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.

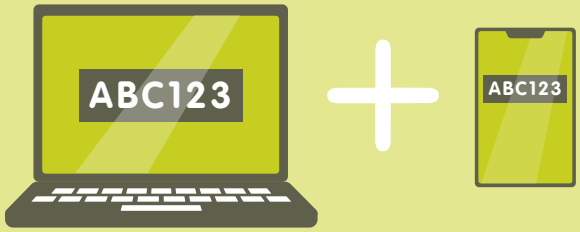
Use 3D secure for online sales

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.