



Zoom Phone
Key to Pay

Contents

1	Introduction.....	2
1.1	Zoom.....	2
2	Zoom Phone – PCI Pal Agent Assist	3
2.1	Application Details.....	3
3	DTMF Payment Journey	5
3.1	Launching the Zoom App – Authentication	5
3.2	Splash Page	6
3.3	Order Data Capture	7
i.	Secured Call	7
ii.	Order Details	7
3.4	Card Collection	9
iii.	Card Collection - PAN.....	9
iv.	Card Collection - Expiry.....	10
v.	Card Collection - CVV	11
3.5	Payment Process	12
3.6	Closing session.....	12
3.7	Troubleshooting & Support.....	14
vi.	Securing the Pay By Phone call:	14
vii.	Obtaining Session Information	14
viii.	App Alerts:	14
ix.	Journey Alerts	15

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.

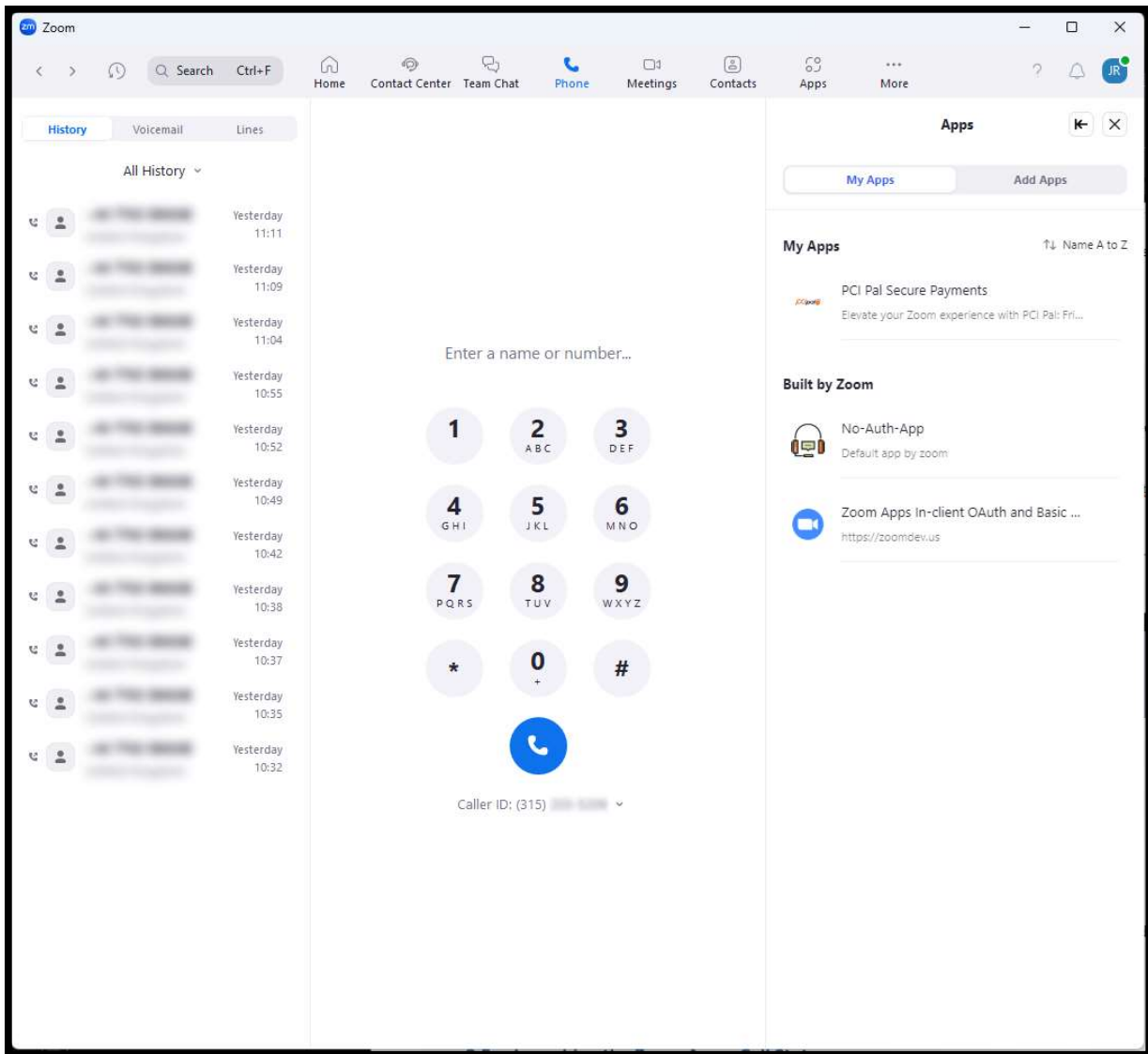
This solution is in partnership with PCI Pal, enabling companies to take payments from their customers over the phone.

This document will take the company Agent through the payment journey focusing on customers using DTMF (telephone keypad) to enter in their card details.

2 Zoom Phone – PCI Pal Agent Assist

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.



The screenshot displays the Zoom Phone interface. On the left, a 'History' sidebar shows a list of recent calls with timestamps ranging from 'Today 11:28' to 'Yesterday 10:32'. The main area features a dial pad with buttons for digits 1-9, *, 0, and #, along with a call button and a 'Caller ID: (315) [redacted]' dropdown. A 'PCI Pal Secure Payments' overlay is visible on the right, featuring the PCI Pal logo and a prominent orange 'LAUNCH SESSION' button.

3 DTMF Payment Journey

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

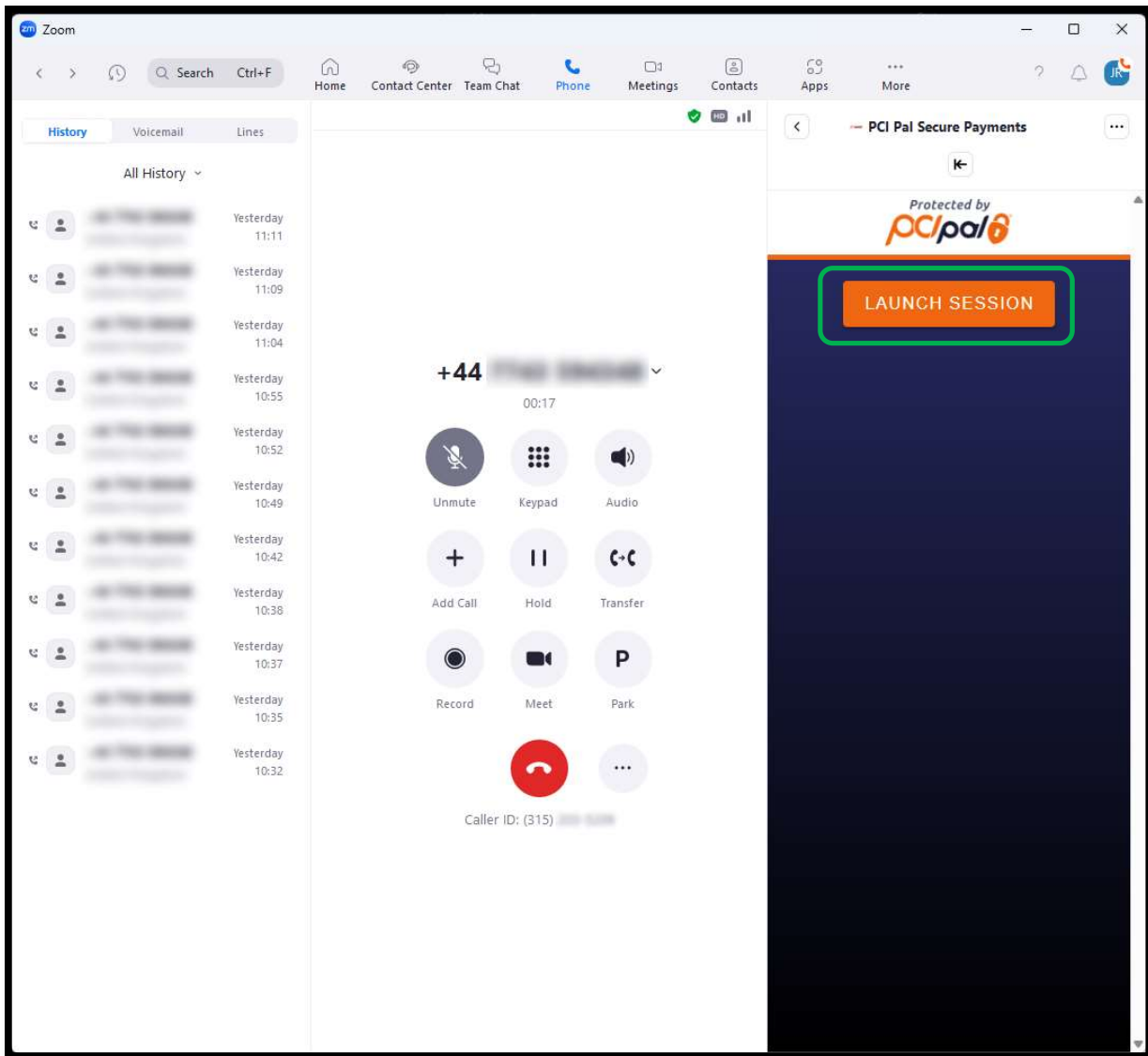
The Agent will call or answer as normal, and go through any standard company processes.

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 SESSION' button to trigger the payment collection.



3.2 Splash Page

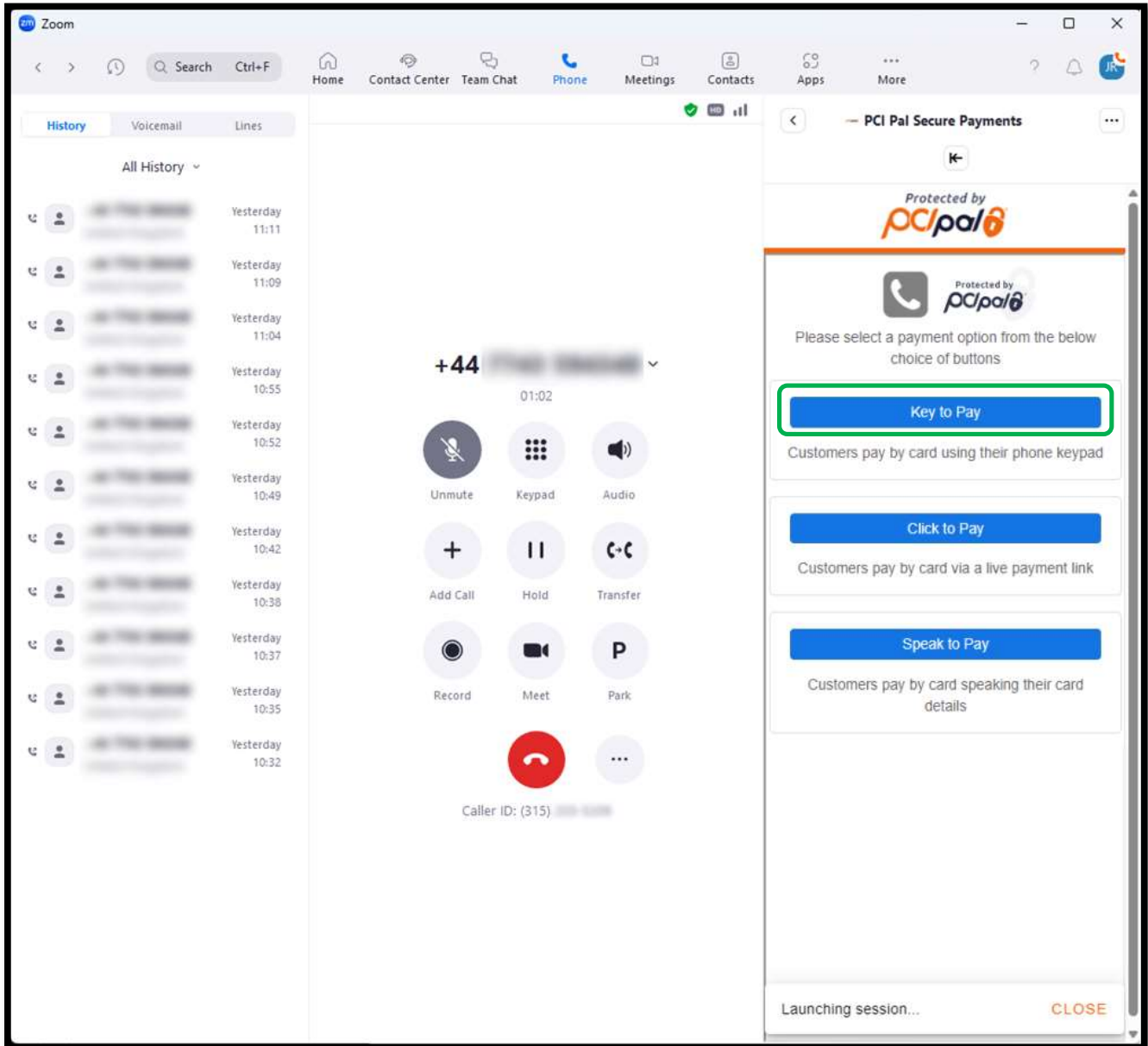
The Agent will be provided with up to 3 payment journey choices from a Splash Page.

- 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 Key to Pay

2. The Agent will select 'Key to Pay'.



3.3 Order Data Capture

i. Secured Call

After selecting Agent Assist, 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:

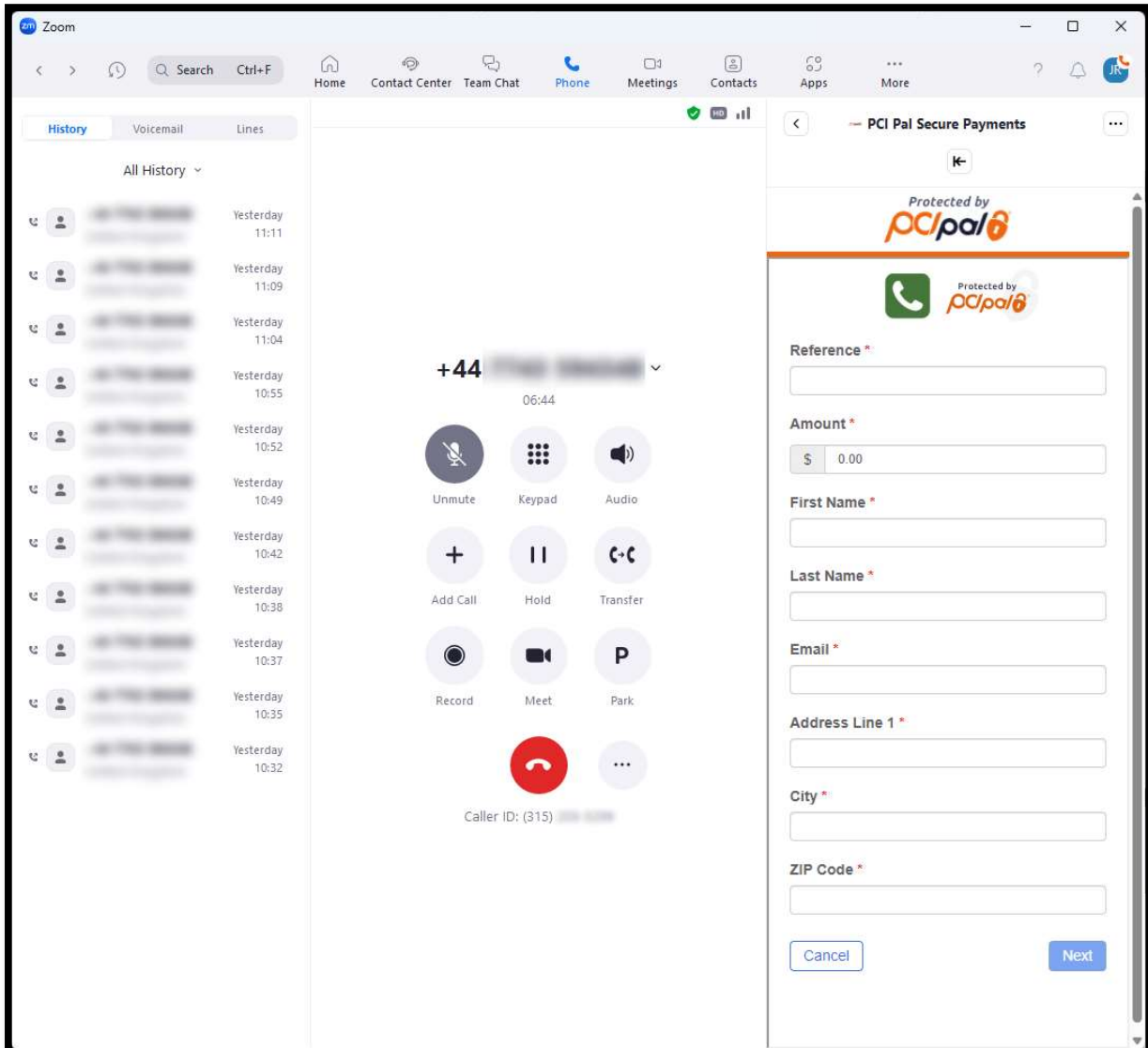


ii. Order Details

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;

The screenshot shows a Zoom desktop application window. On the left, there is a 'History' tab with a list of call records. The main area displays a call control panel for a call from a number starting with '+44'. The panel includes buttons for Unmute, Keypad, Audio, Add Call, Hold, Transfer, Record, Meet, Park, and a red end-call button. At the bottom of the panel, the caller ID is shown as '(315) [redacted]'. On the right, a 'PCI Pal Secure Payments' form is overlaid. The form is titled 'Protected by PCI Pal' and contains the following fields:

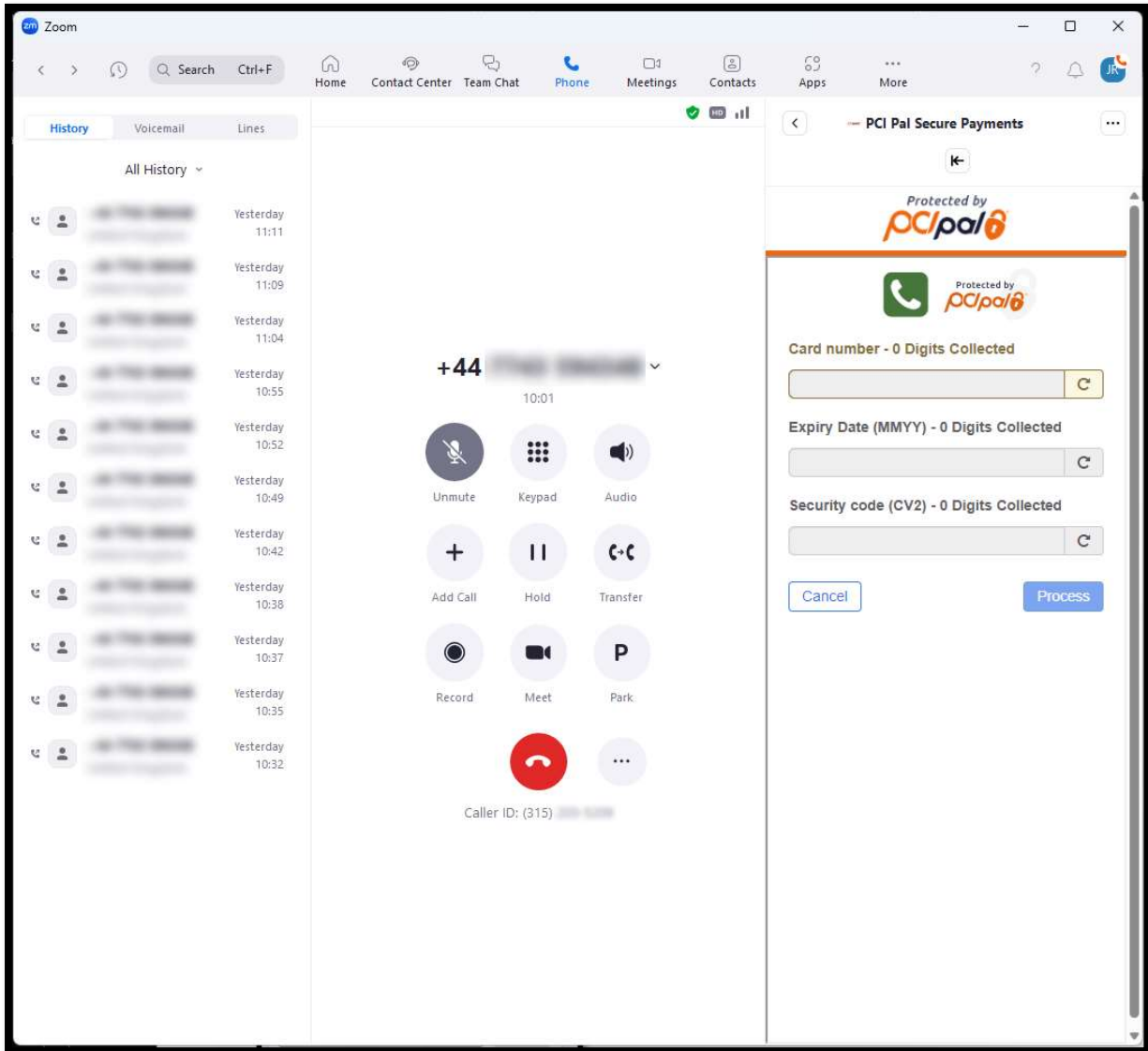
- Reference * (text input): ABC123
- Amount * (text input): \$ 55.00
- First Name * (text input): Joe
- Last Name * (text input): Bloggs
- Email * (text input): joe.bloggs@company.com
- Address Line 1 * (text input): 1 Main Road
- City * (text input): Suffolk
- ZIP Code * (text input): 90210

At the bottom of the form are 'Cancel' and 'Next' buttons.

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.



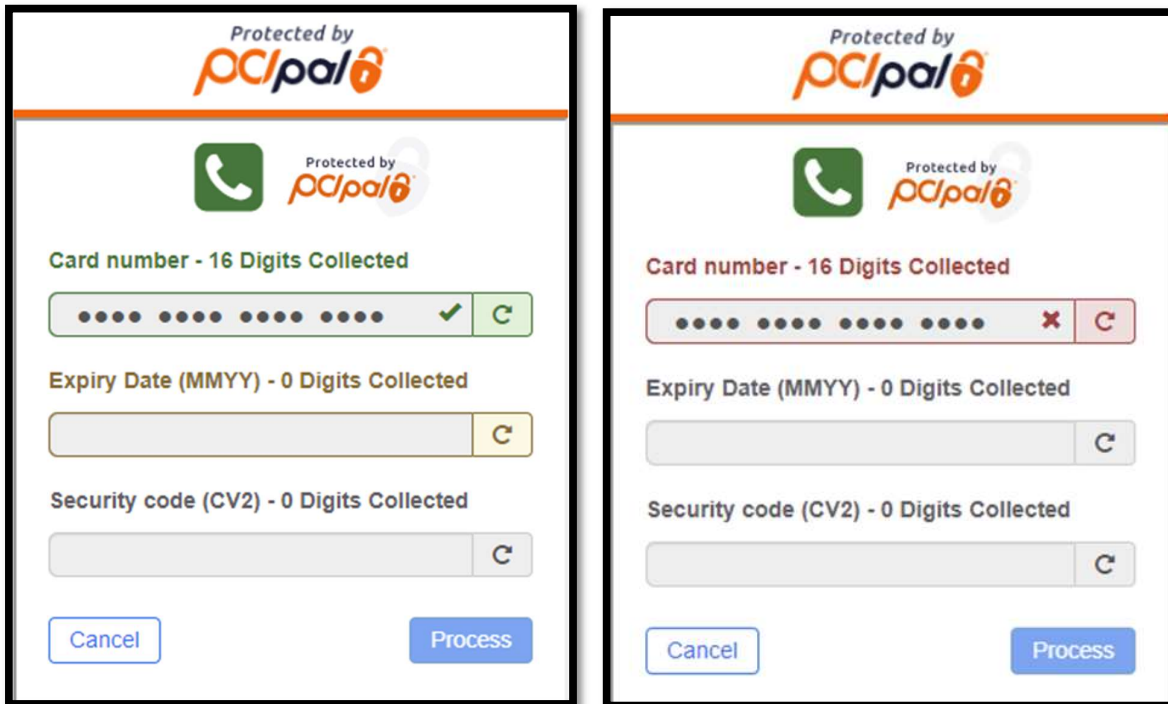
The Agent will ask the Customer to enter in their long card number via their phone keypad.

During this the Agent will hear a standard beep in place of the DTMF tone. The Agent will also see dots in place of the card numbers on the screen.

Once complete with the 16 digits 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 ask the Customer to enter the expiry in the 4-digit format as shown on the card (MMYY).

As before, during this process the Agent will hear mono-tone beeps, and see dots.

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.

Protected by **PCIpal**

Protected by **PCIpal**

Card number - 16 Digits Collected

..... ✓ C

Expiry Date (MMYY) - 4 Digits Collected

..... ✓ C

Security code (CV2) - 0 Digits Collected

..... C

Cancel Process

Protected by **PCIpal**

Protected by **PCIpal**

Card number - 16 Digits Collected

..... ✓ C

Expiry Date (MMYY) - 4 Digits Collected

..... ✗ C

Security code (CV2) - 0 Digits Collected

..... C

Cancel Process

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 ask the Customer to enter the 3-digit security code (4-digit for Amex) from the card.

As before, the Agent will hear a mono-tone beep, and see dots.

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

Protected by **PCIpal**

Protected by **PCIpal**

Card number - 16 Digits Collected

..... ✓ C

Expiry Date (MMYY) - 4 Digits Collected

..... ✓ C

Security code (CV2) - 3 Digits Collected

..... ✓ C

Cancel Process

3.5 Payment Process

Once all the card collection fields are complete, 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 encrypts this and sends 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.

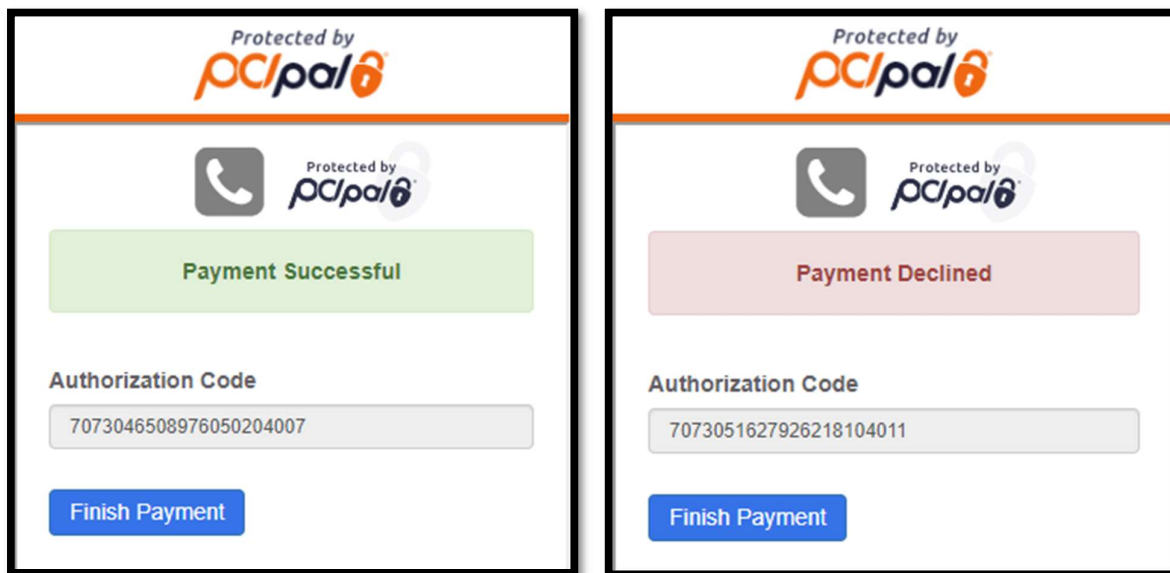
During this process the various Banks are running through all of their checks. This may include some of the following:

- 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.

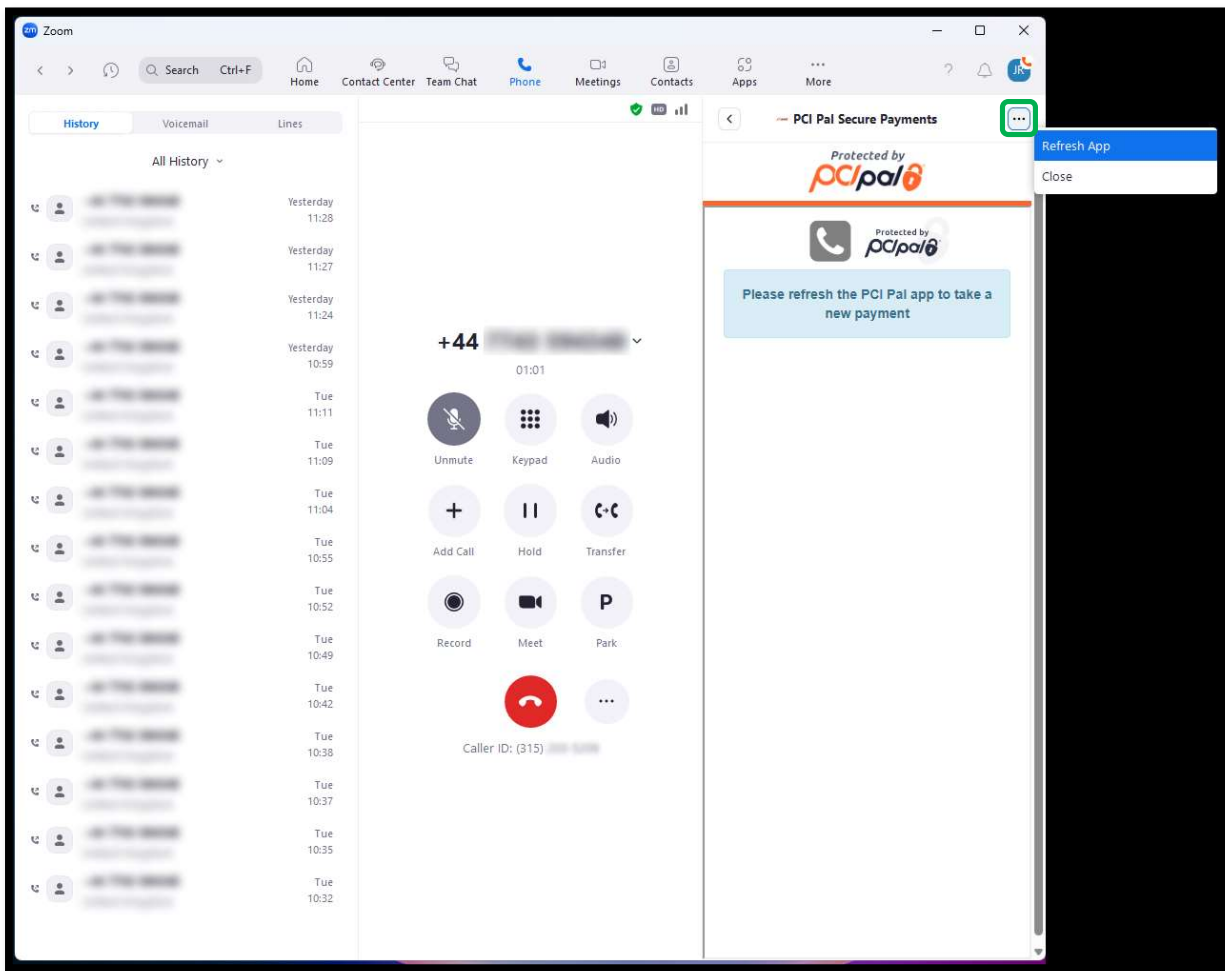
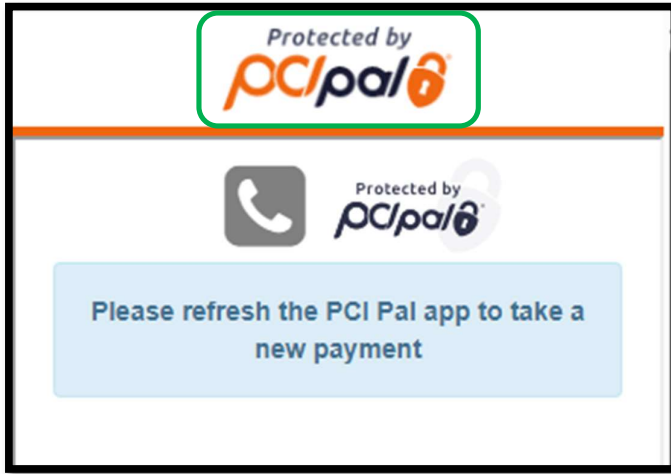
Connection with PCI Pal is complete.



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'



[End of Guide]

3.7 Troubleshooting & Support

vi. Securing the Pay By Phone call:

Unlinked to PCI Pal:



Linked to PCI Pal & Secure:



Linked to PCI Pal, Call not secured:



If your line is not securing, Zoom will need to investigate further.

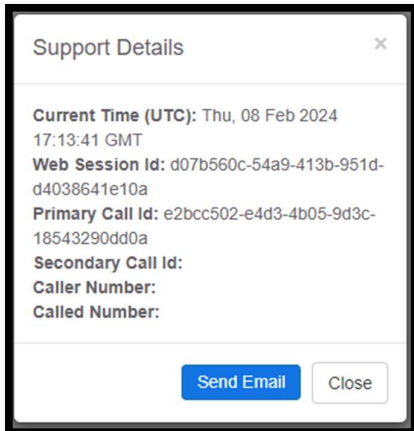
vii. Obtaining Session Information

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

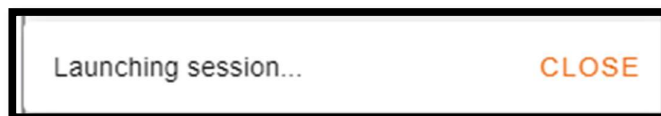


This will open up a popup. The Agent will need to copy and paste this data to the support team.



If unlinked not all data will be populated.

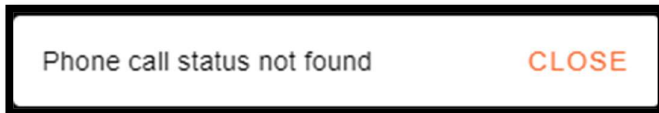
viii. App Alerts:



This alert appears at the bottom of the app when the Payment Journey is starting



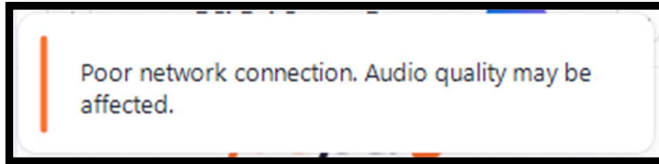
This alert appears at the bottom of the app when the call has been successfully secured



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.

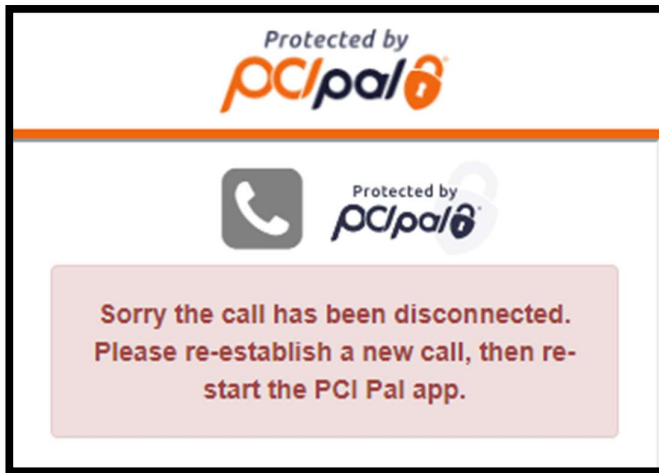


This alert appears at the top of the app should Zoom believe the Agent's network to be weak or comprised during a call. This is a Zoom alert.

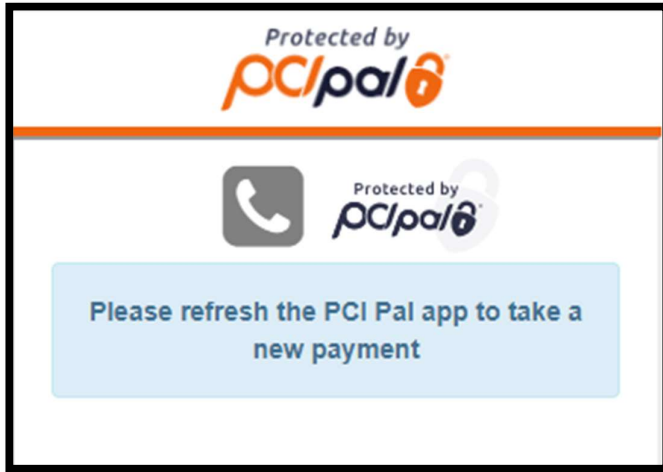
ix. Journey Alerts



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]