Kiwi bank.

INFORMATION FOR MERCHANTS

HE PĀRONGO MĀ NGĀ KAIHOKO

Avoiding Card Fraud

Effective November 2023

As part of our identity, Kiwibank worked with multi-disciplinary Māori artist Tristan Marler (Manawa Tapu) to design a set of tohu (cultural motifs or symbols) that represent attributes of our brand and of a thriving community.

Kia Manaaki - Show Heart and uses the Pātiki tohu. Pātiki communicates balance between people and environment to produce a thriving, resilient community that can manaaki, or care, for others.

Contents
Ihirangi

Effective November 2023

Card fraud can be expensive for your business. It's a real risk, especially when the customer isn't 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 an order and when you store card data.

Make sure that you and your staff read the steps outlined in this guide carefully and put into action where appropriate.

1. Minimise your risk when processing a "card-not-present" transaction

A card-not-present transaction happens when a customer isn't physically present when a card transaction takes place – for example, an order placed over the phone, online, or via mail. As these transactions carry a higher risk of card fraud than when a customer is physically present, we recommend that you and your staff follow the below steps to protect your business.

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 card numbers for any reason.

Take these precautions

To help protect yourself and your business when taking card-not-present payments (e.g. online), ensure you have the below information captured at the time of sale to respond to a fraud dispute:

- Customer name and email address
- The IP address of where the payment was made from
- Confirmation of purchase (what the customer ordered, e.g. a detailed invoice)
- Login details, if relevant
- The device ID the payment was made from
- All dated correspondence to/from the customer.

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

- Validate each order by ensuring you have all necessary information, including:
  - the customer's full name and address,
  - the customer's telephone number(s),
  - the customer's bank, and
  - the country the card was issued from.
- Use your choice of courier to deliver the order, not a courier suggested by your customer.
- Use track and trace where possible when sending a customer purchased goods/items. The goods need to be with the customer within 15 calendar days of the payment (excluding preorders).
- Never deliver goods to unattended premises. Ensure you only send "signature required" deliveries.
- 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.

- Identify and investigate where appropriate multiple transactions charged to one card over a very short period of time.
- If a customer places an order and says they'll pick it up later, let the customer know they'll need the card or a valid 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.

Watch out for 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 below 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.

Customer'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 don't, you shouldn't proceed with the order.
- The initiator of the order admits it isn't their card being used.
- Orders where the delivery address for the goods is different from the customer's address.
- Phone orders where the customer specifies that a friend, relative or employer will pick up the goods.
- Limited personal and contact details provided by the customer.

Shipping details

- Urgent delivery requested – especially when the customer isn't concerned about additional delivery costs.
- Orders shipped to an international address.
- Orders shipped to a country you don't normally ship to.
- Orders shipped to a country where the goods would be readily available locally.
- Orders shipped where the shipping destination country is different from the country where the card was 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 customer requests the additional amount to be transferred via a money transfer service.

- Orders where the transaction is cancelled and the customer 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're suspicious – it may save you money.

2. Your merchant liability

As a merchant, if you accept and process a transaction when the card isn't present ("card-not-present") and it later turns out to be a fraudulent card, you're 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.

3. Authorisation is no guarantee

Minimising card fraud requires more than just seeking authorisation of a card transaction. Authorisation doesn't guarantee payment because it doesn't 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 that the card hasn't, at that point, been reported lost or stolen.

4. 3D Secure for e-commerce websites

3D Secure is an additional layer of security that helps make online shopping transactions safer by authenticating a cardholder's identity at the time of purchase. It's provided by Visa as 'Verified by Visa', and by Mastercard as 'Mastercard SecureCode'.

How 3D Secure works

3D Secure adds an additional step to the authentication of online payments. To complete a transaction using a credit or debit card, a cardholder must provide additional proof of identity, such as a password or other information only known by the cardholder. The bank of the card used holds control over what details are needed to verify the cardholder.

Benefits of 3D Secure

- Blocks fraudulent transactions at the online checkout before goods are sent or services provided.
- Helps protect against chargebacks claimed as unauthorised by the cardholder.
- Increases customer confidence in the safety of e-commerce sites.

Even with the added protection of 3D Secure, it's still important to have strategies in place to prevent fraud.

5. Additional tips to avoid disputes

Here are a few additional suggestions to avoid other possible instances of dispute.

General

- If you agree to refund a customer, reference the first six and last four numbers of the card to be refunded, and the amount to be refunded. Once the agreement has been made you generally have 15 calendar days to complete the refund.
- In cases where a customer gives more than one card number and one works and the other fails and they request a refund, you should consider declining and request that the customer completes a chargeback with their bank instead.
- If you cancel an order for goods or a service, you may need to refund the customer or release a pending authorisation as soon as possible.
- Ensure that the terms and conditions you provide to customers are updated and reviewed often.

Car rentals

- For car rentals and damage, you may need at least two quotes from different repair companies. Send the quote for the smaller amount to be charged and notification of the charge to the customer to review via email. You'll need to allow the customer at least seven days to accept the amount to be charged to the card in writing.

Traffic violations

- For traffic violations, e.g. parking and speeding fines, the infringement needs to be sent to the customer via email seven days before the card is charged.

Accommodation

- If your business is for accommodation and a customer doesn't show up, the card schemes allow you to charge one night for a no-show charge. For example, if a customer books for a five night stay and they don't show up, you can charge for one night.

6. 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 customer 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 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.org/category/credit-cards
- consumerprotection.govt.nz
- visa.co.nz/support/small-business/fraud-protection

How we can help

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 from being processed.

All you need

Kiwibank offers a full range of accounts and services to suit your needs.

To find out more:

Call us

0800 601 601
and +64 4 803 1646 from overseas

Visit us

At your nearest Kiwibank.

Go online

Kiwibank.co.nz/business

Kiwibank Limited
Private Bag 39888
Wellington 5045
Kiwibank.co.nz

BR5203