Guide

Are you fraud aware?
IS YOUR BUSINESS FRAUD AWARE?

Many businesses fall foul of fraudsters because they are not aware of the risks involved when taking card payments. Before trading you should ensure you are aware of the risks involved and implement checks that can help reduce the risk of loss to your business. We recommend you familiarise your employees with the below fraud trends/scams and furthermore, consider what checks your business could implement as part of your fraud prevention strategy.

Additional resource and advice is available from: www.worldpay.com/uk/support-sme-support-security/reducing-fraud

NEVER TRANSFER FUNDS

Be wary of requests to forward on funds to a specified account as part of an agreed sale. We have seen scams whereby:

- A large deposit or full payment will be offered up front for the goods/services offered by your business
- Days after the booking you will be contacted again advising that the services of a third party have been enlisted for additional services e.g. car/coach hire or interpreter.
- A request will be made for you to transfer funds directly to a third party’s bank account to cover these costs.
- Once the fraudster receives the funds there will be no further contact and you will be left to pay the chargebacks made with the stolen card details.

LOOK OUT FOR DAMAGED CARDS

We have seen the following approach used by fraudsters in attempt to encourage a merchant to process a customer present transaction without reading the chip or mag stripe:

- Fraudsters are presenting cards that when inserted into your Chip & PIN device, displays a message advising that the card can not be read and/or the magnetic strip is damaged.
- The fraudster will then suggest you manually enter the card number into your terminal, this will either be taken from the front of the card directly or may be given to you by the fraudster.
- If you are presented with a card that is clearly damaged or your terminal can not read the details, you should advise the customer that you can not accept the card and suggest they get a replacement from their card issuer.
- If they wish to proceed they will have to pay using another method.

ALTERNATIVE AUTHORISATION NUMBER

There are several scams where fraudsters are targeting retailers by claiming to be a Streamline employee. One example, highlighted below, could lead to a compliance breach:

- A phone call will be made from a fraudster claiming that they work for “Streamline” or “WorldPay”.
- The impersonator will claim there to be an issue regarding the authorisation stage of the transactions being processed by your business.
- They will provide an alternative telephone number and request that you obtain authorisation for every transaction you process over a certain period of time.
- The requested information that you are to provide will normally include full card/PAN number, expiry date and the 3 digit security code.
- You should only use telephone numbers contained within your customer operating instructions or on www.worldpay.com/uk/support-sme-support/operating-instructions

BOGUS ENGINEERS

Another tactic used to target Streamline retailers is the bogus engineer scam. All engineer visits would always be advised in advance. We strongly recommend you ask for identification and be suspicious if engineers turn up without any prior arrangement/appointment. If you are unsure, call our Helpdesk on 08457 61 62 63, Option 2 to confirm a visit. Below are some recent indicators of this scam:

- An individual guising themselves as a Streamline Engineer will approach an employee of a business asking to perform a check or update on the terminals.
- They will either request to work on the terminal and take it out of sight or ask you to process certain “test” transactions.
- Similarly you may be informed that the “engineer” needs details relating to past transactions, possibly due to an alleged processing error.
• We strongly advise you never divulge any card details.
• Never let your terminals out of your sight. Only allow authorised personnel access to your terminal.
• Nobody from Streamline will ever request your business and ask you to process purchases or refunds.

THIRD PARTY PROCESSING

It is vitally important that you only process transactions through your terminal that relate to goods/services your business are providing. We have been made aware of several instances whereby businesses are approached with a proposal:

• Your business will be contacted by an individual or group and offered an “opportunity” that will involve you processing transactions on behalf of a third party through your merchant facility.
• The funds processed on behalf of this “other business” will need to be wired to a specific account and, most likely, your business will be offered a cut of the monies in return.
• By processing any other payments you are then responsible for the risk and are fully liable should any debt arise.
• Do not accept any such proposal to ensure your ability to process card payments isn’t affected by Streamline.

COURIER / COLLECTION OF GOODS

This well known scam targets retailers and can leave you fully liable to cover chargebacks, as well as, losing out on goods. The fraudster will make an order and pay using compromised card details, most commonly over the telephone, with goods being collected by the individual or an arranged “courier service”. We recommend ensuring that if ever goods are collected, a customer present transaction is made. Furthermore be wary of customers that offer to arrange a courier service or a friend/relative to collect. Below are some indicators to look out for:

• The initial order is often of large quantity, potentially a higher value than you would process normally.
• When attempting to process the transaction, you may be asked to “split down” the payment amount into smaller amounts and potentially different cards.
• It is likely that there be some declined transactions during this process.
• After the payment has been made, the customer will ask if a friend/relative can come and collect the goods for convenience OR that they have arranged for a courier company/taxi to come and pick up the goods.
• For further information on this particular scam please visit: www.worldpay.com/uk/support-sme-support-security/reducing-fraud

ABUSE OF MANUAL AUTHORISATION PROCESS

It has come to our attention that merchants are receiving chargebacks due to customers abusing the manual authorisation process. This scam can occur when a customer enters their pin and keeps hold of the terminal when a “refer for authorisation” message displays. If they still have control of the terminal they could enter a fake authorisation code to force the transaction through.

• It is your responsibility to ensure the terminal is returned to you as soon as the pin is entered, by the customer.
• Make sure that you follow the normal process if the terminal prompts you to “refer for authorisation”. When attempting this scam it is likely that delaying and distracting techniques will be used. Be wary if a customer has control of the terminal for long periods.
• If an authorisation code has been manually entered into the terminal, it will state that on the receipt. If you are suspicious of a customers behaviour with the terminal, you can check this before completing the sale.
• Once the “refer for authorisation” message displays in the terminal, the only code entered must be one provided by the Streamline Authorisation team.

Worldpay (UK) Limited. Registered in England No. 07316500. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF. Worldpay (UK) Limited is authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 (No. 530923) for the provision of payment services and is authorised and regulated by the Financial Conduct Authority for consumer credit activities. Worldpay, the logo and any associated brand names are all trade marks of the Worldpay group of companies.