



LOCAL SHOPS: ACCEPTING 'CARD NOT PRESENT' PAYMENTS

This guidance is designed to inform convenience retailers about best practice on offering and processing 'card not present' payments during the Covid-19 outbreak for volunteers purchasing groceries on behalf of vulnerable customers or people self-isolating.

Volunteers paying for groceries in local shops

The Government is advising people who are at very high risk of severe illness from Covid-19 to 'shield' themselves from harm by staying at home for a period of at least twelve weeks and avoid going out for grocery shopping. Many thousands of volunteers acting on behalf of vulnerable customers need a means to pay for groceries in convenience stores.

As gift card schemes or digital vouchers are not widely used in the convenience sector, an alternative is for vulnerable customers to pay over the phone via **'card not present' (CNP)** payments, where card details are shared over the phone and entered by the retailer into the card payment terminal.

How can I accept 'card not present' transactions?

1 Retailers should contact their card acquirer or POS terminal provider to enquire about adding CNP services onto their existing agreement.

Card acquirers

	0844 8116666	https://www.barclaycard.co.uk/business/contact-us
	0345 8500195	https://www.elavon.co.uk/customer-centre.html
	0844 8000233	https://www.uk.epayworldwide.com
	020 8081 3840	https://www.fisglobal.com/en-GB
	020 8833 3000	https://www.fiserv.com/en.html
	0345 7023344	https://www.globalpaymentsinc.com/en-gb
	01268 567100	https://www.lloydsbankcardnet.com

2 Mitigate fraud risks from CNP transactions by following your acquirer/terminal provider's anti-fraud advice.

It should be noted that in-store CNP transactions raise additional risks of fraud and chargeback liability for the merchant. To minimise risk you could consider:

- Putting a limit on payment values, for example £100.
- Limiting use of CNP payments per customer, for example three per week.
- Limiting high value products per transaction, for example spirits or tobacco.

3 When on the phone with the customer enter the following details into your card terminal:

- The long card number.
- The card expiry date.
- The three-digit security code or house number/postcode of the card holder.

Do not write down or record customer card details.

Retailers should check with their card acquirer about the information they need to ask for over the phone. More details on card authentication are included below. Some volunteers helping customers may provide a "code word" to use over the phone so the customer knows they are securely giving the payment details to the retailer.

A typical CNP payment scenario:

Volunteer goes to local shop to purchase groceries for an isolating or vulnerable customer.



Volunteer takes groceries to the till and asks the retailer to call the customer for card payment details.



The retailer speaks to the customer on the phone and takes a card payment over the phone using the 'card not present' function.



Payment is made and the volunteer is given groceries and card payment receipt.





LOCAL SHOPS: ACCEPTING 'CARD NOT PRESENT' PAYMENTS

How can I reduce the chances of fraud?

Retailers are strongly advised to authenticate use of the card over the phone via the following fraud detection and prevention tools:

■ Address Verification Services

An Address Verification System (AVS) checks the billing address of the card provided by the customer with the address on file at the customer's bank. This is an instant check made by the customer's bank but retailers taking details for a CNP transaction will need to ask for billing address details too for this to be completed. Results from the AVS check can help retailers decide whether to accept the order. This check is most commonly completed for telephone orders.

■ Card Security Codes

Card Security Codes (CSC) are the three-digit numbers present on the back of most cards. By entering the CSC during a CNP transaction, retailers enable a check to be made that the customer is in possession of the valid physical card. CSCs cannot be recorded or stored by retailers, including for recurring transactions.

■ PCI DSS Standards

The Payment Card Industry Data Security Standard (PCI DSS) is a standard used across all major card brands to protect cardholder account security when account details are shared with retailers and anyone involved in processing and transmitting payment card information. Your card terminal should be PCI DSS compliant, if in doubt please contact your acquirer.

How can I reduce risks of chargeback?

Chargebacks occur when a customer disputes a charge on their card. The customer typically contacts their card issuer and initiates the process for a refund via the acquirer paid for by the retailer. Retailers can challenge any disputes in a process called representation by substantiating the charge and providing verification of the sale. The following best practice to prevent chargebacks is additional to the anti-fraud measures outlined above:

- Retain copies of order forms if applicable and evidence of customer receipt of goods (i.e. signed receipt).
- Use email to notify consumers of the details of sales and to indicate that their cards will be charged.
- Post clear policies for billing, returns, delivery and data privacy on your website. Order confirmation emails should include this information and any further terms and conditions in the content or via a web page link.
- Always provide a clear billing descriptor with a phone number so the customer can contact you directly rather than calling their bank to discuss any dispute.
- If you have a website or social media pages, provide a contact phone number and email address so customers can contact you directly.
- Obtain the customer's phone number and email address.
- Notify customers in writing when a refund has been issued. Provide them with the date the transaction was submitted and a reference number.
- Indicate that the card issuer may require a full billing cycle to apply any refunds, which may not immediately appear on an online statement.



ADDITIONAL INFORMATION



For more details on this guidance, contact Steve Dowling via steve.dowling@acs.org.uk. For more details on ACS: Visit: www.acs.org.uk
Call: 01252 515001 Follow us on Twitter: @ACS_Localshops