Simple Steps to Prevent Payment Card Fraud

A NetPay Guide

intelligent payments

www.netpay.ie
www.netpay.co.uk

NetPay

Payment card fraud cost the UK's small businesses in 2013 £450m in lost revenue, £105.5 million of which was online. If your business is compromised by fraud it can damage your business financially and also have a detrimental effect on your brand reputation within the market place.

Here are our simple steps to preventing card payment fraud from occurring in your business:

Card Not Present Fraud (Online & Mail Order/Telephone Order)

This type of card fraud is where fraudsters obtain consumers card details from things like discarded receipts, email or account hacking and they use this information to purchase high value or desirable goods online, by phone or mail order.

How to prevent this type of fraud

If you are selling your goods and services online then it is important to ensure that your online system is PCI compliant and uses 3D secure which is an extra level of security.

There are a few questions you should ask yourself before proceeding with the order if you answer yes to any of them then you should take further steps to identify the legitimacy of the order:

- Is the sale excessively high in comparison to your usual orders?
- Does the address provided seem suspicious? Has the delivery address been used before with different customer details?
- Is the customer attempting to use more than one card in order to split the value of the sale?

If you are still unsure check the **Industry Hot Card File** to see if the card is registered.

Remember you have the right to decline the order, if you suspect the transaction to be fraudulent make every effort to try and contact the customer and verify their details before making your decision.

Fake Cards

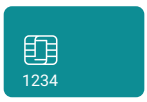
Although on the decline since the introduction of chip and pin in the UK there is still a black market for the manufacturing of fake credit cards using genuine card details. The card details are copied from the magnetic strip of the genuine card using a device called a skimmer. This information is then transferred to the magnetic strip on a fake credit card, so the customer will not be able to use the chip and will ask for the card to be swiped. Although some foreign cards do not use the Chip and Pin you should be wary if a customer asks to swipe.

How can I tell if a card is fake?

Extra vigilance should be taken when accepting cards that are not chip and PIN. Foreign cards and chip and signature cards will still exist. When swiping the card follow your on terminal prompts.

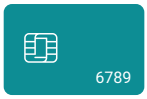
Also look out for these:

- **Check the first four digits** – On MasterCard and Visa cards the first four digits of the embossed card number are also printed above or below
- **Check the last four digits** – Check that the last four digits shown on the front of the card match the last four digits shown on the receipt
- **Check the signatures** – Is the spelling correct? Is it large, messy writing on the signature strip possibly covering the real signature?
- **Check the signature strip for signs of tampering**



Step 1

Check the first four digits of the card number



Step 2

Check the last four digits of the card number

Step 3

Check the signature on the back of the card

Step 4

Check the signature strip for signs of tampering

NetPay Merchant Services

UK

T +44 (0)333 311 0200
E getintouch@netpay.co.uk
W www.netpay.co.uk

Ireland

T +353 (0)1 447 5299
E getintouch@netpay.ie
W www.netpay.ie

Frequently Asked Questions

Should I accept a card that says it is void on the signature strip?

No, these cards should be treated as void and an alternative payment method sought.

How can I tell if a customer is a fraudster

There is no real way to tell whether a customer is in fact a fraudster, there are however some things that you can look out for that may help to identify a fraudster:

- Does the title on the card that you are given match the person? For example if the card says Mrs and the person giving you the card is a man then your suspicion should be aroused
- Is your customer making a low value purchase with large cashback?
- Is the customer nervous or distracting you?
- Is your customer buying a large number of the same item?

What do I do if I am suspicious of a customer?

If you are suspicious of a customer remember that it is important to treat them how you would wish to be treated. Keep hold of the card, unless you feel under threat from the customer. You should make a Code 10 authorisation call using the authorisation centre number provided by your acquirer. Tell the operator that you are making a Code 10 call and then follow their instructions.

If the operator asks you to call the Police then it is up to you to decide, according to the circumstances and your own store policy, if you want to make the call. **NEVER** put yourself or your staff at risk in trying to detain a customer.

Remember: If you feel threatened and do not think it is safe to make a Code 10 call e.g. you are alone in the shop, make the call immediately after the customer has left and provide the operator with all the information you have.

What do I do if I spot a fraudulent card?

If you find a fraudulent card whilst checking the transaction, then it is important to retain the card, whatever you do though, **NEVER** put yourself, colleagues or customers at risk in order to retain the card.

If you do retain a card then it is important that you preserve the evidence so that it can be used by the Police and the bank for investigation

Follow these steps to make sure that the evidence is preserved as far as possible:

- Cut the bottom left corner off the front of the card this is to show that the card is void – Be careful not to damage the magnetic stripe, or chip.
- Try to handle the card as little as possible to preserve any finger prints that may have been left and pop the card into a paper or plastic bag
- If you have CCTV cameras in your store then then retain the footage and make a note of the date and time of the incident
- Fill in an incident description form to note what the fraudster looked like e.g what were they wearing, any accents or distinguishable features.
- Contact your authorisation centre and follow any instructions that you are given.