globalpayments

www.globalpaymentsinc.co.uk

REDUCING THE RISK OF CARD NOT PRESENT **FRAUD**

INTRODUCTION

Many businesses accept Card Not Present (CNP) transactions on a daily basis, either over the phone or via a website. In the majority of cases there are no problems with these orders, but there is an increased risk when accepting CNP transactions as there is no 100% guarantee that the person placing the order is the genuine cardholder. You also have less protection than you'd have if you were processing transactions via Chip and PIN, as your business will be financially liable if a transaction is later reported as fraudulent.

TO HELP REDUCE THE CHANCES OF YOUR BUSINESS BEING TARGETED BY FRAUDSTERS, THERE ARE A NUMBER OF CHECKS THAT SHOULD ALWAYS BE MADE:

01

ADDRESS VERIFICATION SERVICE (AVS) CHECK

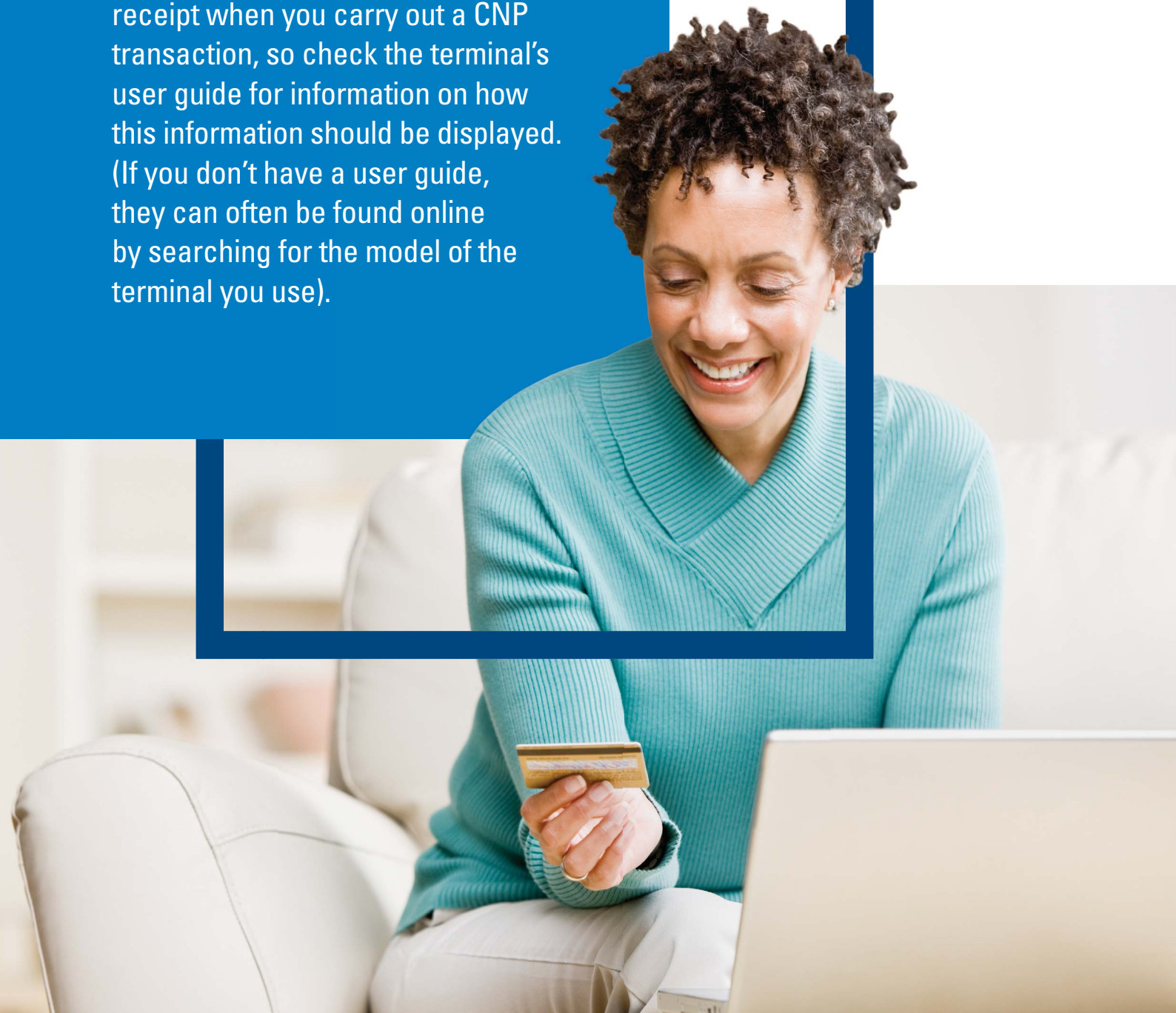
This checks the property number and the numeric part of the post code against the issuer's records. This works for UK issued cards, but non-UK card issuers may or may not perform this check. If this check isn't verified, this may be a sign that the card being used is not from the UK and the order may be fraudulent.

02

CV2 CHECK

The CV2 number (sometimes called the CVV number or security code) is the 3 digit number printed on the back of a credit or debit card. If the CV2 check fails, this is a clear sign that the customer may be using compromised card details. However, if the check does pass, this is still not a guarantee that you are dealing with the genuine cardholder.

The results of these two checks will be printed on the terminal receipt when you carry out a CNP transaction, so check the terminal's user guide for information on how this information should be displayed. (If you don't have a user guide, they can often be found online by searching for the model of the terminal you use).



"IF YOU ARE SEEING MULTIPLE DECLINES WHEN TRYING TO PROCESS A TRANSACTION, YOU SHOULD BE CAREFUL ABOUT PROCEEDING

IN ADDITION TO THESE BASIC CHECKS, THERE ARE OTHER THINGS YOU CAN DO TO IDENTIFY POTENTIAL FRAUD:

03

USE OF MULTIPLE CARDS AND DECLINED ATTEMPTS

Fraudsters often buy batches of compromised card details and will try each set of card details until they can get one to work. If you are seeing multiple declines when trying to process a transaction, you should be careful about proceeding with the order.

04

NON-UK ISSUED CARDS BEING USED FOR ORDERS TO BE DELIVERED TO A UK ADDRESS

A lot of CNP fraud is committed using non-UK issued cards for goods which are to be delivered to addresses in the UK. If you are taking orders online, or using a virtual terminal, many card processors can flag up orders like these, so make sure this check is set up. For other terminal types, one sign that the card is not issued in the UK is that the AVS check doesn't pass. If your system allows you to view the first 6 digits of a card number (known as the Bank Identification Number, or BIN), you can check where a card was issued on various websites by searching for 'BIN list lookup'.

> IF AN ORDER IS BEING PICKED UP BY A COURIER, ASK THEM TO ONLY DELIVER TO THE SPECIFIED ADDRESS

05

PICK-UP FRAUD SCAM

This is one of the most common fraud scams we see. A new customer places an order for goods over the phone and says that they, or a courier/ taxi, will pick the goods up. The fraudster may have the correct name and address details of the genuine cardholder, so things like the AVS check may pass. Sometimes we see cases where a fraudster is prepared to travel a considerable distance to purchase goods which they could easily get closer to home, so be careful with orders like these. As the goods are being picked up there is also no way to confirm where they are actually going, so if you are in doubt, ask the customer to bring their card with them and do the transaction as Chip and PIN.

If an order is being picked up by a courier, ask them to only deliver to the specified address and not to accept any changes to delivery instructions after they have picked the goods up from your business, without checking with you first.

> BE CAREFUL IF A CUSTOMER WANTS YOU TO SEND OUT THE GOODS VERY URGENTLY

06

ORDERING AND DELIVERY

- Take care when you are given an alternative delivery address, particularly if it is in a totally different location to the billing address. Some merchants have successfully prevented fraud by contacting the person at the billing address before sending out orders, so this may be worth considering.
- Be careful if a customer wants you to send out the goods very urgently and is prepared to pay delivery costs which are very high compared to the value of the goods, or if they repeatedly contact you to chase up their order. They may well be trying to have the goods delivered before the card is cancelled and you are alerted to the fraud.
- Use websites such as 192.com, yell.com, Google and Streetview to verify customers and delivery addresses. For example, if you are being asked to deliver goods to a business, then be careful if the address they give you is for a residential property. Businesses can also be checked to make sure they actually exist. If possible, you should also ask for a landline number instead of a mobile number, especially for business customers.
- Some merchants who deal mainly with other businesses have avoided being targeted by fraudsters by asking new customers to pay for orders by bank transfer, or cheque and only offering to accept card payments from them once a business relationship has been established over time.
- If you are taking orders via a website, we strongly recommend that you have 3D Secure (Verified by Visa and MasterCard Securecode) in place. In the majority of cases, the liability for any fraudulent transactions will then be switched from your business to the card issuer.

For further advice on what to do if you believe your business is being targeted by a fraudster, you can call the Global Payments Fraud Team on **0116 252 4984***, or e-mail them at **fraud.risk@globalpay.com**.

If you have been a victim of fraud, you should report it to the Police via the national website: **www.actionfraud.police.uk**.

* Lines are open Monday to Friday, 9am to 5pm except Bank Holidays.

Global Payments is HSBC's preferred supplier for card processing in the UK.

Issued by Global Payments, 51 De Montfort Street, Leicester, LE1 7BB. GP422