How to guard against fraud

AIB Merchant Services

How to guard against fraud

Over the counter transactions

Please ensure all staff accepting payment by cards on your behalf have read and understood the following guidelines which aim to reduce the possibility of fraud. These guidelines could help prevent fraudulent transactions that could result in a Chargeback Dispute to you.

Please remember that authorisation is not a guarantee of payment. If a sale appears too good to be true it probably is.

Chip and PIN

- Chip and PIN is the most secure type of transaction. Merchants are not required to make visual checks of the card, in Chip and PIN situations, as the Cardholder will retain control of the card during the transaction. Follow the prompts on your terminal at all times
- Be on guard if a Chip and PIN card is presented but the PIN is blocked or the incorrect PIN is entered. You should check that this is the genuine Cardholder as you may be at risk if you accept a signature in these circumstances
- Take care that the customer does not interfere with the terminal or PIN pad.

Non Chip and PIN

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 a transaction where the card and Cardholder are present, this will leave you open to risk of a Chargeback Dispute
- Use a Ultra Violet (UV) light to check the card as most genuine cards have special features on them that show up under a UV light – see section 3 for more information
- Check whether the number printed on the terminal sales receipt is the same as that embossed on the front of the card. This is essential for identifying a counterfeit card. Most cases of counterfeit fraud involve 'skimming' or 'cloning', this is where the genuine data in the magnetic stripe on one card is copied onto another card without the legitimate Cardholder's knowledge, often the fraudster will not take the time to re-emboss the card number on the card to match the numbers in the magnetic stripe so the fraud can be easily identified with this check
- Compare the name on the card with the signature and the signed voucher

- Check whether the signature strip on the card appears tampered with, raised or if the original signature appears to have been covered over
- Check as the Cardholder signs whether they are taking an unusual amount of time to sign the voucher.

In any of these circumstances telephone the Authorisation Centre and state code 10.

Check the Customer

- 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, for example not particularly interested in the price of the item or making hasty bulk purchases?
- Are they making small item purchases with maximum value cashback? Please ensure you have AIB Merchant Services agreement before processing any cashback transactions
- Does the title of the card match the gender of the person presenting it e.g. is a male using a card where the title is "Mrs"?
- Be wary if the customer tells you that they are having problems with their card where multiple card transactions are subsequently declined but eventually authorised for a lower value. Most genuine Cardholders are aware of the credit that is available on their cards
- A fraudster may present more than 1 card, often to find a card that will be successfully authorised. If this happens, complete additional checks to validate the transactions, check that the names on the cards presented are the same
- Under no circumstances should a card sale be split between two or more vouchers for the same card to avoid authorisation as these may be subject to a Chargeback Dispute.

Check the Transaction – is it in line with your usual business?

- Is the purchase/order substantially greater than your usual sale, for example your average transaction value is €50 but this transaction is €500?
- Has the customer repeatedly returned to make additional orders in a short period of time, possibly over several days causing an unusual/sudden increase in the number and value of sales transactions?

Remember: if the appearance of the card being presented or the behaviour of the person presenting the card raises suspicion, you must immediately telephone the Authorisation Centre and state "this is a code 10 authorisation". Answer all of the operator's questions and follow their instructions.

Split Sales with Cash, Cheque or Second Credit Card

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. They 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 Merchant Support Centre on **1850 200 417**, then select option 1.

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

Card Not Present (CNP) Fraud, including eCommerce

Please ensure you have agreement from AIB Merchant Services before making any CNP or eCommerce transactions. You will also need a separate MID for eCommerce transactions.

Accepting cards has always carried a risk and especially so when ordering goods by telephone, mail order or electronically such as over the internet. CNP transactions, including eCommerce transactions provide more opportunity for fraudsters, as the card cannot be present at the time of the purchase. Businesses that are affected by CNP and eCommerce fraud can experience costly Chargeback Disputes as well as a loss of goods or services provided.

Under no circumstances should a card sale 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.

Additionally if a customer presents more than one card for payment please take care and complete additional checks to validate the transaction.

Important: 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.

There are a number of additional checks you can make to help ensure that you are dealing with the genuine Cardholder including:

- Pre-registration – before allowing your customer to purchase goods or services online, you can request that 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. You will need them to agree to your use of their personal data, as set out in your

website's privacy policy. You must also ensure that their personal data is being processed fairly and legally and in compliance with the Card Scheme rules

- For business customers not known to you, you could 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). You could 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

Here are some danger signals to look out for 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 ie. friends of the Cardholder, taxi drivers, chauffeurs, couriers or messengers. (However, third party delivery of relatively low value goods such as flowers is acceptable)
- Insist that 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 take extra care and always 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 and insist on 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 the Merchant Support Centre for more information.

Other Fraud Considerations

Do not under any circumstances 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, you must contact the Merchant Support Centre on **1850 200 417**, then select option 1. 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 advise the Merchant Support Centre on **1850 200 417**, then select option 1.

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 calling our Merchant Support Centre who can advise or investigate.

Fraud Prevention Tools

Some businesses are more prone to fraud than others. It is your responsibility to protect your business from financial loss, it is imperative that you and your staff follow the contents of the Merchant Procedure Guide carefully at all times.

- 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 AIB Merchant Services or your PSP 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, Visa and some Laser 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.

Call: **01 218 2100**
Email: **fraud@aibms.com**
or visit **www.aibms.com**

AIBMS/PREVENTION 10/18