acceptcards®

the independent card payment specialists

Card Holder Present Best Practice Guidelines

Here at acceptcards, we are committed to helping our merchants protect their business, and their customers, from the constant threat posed by fraudsters in todays world. We want you to be comfortable with your card acceptance solution and to fully benefit from the advantages it provides. As a merchant it is important that you understand the best practices to follow in order to protect not only card holders, but also your business. Preventing fraud is without a doubt one of the biggest challenges faced by business today. If you are a merchant who has access to, or stores card details in any format, or if you use a service provider who does, it is your responsibility to ensure that your customers' payment details remain secure.

Card Holder Present Transactions

Card holder present transactions are those where the card and the cardholder are present at the point of sale. Card holder present transactions processed with a chip and a pin are the most secure method for taking a card payment, providing you take good care to ensure the card is genuine and follow the guidelines below. You should always maintain possession of the card until the transaction has been completed.

- Check Card Details - Does the card appear genuine?
- Embossing - the card numbers should be raised, clear and straight.
- Visa and MasterCard have the first four card numbers printed under the embossing.

  Note - The numbers are often mismatched or altered on counterfeit cards
- Check expiration dates on all credit cards and never accept an expired credit card.
- Ensure the number embossed on the front of the card matches the truncated number on the receipt.
- Does the name match the customer? Does the gender of the presenter match the name printed on the card? Ask for photo ID to confirm details if you're suspicious.
- Check the front and back to ensure the card contains the following details:

  - Card Issuer's logo
  - Cardholder name
  - Card number
  - Expiry date
  - Signature
  - CVV2/CVC2 – The 3 digit value located on or near the signature panel of the credit card.
    * Holograms should appear three-dimensional and change colour when tilted.

- Always insert the card. Never manually enter the credit card number when the card holder is present. Take extra caution if the customer requests you to manually key a transaction.
- Do not accept declined transactions or split a declined transaction into smaller amounts.
- Be on the alert for counterfeit cards. Check the chip on the card to ensure that it is embedded in the card and not protruding on the surface. You can conduct a simple test by running your finger across the surface of the chip.
- Beware of customers who present a card not in their name and when questioned advise that it is their partner's or friend's card.
- If the customer does not cooperate or the details do not match, do not proceed with the transaction and ask for another form of payment.

In the event that a customer or transaction appears suspicious, before deciding whether or not to proceed with the transaction, you should contact your merchant service provider and ask them to check the details for you. Further information on securing your card terminal is provided on page 3 of this guide.

Card Holder Not Present Transactions

Card holder not present transactions are those where neither the card nor the cardholder are present at the point of sale, such as internet or mail order/telephone order purchases. Merchants who accept card not present transactions face a higher risk of becoming victims of fraud as the anonymity of these transactions make them an appealing target for fraudsters. The following tips will help reduce the possibility of fraudulent card not present transactions:

- Obtain as much information as possible: The credit card number, name of bank, full name, address, expiry date, CVV2/CVC2 and contact telephone number (including landline).
- Use AVS to confirm the card holders address details wherever possible.
- If processing the transaction via a terminal ensure you enter the card details correctly as per the operating guides for MOTO transactions. See further information regarding securing your terminal on page 3 of this guide.
- Call the customer on the quoted contact telephone number to confirm details of the order, especially for large and/or suspicious orders.
- Request further identification such as a photocopy of the front and back of the card. This will ensure the person has the card in their possession. Ensure it is a genuine photocopy, not a photo shopped image.
- If you take payments via a website, contact your gateway provider and see if they have any fraud prevention software which you can utilise.
- Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery, etc.
- Always obtain authorisation for all card not present transactions, regardless of value, and for the full amount of the transaction. Remember, an authorisation only confirms that funds are available at the time of the call and that the card has not been reported lost or stolen. It does not guarantee that the person quoting the card number is the owner of the card or is entitled to use the card.

Unusual Circumstances and Potentially Fraudulent Behaviour to look out for….

- Items ordered of an unusual quantity or multiple orders of the same item.
- Big ticket items or orders that are larger than normal for your business.
- Orders requested as urgent or for overnight delivery.
- When orders are cancelled and customer is requesting a transfer of money to a card or method other than back to the original credit card. (E.g. Money order, money transfer). This is not permitted.
- Different cards are provided (including different cardholder names) but same delivery address given.
- Multiple cards are presented.
- If they do give you multiple card numbers look at the actual numbers, are the first 12 digits the same then they change the last four? For example you have been given three cards:

  51232 1234 1145, 5123 5432 1234 5269, 5123 5432 1234 8537 - Notice the card numbers only vary by the last 4 digits.
- Email messages written in poor or childlike English.
- Multiple transactions charged to one card over a short period of time.

  * Exercise caution when taking foreign orders, such as orders from Asia, the Middle East and Africa which may present a higher risk.

3D Secure – The Online Authentication Tool

3D Secure is an online service designed to make online shopping transactions safer by authenticating a cardholder's identity at the time of purchase. This service is known as Verified by Visa and MasterCard SecureCode. A transaction using Verified by Visa/SecureCode will redirect cardholders to the website of their card issuing bank. The cardholder may then be requested by their bank to enter a password to be authenticated. If a customer is not registered with 3D Secure then they are still able to make a purchase from you website. Following confirmation, the window disappears and the cardholder is returned to the checkout screen. If the cardholder is not confirmed, the transaction will be declined. Participating merchants are protected by their merchant service provider from receiving certain fraud-related chargebacks.

Remember, the liability for all card not present transactions rests with the merchant. Therefore the more information you gather to satisfy yourself that the transaction is valid the more chance you have of identifying fraud and reducing the chargeback risk.

Other Important Information – Fraud Prevention

Securing your terminal

Your card terminal is equipped with a number of in-built security features which are designed to protect your customers' information. By implementing the recommended best practices below, you can protect your business, your customers and your reputation from credit and debit card fraud or misuse.

- Always ensure that terminals are secure and under supervision during operating hours, do not leave terminals unattended.
- Ensure that only authorised employees have access to your terminals and are fully trained on their use when closing your store or kiosk, always ensure that your terminals are securely locked and not exposed to unauthorised access.
- Never allow your terminal to be maintained, swapped or removed without advance notice from your merchant service provider. Be aware of unannounced terminal service visits.
- Only allow authorised personnel to maintain, swap or remove your terminal, and always ensure that security identification is provided.
- Inspect your terminals on a regular basis, to ensure that the terminal casing is whole with external security stickers remaining unbroken and of a high print quality.
- Ensure that there are no additional cables running from your terminal
- Make sure that any CCTV or other security cameras located near your terminal(s) can't observe Cardholders entering details.
- It is important to notify your merchant service provider immediately if:
- Your terminal is missing
- You, or any member of your staff, is approached to perform maintenance, swap or remove your terminal without prior notification from your merchant service provider and/or security identification is not provided
- Your terminal prints incorrect receipts or has incorrect details
- Your terminal is damaged or appears to be tampered with.

.

Delivery of goods

A common area of fraudulent transactions is allowing someone, particularly a third party, to pick up the goods from your store after a telephone order has been placed without the card being presented. Deliveries should always be made by your carrier or by a reputable courier engaged by you, not by your customer.

For deliveries the following procedures are recommended:

- Ensure the person making the delivery delivers the goods to a person inside the premises, not someone waiting outside.
- The deliverer should always obtain the signature of the person taking the delivery.
- Never deliver to car parks or parks.
- Try to deliver only to physical addresses, take extra caution when delivering to hotels and PO BOX addresses.
- Be wary of orders going overseas, recent fraud trends have indicated Africa and Asia fraudsters targeting merchants with stolen credit card numbers.
- Sight the card wherever possible upon delivery of the goods.
- Check internet maps and street views to verify business.

Refunding

You are not permitted to:

- Refund a transaction back to a card other than the one used to make the original purchase.
- Send the refunded amount to the customer via the Internet, money order or international money transfer.
- It is also beneficial to monitor all refunds processed. An increasingly common form of fraud involves employees processing refunds to their own cards. Ensure only authorised staff have access to process refunds and be aware of your refund limits.
- Regularly change your refund password. Do not use a generic password such as 9999

Third party processing

Third party processing is forbidden. Third party processing is where you process a transaction on behalf of another company or person. If any transactions are deemed as fraudulent, you will be responsible for the chargeback of that transaction. Here are some typical scenarios of third party processing:

- 'If you process these transactions I will give you 15% of the total sales'.
- 'My terminal is broken and the bank can't fix it till later this week, can you please process this transaction for me as I will lose the sale?'.

Chargebacks

A chargeback is a reversal of a credit card transaction and usually occurs when a customer raises a dispute with their financial institution (also known as the Issuer) in relation to a purchase made on their credit card. A chargeback may cause the amount of the original sale and a chargeback fee to be deducted from the merchant's account. The reasons why chargebacks arise vary greatly but are generally the result of a customer being dissatisfied with their purchase or due to illegal or fraudulent activity/use of their card.

Common chargeback reasons:

- Transaction not recognised by the cardholder
- Transaction not authorised by the cardholder
- Duplicated transactions
- Cancelled recurring/direct debit transactions
- Goods/services not received or faulty
- Goods/services not as described
- No authorisation obtained
- Fraud enquiries
- Legal proceedings
- Point-of-Sale errors

The Chargeback process

1. Transaction is disputed. Cardholder raises problem with their financial institution (known as the Issuer) or the Issuer discovers a breach of the card scheme rules.

2. Issuer advises the Merchant service provider.

3. The Merchant service provider may request documentation from the merchant to verify the transaction. The merchant has a set timeframe to respond to retrieval requests, usually 14 days.

4. If the chargeback is invalid The Merchant service provider will decline the chargeback and return it to the Issuer.

5. If the chargeback is valid, the chargeback amount is debited from the merchant's account and written notification is provided to the merchant. A chargeback fee is also usually charged to the merchants account.

Important Points to Remember

- If you are suspicious, contact your Merchant service providers fraud team prior to dispatching of the goods.
- Always obtain authorisation, especially for online transactions, regardless of value and for the full transaction amount.
- Look at the decline codes on the terminal when a transaction rejects, does the code indicate the card is lost or stolen? If so retain the card.
- Is the card number valid? If not do not proceed with the transaction or accept another card.
- Do not lower the amounts, split sales or accept card after card.
- Be mindful of overseas orders.
- Never conduct third party processing.
- Store your customer's information securely. Ensure all your computer systems are password protected and data maintained on databases should be encrypted.
- Ensure all paper records are securely stored with restricted access. Never store the CVV2/CVC2 or full card track data.
- Report all security incidents.
- Train your staff. Ensure your staff are aware and vigilant of potential fraudsters.
- Be aware of what your staff are processing. Staff have been found to be involved in fraudulent activity.
- Look out for staff refunding to their own credit cards or storing unnecessary customer information.
- Be extra cautious on high risk transactions including: card not present, manually keyed or no authorisation obtained transactions.

Adopting these suggestions may help reduce fraud but will not guarantee that you will not be a victim of credit card fraud.
It is your responsibility to confirm that the purchaser is the genuine cardholder, as you may be liable for the transaction in the case of a chargeback under your merchant agreement terms and conditions. Merchants should be aware of their responsibilities under their Merchant service providers Terms & Conditions.

All in all a common-sense approach is needed, Trust your instincts, and if in doubt check with your merchant service provider or request payment by an alternative method.