Selling goods and services safely

How to keep fraud out of your business

If you are a retailer you probably let some of your customers pay remotely - either online, over the phone or by mail order.

These card-not-present (CNP) transactions are particularly vulnerable to fraud because the buyer is 'invisible' and normal face-to-face precautions aren't possible.

This guide explains how easily fraud can happen during a card-not-present sale and looks at the practical things you can do to keep your business safe.

Preventing CNP fraud makes good business sense.

- You protect your sales.
- You reduce the risk of being left out of pocket when the card issuer reverses a fraudulent payment (called a chargeback).

What is card-not-present (CNP) fraud?

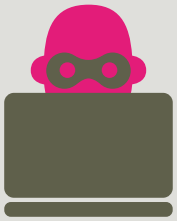
A card-not-present (CNP) transaction is when the customer is not physically present (with their card in their hand) at the time of payment.

It is easy for criminals to use CNP transactions to make fraudulent purchases using other people's card details that have been stolen or cloned.

Beware of CNP risks when selling

Most CNP frauds happen in one of two commonplace situations

As part of an online transaction



or

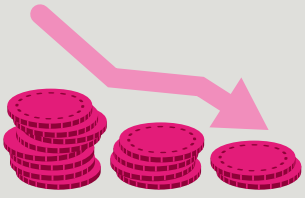
During a phone or mail order sale

(When you input the customer's card details yourself.)

The card authorisation process does not guarantee these payments.

It checks only that there are sufficient funds in the cardholder's account and that the card hasn't been reported lost or stolen.

Fraudulent payments can be reversed by the card issuer, leaving you - the retailer - out of pocket.



Know the signs

Any of these should sound the alarm.

1. Several transactions are declined before one finally goes through.

2. The delivery address has been used before but with different customer details.

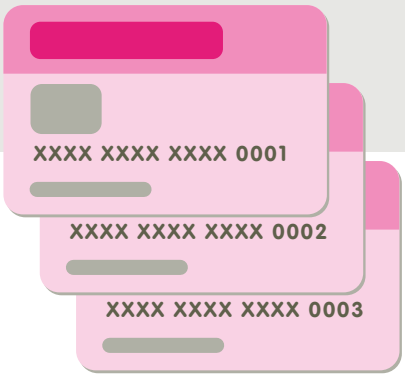
3. An order has a delivery address that is different from the registered card address.

4. Large bulk orders of identical or similar items have delivery addresses that are residential or self-storage facilities.

5. A single card is being used across several customer accounts.

6. The same phone number/email address/ delivery address has been used with more than one card or account.

7. Several cards are used, and their numbers are sequential or similar apart from the last few digits.



8. The customer wants to spread the cost of a purchase over several cards and some of them are declined.

9. The customer wants their purchase to be despatched immediately but seems unconcerned about the shipping costs.

10. During a telephone order you can hear the caller being prompted by someone in the background, or they have a problem remembering their own contact details.

11. The caller asks to remove items from the order to reduce the value (perhaps to take it below the card issuer's authorisation threshold).

12. The transaction is in some way unusual for your business.

FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

Thanks to Sarah O'Shea from Barclays for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights the risks of card-not-present fraud when selling goods and services. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.

Selling goods and services safely

How to keep fraud out of your business

Love business Hate fraud

A checklist

Ask yourself...

- **Am I sure this customer is genuine?**
- **Am I using the basic security measures recommended by my card processor or bank?**
- **Is the purchase (or pattern of purchases) unusual?**

Do...

- Review transactions for anything out of the ordinary.
- Use 3D Secure (Mastercard Identity Check and Visa Secure) and CSC/AVS (Card Security Code/Address Verification Service).
- Turn on two-factor authentication (2FA) when creating new customer accounts.
- Review your chargeback records looking for anything of concern among the delivery and IP addresses.
- Make refunds only to the same card used for the original purchase – and always check the card details again.
- Be wary of customers who purchase high-value items or large quantities without asking about things like quality, size, style, colour or price.

Don't...

- Input an authorisation code given to you by the customer.
- Accept an order with an incorrect CSC code.
- Accept new orders with an invalid card expiry date.
- Lose sight of your card terminal – fraudsters will try to use distraction techniques to get hold of it.

Protecting your business

Some simple steps can make your business safer.

Use 3D secure for online sales

Use Mastercard Identity Check and Visa Secure so that online customers must complete an extra verification step.

Use two-factor authentication (2FA) for new accounts

2FA requires new customers to verify their phone number when setting up an account, helping to make sure they are genuine.

Two-factor authentication

Use Card Security Code (CSC) and Address Verification Service (AVS)

Ask customers to provide the CSC on the card (usually 3 or 4 digits) and the street number and postcode of the cardholder's billing address.

Verifying the CSC helps to show that the customer is in possession of the physical card. AVS checks that the address provided by the customer matches the one held by the card issuer.

Use fraud screening tools

Rule-based fraud detection tools can enable you to cross-check whether a customer's name and contact details (including email address and phone number) have been flagged as suspicious.

Never enter an authorisation code provided by the customer.

FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

Thanks to Sarah O'Shea from Barclays for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights the risks of card-not-present fraud when selling goods and services. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.