FRAUD DETECTION AND PREVENTION

Fraud Detection And Prevention

Fraud has become a global epidemic that threatens everyone, so for your security you need a card processor who is at the cutting edge of fraud-prevention technology. In addition, you need advice and services that help you implement business practices to minimise the risk and cost of fraud.

Your Dedicated Anti-Fraud Team

As one of our customers, you'll have the protection and reassurance of working with a team that is dedicated to reviewing merchant trading patterns to determine if any fraudulent activity has or is about to occur. When they see something suspicious, they'll begin detailed and expert checks to establish whether the transaction is genuine.

If everything checks out, that's fine; we don't need to trouble you. But if our team has concerns that the payment could be fraudulent, they will then contact you to escalate any concerns and advise you not to release any goods or provision of services.

This commitment to our customers has prevented millions of pounds of fraudulent orders from being dispatched.

The Risks You Face

It's tempting to think that once a payment is authorised, you're assured of receiving your money. Unfortunately, that's not the case; in fact, there are several potential pitfalls that could threaten your income.

We will work closely with you to ensure you understand exactly what is happening throughout a transaction and who bears the risk and responsibility. For example:

Authorisation Doesn't Guarantee Payment

When authorisation is provided, all this confirms is that funds are available, and that the card hasn't been reported lost or stolen - yet. But the rightful holder might not know that the card is missing, so the transaction could still turn out to be fraudulent.

Additional security measures like Address Verification Service (AVS) and Card Security Code (CSC/CVV/CVV2) for transactions where the customer isn't present undoubtedly help to reduce fraud. By making life more difficult for a fraudulent purchaser, this can provide a level of comfort that the buyer is who they say they are. But, it's still not a guarantee.

This is an important consideration for Customer Not Present (CNP) transactions like mail/telephone order or internet purchases, because these transactions are made at your own risk. After a purchase, the customer has up to 120 days to challenge the transaction as not being genuine. If that challenge is successful, its value could be charged back to you - that's a possible four months of uncertainty on every CNP transaction.

Closing The Security Door

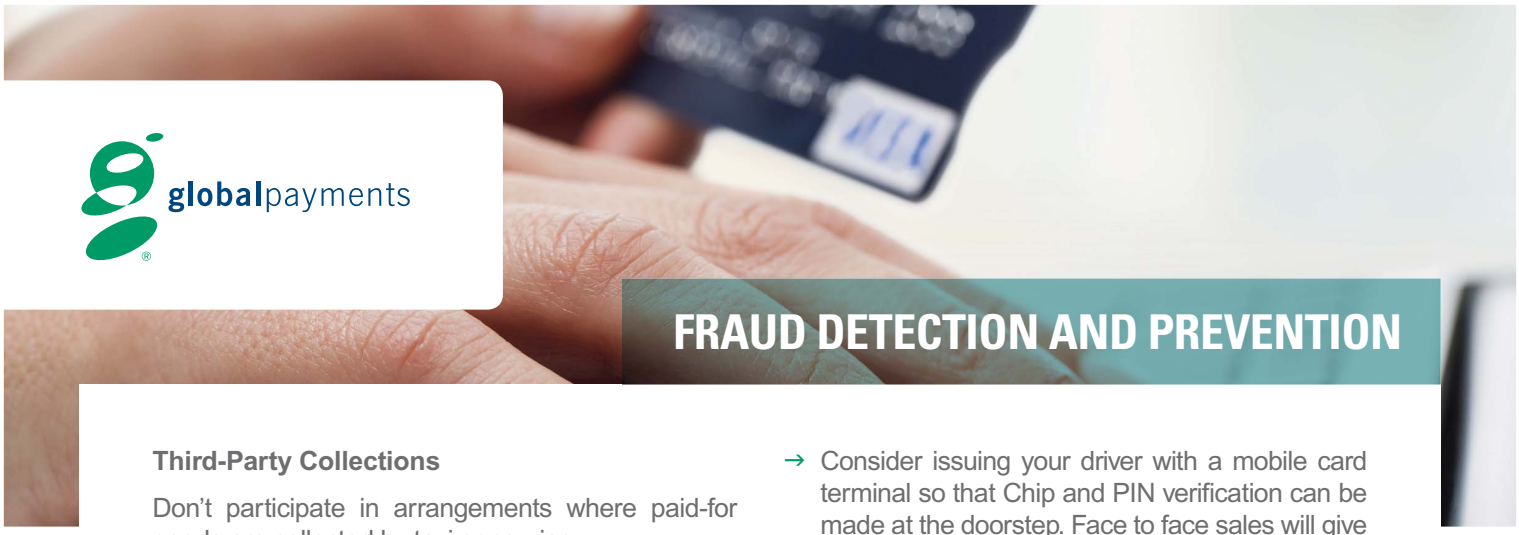
Fraudsters are ingenious, creative and adaptable. If something doesn't feel right, then trust your instincts and refuse to participate. Here are a few typical scams to look out for:

Inbound Authorisation Calls

Don't accept an inbound call from an Authorisation Centre. Be suspicious should you receive such a call. Politely decline/end the call and then call your Authorisation Centre yourself.

Why not give us a call on **0800 731 8921***, or go to **www.globalpaymentsinc.co.uk**

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. Calls may be recorded. We also provide a Textphone service on 0845 602 4818.



FRAUD DETECTION AND PREVENTION

Third-Party Collections

Don't participate in arrangements where paid-for goods are collected by taxi or courier.

Non-Standard Procedures

Refuse transactions that look suspicious. Non-standard procedures can easily take you outside your required PCI - DSS compliance and leave you exposed.

Overpayments

Decline requests to forward overpayments by money transmission services to third parties such as intermediaries or facilitators.

Suspicious Internet Payments

Don't be afraid to decline suspicious orders. Remember - you are under no obligation to fulfil a transaction you consider to be fraudulent. Be cautious of unsolicited email contact or orders emanating from free email accounts where the customer's name isn't reflected in the narrative and where a mobile telephone number is the only means of customer contact.

As a general rule, always suspect any deviation from normal purchasing.

Boosting Your Security

Adding a few simple tweaks to your operations can do a great deal to increase your security, and reduce instances of fraudulent transactions. These can include:

- → Always validate the customer's billing details and card security code via the terminal.
- → Have your own delivery driver ask to see the card used to make payment.
- → Consider issuing your driver with a mobile card terminal so that Chip and PIN verification can be made at the doorstep. Face to face sales will give you greater security and peace of mind.
- → Capture and verify a land line telephone number
- → Enrol in the 3D Secure initiative offered by MasterCard and Visa for internet transactions. This can protect you from chargebacks where a cardholder claims that they didn't authorise a payment.

The Internal Threat

Not all fraud attacks come from outside. Unfortunately, your own staff can sometimes get involved in fraudulent card processing activities, such as refunds being refunded into their own bank account rather than into a customer's. This often happens behind your back and can affect your profits.

The good news is that many of these activities leave tracks in the card transaction trail and we can help you detect these.

You Can't Afford To Get It Wrong

The vast majority of card payments are completed without problem. But just one rogue transaction can stop you in your tracks, soaking up your time and potentially costing you a significant amount of money as well as damage to your reputation. So today's a good time to do something positive to make sure you're in the strongest possible position.

Find out more by calling us today on **0800 731 8921*** or by visiting **www.globalpaymentsinc.co.uk**

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. Calls may be recorded. We also provide a Textphone service on 0845 602 4818.

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

GP205