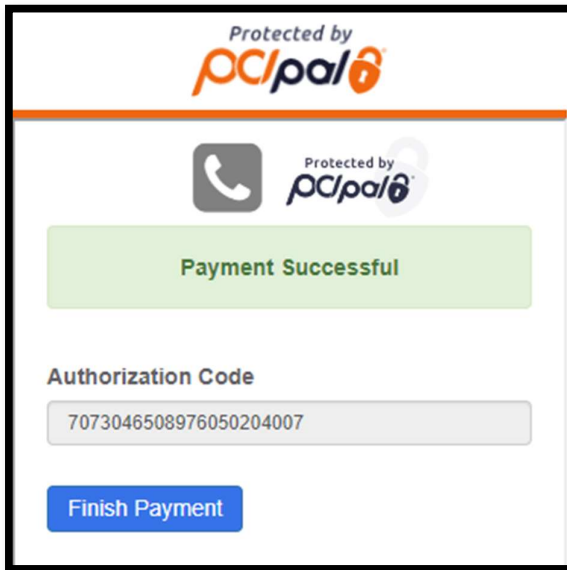
3.6   Closing session

The Agent will click the 'Finish Payment' button which will take them to the end of the payment process.

To refresh the app, the Agent can either click the 'Protect by PCI Pal' Logo at the very top of the app.
Or by clicking the […] button in the top right corner of the App window, and choosing 'Refresh App'

After the call has ended, ensure that you complete the engagement by adding any notes needed in accordance to your company processes and clicking 'Done'.

[End of Guide]

3.7   Troubleshooting & Support

vi.   Securing the Agent Assist call:

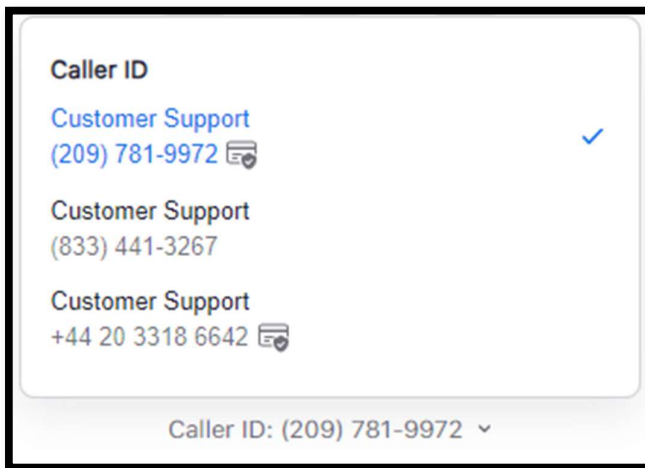Unlinked to PCI Pal:

Linked to PCI Pal & Secure:

Linked to PCI Pal, Call not secured:

If your line is not securing, ensure you are using a number enabled to Secure Calls
You are able to see this by clicking on the Caller ID Dropdown and viewing all numbers available. The lines that are enabled to secure calls are represented via the credit card icon.

If you are using a line that is enabled in securing calls, but the calls are still unable to secure, Zoom will need to investigate further.

vii.   Obtaining Session Information

When opening a support case, the team will need some specific information in regard to the PCI Pal element of the call. Please note that this needs to be collected by the Agent BEFORE closing the flow.
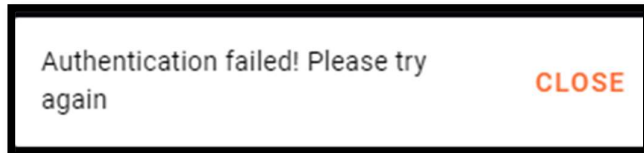The Agent will need to kick on the PCI Pal logo at the top

This will open up a popup. The Agent will need to copy and paste this data to the support team.
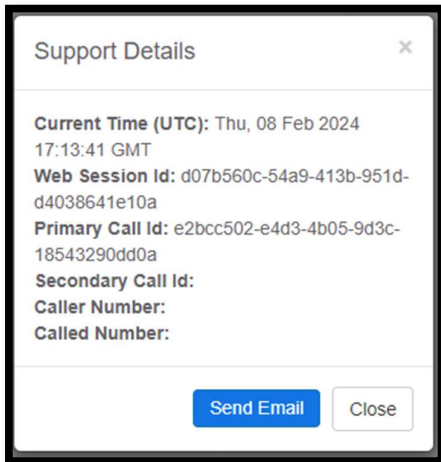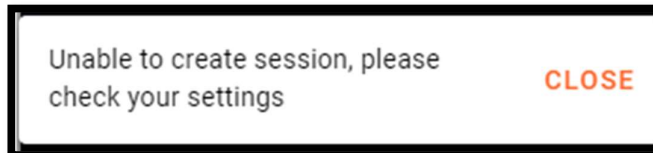
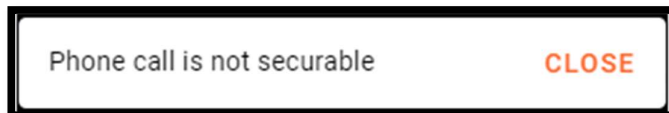*If unlinked not all data will be populated.*

viii. App Alerts

This alert will appear if the App is unable to confirm authentication of the settings set up by the Admin. The Launch button will not appear

This alert will appear if the app is unable to launch a session to take a payment
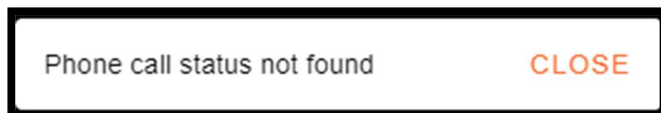

This alert will appear if the call is on a non-securable line. Zoom will need to investigate this.
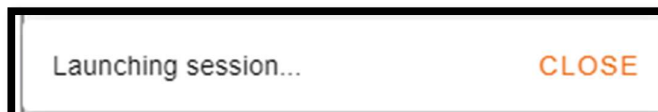
This alert appears at the bottom of the app when the Payment Journey is starting
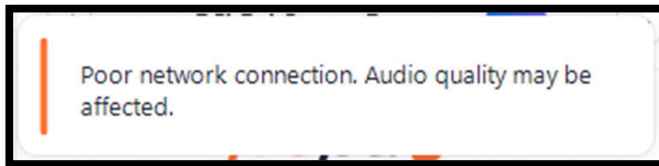

This alert appears at the bottom of the app when the call has been successfully secured


This alert appears when PCI Pal is un-sure whether the call is securable. The Agent will likely need to re-establish a new call, or take the payment via the Digital payment journey.

This alert appears at the top of the app when the call has been disconnected.
This is a Zoom alert.

This alert appears at the top of the app should Zoom believe the Agent's network to be weak or comprised during a call.
This is a Zoom alert.
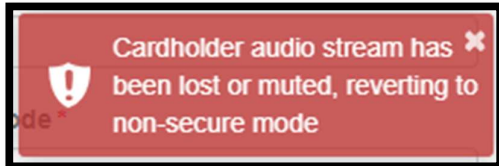
This alert will appear should the call be unable to keep secure. At the same time the Phone icon will go from Green to Red.
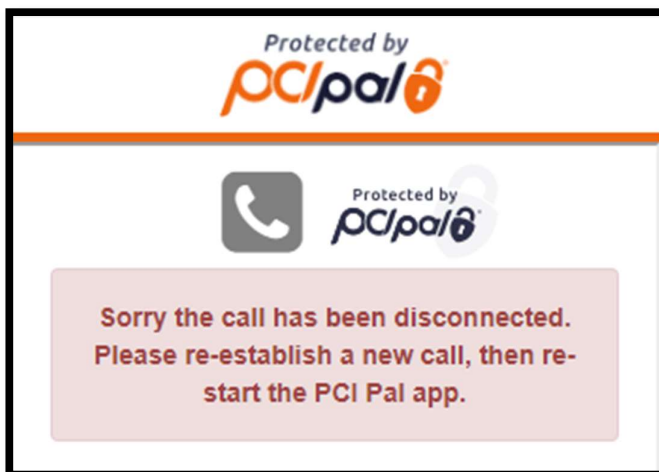

This alert will appear if the call was on a secure line, but unable to be secured successfully. It will re-attempt a few times. *The Session ID will differ for each call.*
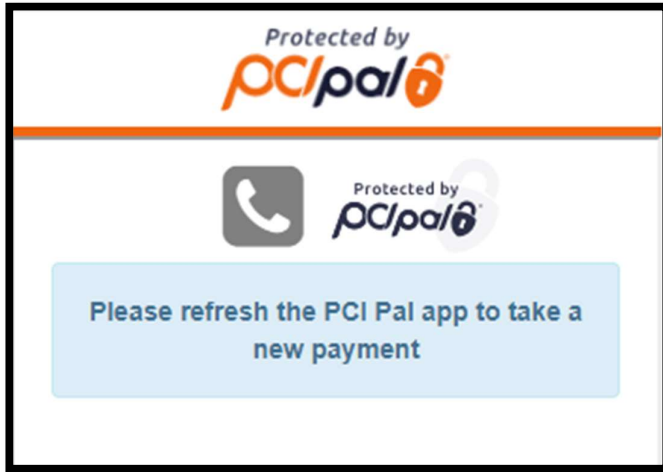
ix. Journey Alerts

This alert will appear whilst processing a payment. Showing the Agent that the payment gateway is reviewing the card data and deciding if the transaction is successful or not.

This alert will appear if the call has been disconnected before the full payment journey was completed.

This alert will appear at the end of a full payment journey. You are able to take additional payments from the same caller after this page, without the need to hang up the call.

[End of Document]