Top tips for fraud prevention

from

fidelitypayment

Keep your business and customers safe

Chip and PIN

Fraud Prevention Tips

fidelity payment

Fraud support team

☎ 0345 481 2188

Chip and PIN is most secure type of transaction. Merchants not required to make visual card checks of the card as Cardholder retains control of card during transaction. Follow all prompts on your terminal

Take care that the customer does not interfere with **terminal/PIN pad.** If you are presented with a card that does not have Chip and PIN, be extra vigilant.

Do not key a card number into your terminal for transaction where card and Cardholder are present, this will leave you open to risk of **Chargeback Dispute.**

Be on guard if a Chip and PIN card is presented but **PIN blocked or incorrect PIN entered.** Check this is genuine Cardholder as you may be at risk if you accept a signature

Use **Ultra Violet (UV) light** to check card as most genuine cards have special features that show up.

Check whether number printed on terminal sales receipt is same as that embossed on front of card. Counterfeit fraud often involves **'skimming' or 'cloning'** where genuine data in magnetic stripe on one card is copied onto another card without legitimate Cardholder's knowledge. Often the fraudster will not re-emboss the card number on the card to match numbers in magnetic stripe so fraud can be easily identified.

Compare name on card with **signature** and signed voucher.

Check whether **signature strip** on card appears tampered with, raised or if originalsignature appears to have been covered over.

Check as the Cardholder signs whether they are taking an unusual amount of **time** to sign.

Does the **Cardholder** appear nervous/agitated/hurried or are they trying to distract you by being rude or overly friendly?

Are they making **indiscriminate purchases** eg not interested in the price of item or making hasty bulk purchases?

Are they making small item purchases with **maximum value cashback**? Please ensure you have Fidelity Payment's agreement before processing any cashback transactions.

Does title of card match **gender** of person presenting it.

Be wary if the customer say that they are having problems with their card where **multiple card transactions** are subsequently declined but eventually authorised for lower value. Most genuine Cardholders are aware of credit available on their cards.

A fraudster may present more than one card, If so complete additional checks to validate transactions and check names on the cards.

Card sales should never be split between two or more vouchers for the same card to avoid authorisation as these may be subject to a **Chargeback Dispute**.

Is purchase/order substantially greater than your usual sale.

Has customer repeatedly returned to make **additional orders** in short period of time,causing unusual/increase in number and value of sales transactions? If the card or person raises suspicion, telephone the Authorisation Centre and state "this is a code 10 authorisation". Answer all of the operator's questions and follow their instructions.

Card Not Present (CNP) Fraud, including eCommerce

Fraud Prevention Tips

fidelity payment

Fraud support team

☎ 0345 481 2188

Please ensure you have agreement from Fidelity Payment before making any CNP or eCommerce transactions. Obtain separate MID for eCommerce transactions. **CNP transactions provide more opportunity for fraudsters**, as the card cannot be present at the time of the purchase, (by telephone, mail order or electronically). A card sale should never be split between two or more vouchers for the same card to avoid authorisation as these card transactions may be subject to a **Chargeback Dispute**. If a customer presents more than one card for payment please complete additional checks to validate the transaction. Under no circumstances can goods purchased by CNP or over the internet be handed over the counter or collected by the customer. You will be liable for a Chargeback Dispute if the transaction is disputed at a later date. If a customer wishes to collect the goods then they must attend your premises in person and produce the card. Destroy any sales voucher that may have been prepared and process an over the counter transaction. If you have already processed a CNP or eCommerce transaction you must either cancel it or perform a refund.

Also:

- **Pre-registration** – before allowing your customer to purchase goods or services online request they first register as a user. You can then ask for a variety of data to establish a customer profile. Firstly, verify the name and address details before deciding to accept or decline the user. They need to agree to your use of their personal data, as set out in your website's privacy policy. Also ensure their personal data is being processed fairly and legally and in compliance with the Card Scheme rules.

- For **business customers not known** to you, check their details in the local business directory or internet search/map engine.

- Independently obtain a telephone number for the Cardholder's address and telephone the Cardholder on that number to confirm the order (not necessarily straight away). Also consider writing to the customer before dispatching goods, if you are suspicious and unable to validate by other means.

- For **internet transactions** monitor the Internet Protocol (IP) for repeated use on a number of different transactions.

- Apply **sensible limitations** to the number of cards that customers can have registered to an account and consider limiting high risk services until a customer has been validated.

Delivery Warning Signals. Look out for these when arranging delivery of goods:

- If the Cardholder's delivery address is **overseas**, consider if the goods or services are readily available in the Cardholder's local market.

- **Goods should not be released to third parties** i.e. friends of the Cardholder or couriers (However, third party delivery of low value goods e.g. flowers is acceptable).

- Goods should only be delivered to the **address** that matches the Cardholder's card. If you do agree to send goods to a different address keep a written record of the delivery address with your copy of the transaction details.

- Don't send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier with a signed and dated delivery note.

Instruct your Couriers

- To ensure the goods are delivered to the **specified address** and not given to someone who 'just happens to be waiting outside'.

- To return the goods if they are unable to effect delivery to the agreed person/address.

- Not to deliver to an address that is obviously vacant.

- To obtain signed **proof of delivery**, preferably the Cardholder's signature If you have your own delivery service, you may want to consider portable terminals; please contact us for more information.

Split Sales with Cash, Cheque or Second Credit Card

Fraud Prevention Tips

fidelity payment

Fraud support team

☎ 0345 481 2188

If the **total sale is equal to or exceeds your ceiling limit** and payment is offered partly by MasterCard, Visa, internationally issued Maestro or Laser and partly by cheque, cash or any other method, authorisation must be obtained for any part of the card transaction being paid with by card .

Even when the card amount is below your ceiling limit.

The **Authorisation Centre should be informed** that the request for authorisation is in respect of a split sale.

The **Authorisation Centre** may require further details.

Note: If a transaction is above your ceiling limit, you should contact the **Merchant Support Centre** to request an increase in your ceiling limit and not accept split payments.

If you have **any questions or require guidance** in relation to authorisation issues, please contact the Fidelity support team on **0345 481 2178**.

For security reasons your ceiling limit should never be displayed to the general public.

Other Fraud Considerations

fidelity payment

Fraud support team

☎ 0345 481 2188

Never process transactions for any business other than your own. Fraudsters may offer commission to process transactions when they have not been successful in obtaining their own credit card facilities, or you may be asked to process transactions on behalf of a third party while they are waiting for their own facility. If you process transactions on behalf of any other business/person you will be liable for any Chargeback Disputes and doing so is in breach of your Terms and Conditions and will lead to termination of your agreement. Your card transactions must not involve any card issued in:

- Your name or your account
- The name or account of a partner in, or director of your business
- The name or account of a spouse or any member of the immediate family or household of any such person detailed above.

Transaction Laundering

If you are approached with a proposal to buy card transactions, please contact us. This is a form of money laundering and is contrary to the terms of your Merchant agreement.

Phishing E-mails/Calls

If you are contacted by somebody claiming to be a bank or an official business asking for transaction details of cards recently accepted for payment, please contact us. This is a fraud tactic to obtain card details. A bank or any other official business would not make contact in this way to request card information. Please take care when receiving calls or visits from 'terminal engineers'. Fraudsters will attempt to gain access to your terminal or may manipulate you into processing fraudulent refunds. Please always validate these by contacting us to advise or investigate.

Some businesses are more prone to fraud than others. It is your responsibility to protect your business from financial loss.

- Analyse **Chargeback** Disputes and fraud previously suffered, it will help to identify where your business is most at risk and how fraud can be prevented in future
- Speak to Fidelity Payment about potential fraud **screening services.**
- Ensure staff are continuously educated on your **risk management procedures**, your front line staff are key to identifying and reducing instances of fraud.
- If you are concerned that you may be vulnerable to **fraud attack**, perhaps because of your business location, products or services sold or local intelligence, please contact the Merchant Support Centre and ask to speak to the fraud department who will be happy to give guidance on best practice.

Terminal Security – Protecting your POS Equipment

- It is your responsibility to ensure that all **staff are properly trained** in how to use your terminal(s) and the security checks associated with checking cards presented for payment

- **Supervisor cards** should be used by staff members who are fully knowledgeable in terminal operation.

- Supervisor cards should be kept secure and not alongside the terminal.

- If you have any concerns that the terminal has been tampered with, contact terminal support on the numbers provided. Card Security Code (CSC/CVV2/CVC2) The Card Security Code (CSC) is the last three or four numbers on the signature strip on the back of the card. For all MasterCard and Visa cards the code is the 3-digit number that follows directly after the card number. On some cards, only the last 4 digits of the card number are repeated in the signature strip, followed by the 3-digit CSC.