

Avoiding Card Fraud

**Information
for Merchants**

Effective June 2013

**Business
Banking.**

**Kiwi
bank.**

Card fraud can be expensive for your business. It is a real risk, especially when the customer is not present and an order is placed by internet, phone or mail.

There are practical steps you can take to minimise the risk and cost of card fraud when you take such an order and when you store card data.

Please ensure that you and your staff read and take the steps outlined in this guide.

Processing a “card-not-present” transaction: Minimise your risk

If the customer is not physically present when a card transaction takes place, it is referred to as a card-not-present transaction. Orders placed over the phone, by mail or on the internet are examples of card-not-present transactions. These transactions carry a risk of card fraud. We strongly recommend that you and your staff follow these steps to protect your business.

1. Ask for Secure ID

You must always ask for the Cardholder Security Code (also called Card Verification Code, CVC, for MasterCard or Card Verification Value, CVV, for Visa) when processing a transaction. This is a three digit number located on the back of a Visa or MasterCard. If the customer can give you this number, it shows that the person using the card is likely to be in possession of the card at the time of the transaction.

Never store these numbers for any reason.

2. Take these precautions

- Validate each order by ensuring you have all necessary information, including the customer’s full name, full address, telephone numbers, cardholder’s bank and country in which the card was issued.
- Use your choice of courier to deliver the order – not a courier suggested by your customer.
- Never deliver goods to unattended premises. Ensure deliveries are made ‘signature required’.
- Check that the delivery country of the goods and the issuing country of the card are the same.
- Confirm suspicious or large ticket orders separately before shipping or delivery.
- Identify multiple transactions charged to one card over a very short period of time.
- If a customer places an order and says they will pick it up later, let the customer know they will need the card or some form of photo identification to collect the merchandise.

- Deliver and maintain a customer database in accordance with Payment Card Industry Data Security Standards (PCI DSS). Use this database to track buying patterns and identify changes in buyer behaviour.

3. Watch out for these warning signs

You and your staff need to identify the warning signs of potential fraud.

Take extra care with internet and mail/telephone orders having any combination of the following warning signs:

Card options

- The card authorisation is declined and a second card is readily available.
- The card numbers used are similar or in sequential numbers e.g.
4557 0220 0000 0010
4557 0220 0000 1252
4557 0220 0000 1562
- Orders are shipped to a single address but billed to multiple cards.
- Multiple orders using one card or similar cards with a single billing address but multiple shipping addresses.
- A number of declined transactions before an approved one.
- The total amount is split over numerous cards.

Cardholder's details

- Orders from internet addresses using free email services (e.g. Hotmail, Yahoo, Gmail etc.) or with domain names that can be set up by anyone.
- The customer should know which bank has issued the card. If they do not, you should not proceed with the order.
- The initiator of the order admits it is not their card being used.
- Orders where the address the goods are to be sent differs from the cardholder's address.
- Phone orders, where the cardholder says a friend, relative, employer will come in to pick up the goods.
- Limited personal and contact details are provided by the customer.

Shipping details

- Urgent delivery is requested – especially when the customer isn't concerned about additional delivery costs.
- Shipped to an international address.
- Orders shipped to a country with which you do not normally deal.
- Orders shipped to a country where the goods would be readily available in the local market.
- Orders shipped where the shipping destination country is different than the country where the card is issued.
- Orders with high shipping charges.

Transaction amounts and volumes

- Large one-off purchases that allow a fraudster to minimise the possibility of identification.
 - Larger than normal orders that could maximise the use of stolen or counterfeit payment card accounts.
 - Orders consisting of multiples of the same item or big-ticket items.
 - Orders where an extra amount is charged to the card and the cardholder requests the additional amount to be transferred via a money transfer service.
 - Orders where the transaction is cancelled and the cardholder requests the refund be processed to another card, bank account or via a money transfer service. **Note: All refunds must be processed to the card number that the original purchase was charged to.**
 - Multiple transactions charged to one card over a short period of time.
-

Don't be afraid to decline a sale if you are suspicious – it may save you money.

4. Your merchant liability

If you as a merchant accept and process a transaction when the card is not present (“card-not-present”) and it later turns out to be a fraudulent card, you are liable for the transaction under the terms and conditions of your Kiwibank Merchant agreement. The transaction can be charged back to you and Kiwibank may debit your nominated account.

When accepting an internet or mail/telephone payment by Visa or MasterCard, you must obtain authorisation for all transactions regardless of the value.

5. Authorisation is no guarantee

Minimising card fraud requires more than just seeking authorisation of a card transaction. Authorisation does not guarantee payment because it does not guarantee that your customer is the legitimate owner of the card. Authorisation is an automated process that occurs when a card transaction is processing that simply confirms that the card is valid, funds are available at the time you obtain an authorisation and the card has not, at that point, been reported lost or stolen.

Storing card details: Payment Card Industry Data Security Standards

The Payment Card Industry (PCI) has developed the Payment Card Industry Data Security Standards (PCI DSS) to protect stored cardholder data, including protection from fraudulent use. All merchants who store card details must comply with these standards.

Some basic steps to follow are:

1. Never store payment information in a readable form on your computer server.
2. Avoid storing card details in paper form. If card numbers and expiry dates must be stored, they should always be stored securely.
3. The Secure ID (CVC or CVV) should never be stored for any reason.
4. Limit employee access to sensitive data and payment systems.

For more information about PCI DSS and your full responsibilities, visit <https://www.pcisecuritystandards.org>

Contact information

If you experience card fraud, please contact us immediately. If the goods in question are still in transit, try to stop the delivery and arrange for the goods to be returned to you.

For more information or to discuss card fraud, please contact 0800 233 824.

For up to date global information on card fraud, you can visit the following websites:

- scambusters.com/creditcardfraud
- consumer-ministry.govt.nz
- visa-asia.com/ap/nz/merchants/riskmgmt/cardaccept_notpresent.shtml

How we can assist

Merchants may be contacted from time to time to be made aware of potentially fraudulent transactions and to discuss these transactions. However, all merchants should have their own procedures in place to prevent such transactions being processed.

All You Need.

Kiwibank offers a range of accounts and services to suit your needs. To find out more:

 | **Call us**

0800 601 601

 | **Visit us**

At your local Kiwibank

 | **Go online**

kiwibank.co.nz/business

Kiwibank Limited
Private Bag 39888
Wellington 5045

BR5203 JUN13

**Kiwi
bank.**