User Guide

Credit card fraud protection

Best practices

tillpayments.com

What's **Inside.**

01 Reducing risk of Card Present fraud

How to reduce the risk of Card Present (CP) fraud

When the card is present at the point-of-sale, take a good look to ensure that it is genuine. Ensure that you maintain possession of the card until the transaction has been completed.

Check card details

- Does the card appear genuine? Is the embossing clear and even, and does the printing look professional?
- Check the front and back to ensure the card contains:
  - Card Issuer's logo
  - Cardholder name
  - Card number
  - Expiry date
  - Signature
  - CVV2/CVC2 – The three-digit value located on or near the signature panel of the credit card
  - Hologram (Should appear three-dimensional and change color when tilted)
- If the customer is paying with a foreign-issued card and using a signature rather than a PIN, check the cardholder's signature on the receipt against the actual credit card.
- Check expiration dates on all credit cards. 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? For example: does the gender of the presenter match the salutation of the name printed on the card? Ask for photo identification to confirm details if suspicious.

Always swipe or insert the card

Never manually enter the credit card number. Take extra caution if the customer requests you to manually key a transaction.

What to look out for

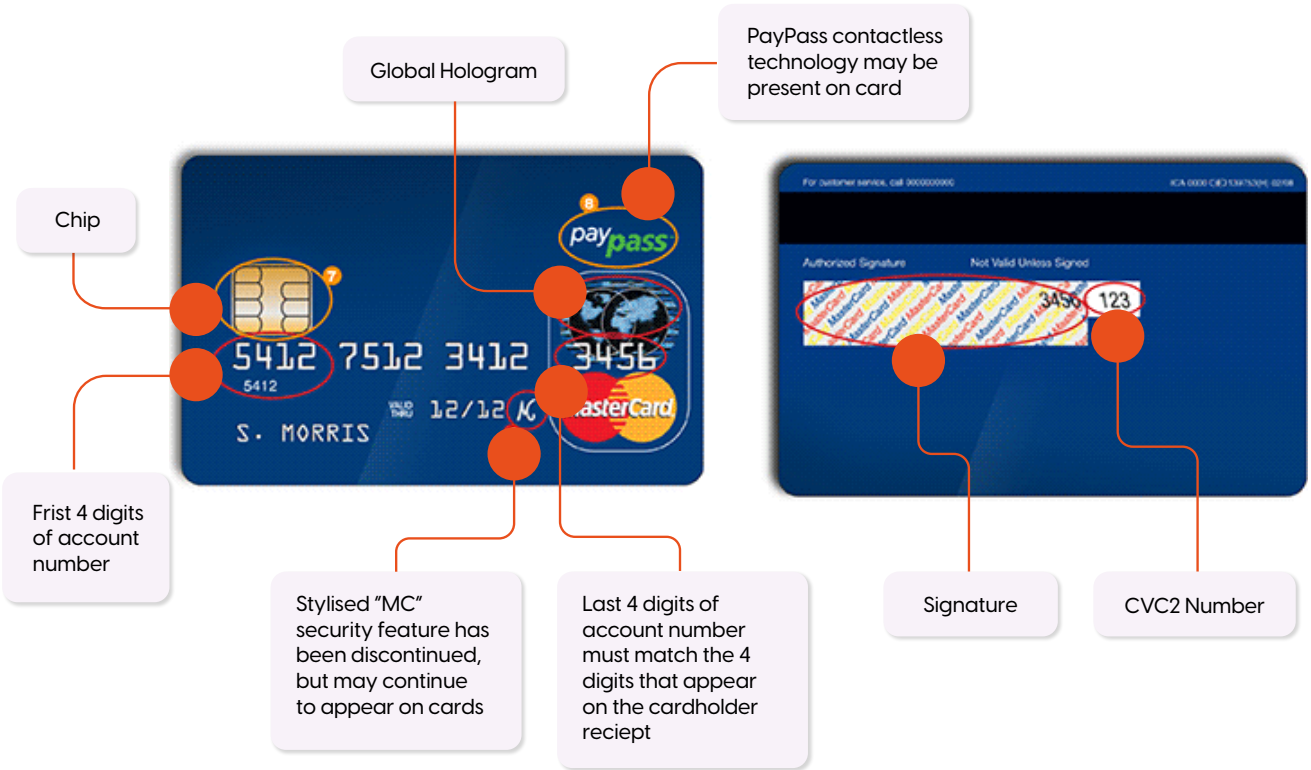
Being vigilant about unusual credit card spending can help you avoid becoming a victim of a potential fraud attack. Look out for:

- Customers who appear nervous or anxious, or hurries you at closing time.
- Customers who seem to not care about the item they are purchasing. For example, those who do not check the size or the price of an item, grab several items quickly, or do not worry about the warranty.
- Customers who request immediate delivery, that is, they want to take large and expensive items immediately.
- Customers who request you to manually key the card number.
- Multiple cards presented. Be wary of people that give you more than two card numbers, or try to split the order.
- Do not accept declined transactions. Note: Do not split a declined transaction into smaller amounts.
- If the customer does not cooperate or the details do not match, do not proceed with the transaction or ask for another form of payment. Contact TIII Payments.

Common card designs

A Visa International - Card Security Features

B Mastercard Worldwide – Card Security Features



02 Reducing risk of Card-Not-Present fraud

How to reduce the risk of Card Not Present(CNP) fraud

Card-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 card-not-present transactions make them appealing targets for fraudsters.

The following tips may 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).
- If processing the transaction via a terminal ensure you enter the card details correctly as per the operating guides for MO/TO transactions.
- Use some form of additional validations, such as the electronic white pages to cross-check details provided.
- 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. Beware of fake Photoshop images, as some of our merchants have received completely bogus cards in a JPEG format. It must be a genuine photocopy.
- If you take payments via a website, contact your gateway provider and see if they have any fraud prevention software which you can utilize.
- 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.
- Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery, etc.

What to look out for

- Items ordered are an unusual quantity or multiple orders of the same item.
- Big ticket items or orders that are larger than normal for your business. If it seems "too good to be true" it probably is.
- Orders requested as urgent or for overnight delivery.
- You are not permitted to sell items that are different from the products you normally sell.
- 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 presented. Be wary of people that give you more than two card numbers, try split the order, or if one card declines and another card is readily available.
- 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:

4876 54 **** 1145, 4876 54** **** 5259, 4876 54** ****8537**

Notice that the card numbers only vary by the last four-digits.

- Be wary of Internet orders using the generic Internet addresses using free email services.

- Email messages written in poor or childish English.
- Multiple transactions charged to one card over a short period of time.
- Exercise caution when taking foreign orders. Orders from Asia, the Middle East and Africa may present higher risk.

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. It is in your interest to ensure you have sound fraud detection steps and risk minimisation polices in place for your sales people.

03 Delivering the goods

For deliveries the following procedures are recommended:

- Ensure the person making the delivery delivers the goods to a person inside the premises, not someone outside, for example hanging around the veranda.
- 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 Australian merchants with stolen credit card numbers.
- Take a card imprint wherever possible on delivery.

Handy Hint: Check Internet maps and street views to verify business.

04 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.
- Be cautious if you are asked to refund or transfer money for an overpayment or freight charges.
- It is also beneficial to monitor all refunds processed. An increasingly common form of fraud involves employees using your EFTPOS solution to process 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 OOOO.

05 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:

Example 01

"If you process these transactions I will give you 20% of the total sales"

Example 01

"My terminal is broken and the bank can't fix it till next week, can you please process these transactions for me as I will lose the sales"

What to do if you suspect a *fraudulent transaction*

→ If you identify a lost or stolen card attempt to retain the card and call Till Payments on **347 991 5997** or the police. Your safety comes first – do not take any risks.

06 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.

Common chargeback reasons

- Transaction not recognized by the cardholder
- Transaction not authorized by the cardholder
- Duplicated transactions
- Cancelled recurring/direct debit transactions
- Goods/Services not received or faulty
- Goods/Services not as described
- No authorization obtained
- Fraud enquiries
- Legal proceedings
- Point-of-Sale errors

The chargeback process

- 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.
- Issuer advises Till Payments.
- Till Payments may request documentation from the merchant to verify the transaction. The merchant has a set timeframe to respond to retrieval requests, usually 15 days.
- If the chargeback is invalid, Till Payments will decline the chargeback and return it to the Issuer.
- 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 may also be charged to the merchants account.

07 Points to remember

- If you are suspicious, contact Till Payments prior to the processing and dispatching of the goods.
- Always obtain authorization regardless of value and for the full transaction amount.
- Do not let customers coach you on how to use the terminal; you are in charge of it, not them.
- Secure your equipment – do not leave terminals unattended.
- Look at the decline codes on the EFTPOS 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 do 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 to 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, no authorization obtained or fallback 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 Till Payments Merchant Agreement General Terms. A copy of the agreement can be found at support.tillpayments.com

Need a bit of help?
Contact us

Call **347-991-5997**

Email us at **us-support@tillpayments.com**

This user guide is intended to provide all the necessary information regarding Till Payments Merchant Portal. Our dedicated team of experts can assist you over the phone 24/7 with questions, problem resolution and extra training.

For more information, please visit **tillpayments.com**