BNZ Merchant service guide

Your guide to using your BNZ Merchant facility

May 2024

Table of contents

Welcome to the Bank of New Zealand

Thank you for choosing BNZ as your merchant facility provider. This Merchant Service Guide is designed to help you become familiar with the day-to-day operation of your merchant facility.

We recommend you and your staff read this guide thoroughly and keep it handy for future reference. Although there are requirements in this guide you must comply with, it should be read alongside your Merchant Agreement – Master Terms and Conditions, and your Letter of Offer.

This Merchant Service Guide forms part of your agreement with us for merchant facilities and may be varied or replaced by us from time to time by written notification, which may be provided by mail, e-mail, or through our website.

Getting started

How to contact us

For merchant enquiries, please contact our Merchant Hub on **0800 737 774**, or send an email to bnz_merchantpayments@bnz.co.nz
We're available Monday–Friday, 8:30am–5pm (closed on national public holidays).

BNZ postal address:

BNZ
Private Bag 39806
Wellington Mail Centre
Lower Hutt 5045

Your responsibilities as a BNZ Merchant

To fulfil your responsibilities as a BNZ Merchant, you must:

- follow the instructions in this Merchant Service Guide
- only process transaction types that we have approved you to process. These are detailed in your Letter of Offer
- check your merchant statement regularly and notify us of any irregularities
- accept and validate all nominated payment types presented for payment – see page 6 for more information
- ensure that the cardholder authorises all transactions by using biometrics, PIN, or signature, unless the transaction is a contactless transaction less than $200.00, or is a mail/telephone order
- ensure that the cardholder authorises all internet transactions by using biometrics or 2-factor authentication steps
- do not split the cost of a single transaction between two or more sales to avoid authorisation limits
- do not give cash out with credit card transactions (including refunds)
- do not impose a minimum or maximum amount on transactions
- retain paper or electronic records of all transactions in a secure place for 18 months and then securely destroy
- be alert to possible fraud and report all instances to us
- ensure the logos of cards you are approved to accept are displayed clearly at your point of sale
- process all transactions in NZD unless you have been approved to accept transactions in other currencies
- never store the card security code (the 3-digit security code on the reverse of the card)
- never use your own card for a purchase through your merchant facility unless it is for a genuine purchase of goods
- never use your merchant facility to transfer funds between your own accounts
- never process a transaction for anything other than the business activity the merchant facility is approved for
- never process a transaction for more than the value of the goods or service, inclusive of a surcharge, you are providing
- always process refunds to the original card used for the transaction
- if a card is accidentally left behind on your premises, you must retain the card in a safe place for a period of two business days, and hand the card to the claimant only after having established the claimant's identity. If the card is not claimed within two business days, please contact the issuing bank, or destroy and securely dispose of the card.

Settlement, service fees and statements

Settlement procedures

Settlements for your card transactions will be deposited into your nominated account daily.

For information on settlement procedures, refer to bnz.co.nz/merchantsettlements

Understanding merchant service fees (MSF)

Merchant service fees (MSF) are charged to cover the cost of processing transactions through your merchant facility. BNZ does not charge MSF for EFTPOS transactions where a customer inserts or swipes their New Zealand card and selects CHQ or SAV. To learn more about Merchant Service Fees, please visit bnz.co.nz/AboutMSF

Understanding your statement

Merchant statements are sent out each month. The statement itemises charges relating to transactions you have processed through your merchant facility. It is your responsibility to regularly check your merchant statement and report any inconsistencies to BNZ.

An example of a Merchant statement showing split pricing.

Volume summary

1	2 No. of transactions	3 Sales value	4 No. of refunds	5 Refund amount	Net value of transactions	6 Rate	7 Service charges
Domestic Debit Contactless	227	$3,304.25	0	$0.00	$3,304.25	0.70%	$23.13
Domestic Standard	83	$1,360.50	0	$0.00	$1,360.50	1.50%	$20.41
International	127	$2,057.00	0	$0.00	$2,057.00	2.95%	$60.68
Amex	17	$287.00	0	$0.00	$287.00	1.50%	$4.31
Asia Payments	0	$0.00	0	$0.00	$0.00	1.50%	$0.00
TOTAL	**454**	**$7,008.75**	**0**	**$0.00**	**$7,008.75**		**$108.53**

Figure 1: Rates are indicative and subject to change

8

Transaction summary

Date	Deposit amount
01 January	$293.00
02 January	$204.00
03 January	$440.00
04 January	$192.00
05 January	$308.00
06 January	$330.00
07 January	$143.00
08 January	$225.50
09 January	$226.00

9

Domestic Debit Contactless

	No. of transactions	Value of transactions
V DR Electronic	189	$2,667.75
M DR PayPass	11	$304.50
M DR Tokenized Contactless	2	$55.00
M DR PayPass Micro	25	$277.00
TOTAL	**227**	**$3,304.25**

1. The type of card accepted
2. Number of sales by card type
3. Value of sales by card type
4. Number of refunds conducted
5. Amount of refunds processed
6. Rate of service charge
7. Amount of service charge
8. Daily transaction summary
9. Breakdown of card type by transaction number and value

For a breakdown of the various transaction notations, refer to below table:

Abbreviation	Description
V	Visa
M	Mastercard
DR	Debit
CR	Credit
CP	Card present
PP	Prepaid
Micro	$15 or less
PayPass	Mastercard contactless product

Accepting and validating cards

Which cards can I accept?

You must accept all valid nominated payment types your facility has been approved for. Appropriate industry limits may apply. For more information, contact the Merchant Hub.

Getting paid

Processing transactions

Payments can be taken in person or online depending on your business needs. This will be discussed with you during the application process, and your facility approval confirmation will identify the card types and transaction types you have approval to process.

Authorisation

All transactions must be authorised. An authorisation is an automated response code, or message, providing confirmation that at the time at which a transaction is processed, the card has not been reported lost, stolen, or blocked for use and that there are sufficient funds available to cover the cost of the transaction. An authorisation does not guarantee payment - if later the transaction is found to be an invalid transaction, it may be charged back to you. See page 11 for more information on chargebacks.

Mobile wallets

A mobile, or 'virtual' wallet, acts like a physical wallet, but rather than containing plastic cards, card numbers are digitised and stored securely in mobile wallet apps on devices. Mobile wallets provide a convenient way for customers to make in-store payments and can be used anywhere that accepts contactless transactions. Some mobile wallets can also be used for making purchases online.

If your EFTPOS terminal accepts contactless transactions, you're ready to accept mobile wallets. Mobile wallet transactions may require a PIN - in most cases, the cardholder can use biometric data, passcode, or pattern on their mobile device to authorise the purchase. All transactions accepted using digital wallets incur a merchant service fee.

Taking payments in person

A card present transaction is one where the cardholder is physically present during the transaction. These transactions are processed via a point-of-sale terminal, for example an EFTPOS, PayClip, or BNZ Pay terminal, and authorised in real time. If your terminal displays the message 'accept with signature', the cardholder must authorise the transaction by signing the transaction receipt. When they have signed the receipt, compare this with the signature on the reverse side of the card.

Contactless transactions

A contactless transaction is a form of credit and debit card acceptance and requires the cardholder to hold their card over the payment device until the transaction has been processed. If the value of the transaction is less than $200, a PIN or signature is not required and an 'accepted or declined' message will appear on the payment device once the card has been tapped on the card reader. If the value of the transaction is more than $200, biometric verification, PIN, or signature will be requested to authorise the transaction. All contactless transactions incur a merchant service fee which will be set out in your Letter of Offer.

Electronic Offline Vouchers (EOV)

EOV enables your business to continue processing transactions if your EFTPOS terminal loses its connection to the payment or telecommunications network. EOV allows for emergency processing; it should not be triggered intentionally.

On most terminals, EOV is set up by default. If your terminal loses connectivity, it will ask you if you would like to switch to EOV (offline) mode where it can continue accepting purchase only transactions by swiping or inserting cards.

The cardholder will be required to sign the receipt instead of entering a PIN. You will need to validate the signature against that displayed on the card and keep hold of the receipt for 18 months. Once connectivity has been restored, your terminal will upload the stored transactions to your payment network for processing. Until the stored EOV transactions have uploaded, you must ensure no changes are made to your terminal, such as unplugging it. Should the terminal cease to function, or the software is updated before the upload process is complete, you are at risk of losing any stored transactions on the terminal. If you are experiencing issues uploading transactions to the payment network, please contact your terminal provider or your payment network provider.

There are several limits and restrictions to EOV mode, these include:

- the maximum dollar amount per EOV transaction is $300
- on the Worldline network, the maximum number of EOV transactions per EOV session is 99
- on the Verifone network, the maximum number of EOV transactions per EOV session is 200
- only one EOV transaction per card, per EOV session, is permitted on each terminal
- an EOV session on a Worldline connected terminal is restricted to a maximum of 36 hours.

The following cannot be processed in EOV mode:

- UnionPay International, AMEX cards, Alipay payments or proprietary cards (e.g. giftcards)
- contactless
- refunds, cash advances, or cash out
- internationally issued cards.

EOV limits and restrictions are governed by the card issuer, and they may impose different restrictions on their cardholders from time to time.

Taking payments online

A Card Not Present (CNP) transaction occurs when the cardholder, and their card, are in a different location to the merchant. CNP transactions can be initiated by either the cardholder or the merchant and are authorised electronically in real time. They are usually processed via an internet payment gateway, or can be manually entered by the merchant into an EFTPOS Terminal using the mail-order/telephone order (MOTO) function if your business has been approved for these types of transactions.

Mail-Order/Telephone-Order (MOTO)

If you would like to take mail-order and telephone-orders for your goods and services, you can request for 'MAN-PAN' functionality to be added to your EFTPOS or PayClip terminal. 'MAN-PAN' refers to manual primary account number entry, which allows manual entry of card details into the EFTPOS or PayClip terminal when the cardholder and card is not present. MOTO transactions can also be processed using a Virtual Terminal. A Virtual Terminal enables merchants to manually key cardholder details into a secure online portal for processing payments. If you want the ability to accept CNP transactions, including MOTO, you need to be approved by us first.

E-commerce transactions

E-commerce transactions are used for taking customer payments online through a website, using an internet payment gateway. If you want the ability to accept E-Commerce transactions, you need to be approved by us first.

3D Secure (3DS) for e-commerce websites

3D Secure verifies cardholder's identity as they shop online. This additional layer of security, applicable to Visa and Mastercard, helps prevent the unauthorized use of cards and helps to protect you from exposure to fraud. For BNZ merchants, 3D Secure is compulsory.

For more information, please refer to bnz.co.nz/3dsecure

Other transaction types

Pre-authorisations (Pre-auths)

A pre-authorisation allows a merchant to place a hold of funds on a customer's card until the good or service is provided, at which point the merchant can complete the transaction for the full amount.

For example, a hotel may use a pre-authorisation to hold funds on the customer's card to cover the cost of the stay. Once the customer has checked out, the hotel staff will complete the transaction by taking the pre-authorised funds as payment.

Note: It is a requirement to complete the authorisation. $1 authorisations are not permitted. Instead, we recommend a verification check on the customer's card. On certain terminals, this can be completed using a status check under the pre-authorisation menu.

If you want the ability to process pre-authorisation transactions, you need to be approved by us first. We also recommend discussing pre-authorisations with your payment gateway or terminal provider.

Pre-authorisation is a two-step process.

Step 1

Pre-authorisation: This holds the money that the merchant requires. These held funds are unavailable for use by the cardholder until either the transaction is completed or the hold on the funds has exceeded its expiry period. This period is set by the card issuing bank. Pre-auth transactions are stored securely in the terminal memory, or via your payment gateway; however, merchants must retain their pre-auth EFTPOS receipts in case of unforeseen hardware or software issues.

Step 2

Completion: A completion transaction is the completion of a stored pre-auth transaction. To receive payment, the merchant must complete the pre-authorisation transaction once the goods or service is provided, prior to the authorisation expiring. Pre-auth funds are generally held for up to 14 days, but the hold period can be less or more depending on the industry, merchant category code or card issuer. The completed amount can be different to the original pre-auth amount, but the completion should not exceed the authorisation amount by more than 15%. Completion transactions greater than the value of the authorisation may be declined.

Recurring transactions and account on file transactions

A recurring payment is an arrangement where the cardholder authorises (either electronically or in writing) a merchant to automatically charge their card on a recurring basis, for example paying a monthly phone bill. Payments can be made periodically depending on what the card holder and the merchant agree, and recurring payments can be a fixed dollar amount, or they can fluctuate.

They are initiated by the merchant as a CNP transaction, either through an internet payment gateway or keyed manually into an EFTPOS terminal, by selecting the recurring option, if your terminal has been enabled for this. Interchange reimbursement fees on recurring transactions can differ from the standard. For more information, refer to bnz.co.nz/interchangefees

An account on file payment can be used in cases where a cardholder agrees for their card to be retained online by the internet payment gateway for future use. While technically it is still a CNP transaction, they are initiated by the cardholder making a purchase.

Accepting recurring and account on file transactions offers several benefits to merchants and cardholders, including:

For cardholders

- earn rewards on eligible transactions by paying monthly bills
- avoid late payment fees
- setup recurring purchases/transactions with no ongoing intervention.

For merchants

- lower domestic interchange fee for recurring payments meaning merchants on Interchange Plus pricing incur a lower merchant service fee for these transactions
- ease of processing and less errors.

Note: Transactions processed as recurring and account on file need to be clearly identified by the payment gateway to ensure they are processed correctly. Contact your payment gateway for more information about these transaction types.

Refunds

As a merchant, you should let your customers know your refund policy at the time of purchase to avoid questions or disputes later. Refunds on card transactions must be returned to the same card used for the original sale. You should never give cash refunds for card transactions, and you should always provide the cardholder with a completed transaction receipt as proof that you have honoured their refund request. As a best practice, staple the slip to the original receipt so the cardholder has all related documents together.

All EFTPOS terminals are capable of processing refunds but usually require the use of a refund card or password to confirm the transaction. Refund cards should be kept in a secure location and only accessible by authorised staff with permission to perform refunds. If you don't have refund functionality enabled, contact our 'Merchant Hub on **0800 737 774** for more information.

Most internet payment gateways have refund capability via an online merchant portal.

Fallback mode

Fallback occurs when an EMV (chip) card is not read correctly by your terminal and the customer must swipe the card's magnetic stripe. The terminal may not read the chip for various reasons including a damaged chip or faulty terminal. If you notice this happening on a regular basis there could be a problem with the terminal, and you should contact your terminal provider for assistance.

Transacting in fallback mode carries higher risk for merchants, including a higher risk of chargebacks. Because a lower form of security has been used for processing the payment, the merchant is liable for any transactions which are challenged by cardholders as being incorrectly charged.

Surcharging

Surcharging can be applied to your terminal or website to recover the cost of your merchant service fee, in addition to the value of the sale. If you are applying a surcharge fee you must advise the cardholder and give them a chance to opt-out before processing the transaction. For information on surcharging, please refer to the procedures set out in clause 3.9 of the BNZ Merchant Agreement – Master Terms and Conditions, visit our website bnz.co.nz/AboutMSF, or contact the Merchant Hub on **0800 737 774**.

Tipping

Some terminals allow customers to add a tip on top of the transaction amount. When presented with the payment terminal, customers will be asked if they would like to add a tip and to confirm the amount. To enable tipping on PayClip, please contact us. If you have an EFTPOS terminal, please contact your terminal provider for more information.

CurrencySelect Eftpos and CurrencySelect Online transactions

CurrencySelect makes it easier for you to sell your goods and services to the world by converting your New Zealand Dollar sale price to your international cardholder's home currency at the time of sale. CurrencySelect enables you to process your Visa and Mastercard transactions in the following 12 foreign currencies:

Australian Dollar (AUD), Canadian Dollar (CAD), Chinese Yuan (CNY), Euro (EUR), Hong Kong Dollar (HKD), Japanese Yen (JPY), Korean Won (KRW), Singapore Dollar (SGD), South African Rand (ZAR), Swiss Franc (CHF), UK Pound (GBP), and US Dollar (USD).

By letting international customers make purchases in their own currency, customers will feel more at ease because they can buy in a familiar currency, and you're helping to give your business a competitive advantage. CurrencySelect gives your business the freedom to set your prices in fixed foreign currency amounts, or to calculate each currency you offer from a base currency, such as New Zealand dollars. Settlement will be made to your nominated Bank of New Zealand account in NZD. There are several benefits for both merchants and customers with CurrencySelect.

For merchants

- CurrencySelect Eftpos merchants receive a merchant service fee rebate on international Visa and Mastercard transactions that are converted to the international cardholder's home currency – payable as a lump sum payment.
- CurrencySelect Eftpos transactions are converted automatically, into the desired currency, at the time of transaction. CurrencySelect Online transactions are not converted automatically. You are required to enter the nominated transaction value into the foreign currency price.
- Improved customer service, experience, and satisfaction – the international cardholder knows exactly how much they are paying in a currency they know best – and this may lead to increased sales for you.
- CurrencySelect Eftpos merchants can access reporting via a web-based console to understand where your international customers are from, and payment trends.

For customers

- Choice of currency - provides international Visa and Mastercard cardholders with the option of paying in their home currency at the time of the sale.
- Instant knowledge – they know exactly what exchange rate has been used before choosing to pay in their home currency.
- Certainty – the amount they sign for is the amount that will be debited to their account.

To see CurrencySelect foreign exchange rates, visit bnz.co.nz/support/rates-and-fees/CurrencySelect You can also access the CurrencySelect exchange rates in XML format, giving you the ability to easily import these rates into your own applications.

For more information, call our Merchant Hub on **0800 737 774**.

Receipt requirements

Card present transaction receipts

For all card present transactions, you must provide the cardholder with the 'customer copy' of the transaction receipt. This may be in the form of a printed or digital receipt depending on the capability of your terminal. This provides the cardholder with a detailed record of their purchase from you. You must retain the 'merchant copy' of all transaction receipts in a secure location for at least 18 months.

Card not present transaction receipts

For an e-commerce or MOTO transaction, you must send the cardholder a copy of the receipt immediately following completion of the transaction. The receipt may be sent by e-mail, text message, or post. If a link to a website is provided, you must provide clear instructions to the cardholder for accessing the receipt on the website. It is best practice to always provide customers with a receipt which includes the business name, company number, the date of supply, the product or service, the price, and clearly outline your returns process, and any other terms and conditions.

Business protection

Chargebacks and disputed transactions

There may be times when it is necessary for us to reverse a previously accepted transaction. This is referred to as a chargeback. A chargeback occurs when a cardholder (or their bank) raises a dispute about a transaction processed by you.

Chargebacks, depending on the card scheme, chargeback reason, and business, can occur between 60 and 540 days post the date of the transaction, or the date the goods and/or service were expected to be received by the cardholder. For this reason, you must retain receipts for the prescribed 18 months.

You and your business are financially liable for all chargebacks. If the dispute is resolved in favour of the cardholder, the transaction is charged back to you and the value is debited from your nominated bank account(s). As the merchant, you could possibly lose the value of the sale as well as incur a chargeback fee.

Information regarding this type of transaction is covered in your Merchant Agreement Master Terms and Conditions. We have also included a list of common chargeback reasons and recommended action below.

There are times when the Bank requests documentation to support transactions processed by you. We require a response within five business days to these requests. Failure to do so may result in a legitimate transaction being debited (or charged) back to you.

Note: Never re-process a transaction that has been charged back as a new sale. This violates card scheme regulations and could lead to the termination of your merchant facility.

It is important to keep a copy of all documentation you forward to us as a precaution against the documents being misplaced or lost in transit between yourself and us. If you have any questions about chargebacks, please call our Disputed Transaction Team on **0800 930 110**.

Chargeback guide

The following table details common chargeback reasons and strategies to avoid chargebacks.

Chargeback reason	Reason chargeback occurred	How to avoid future chargebacks
Cancelled recurring transaction	The cardholder was charged for a recurring transaction despite cancellation notification	Ensure recurring transactions are cancelled on receipt of notification
Card expired at the time of sale	The card used by your customer had expired at the time of the sale	At the time of sale check the card to ensure that it has not expired
Cardholder cancelled merchandise	The cardholder cancelled the merchandise order, and a credit was not processed to their account	Cancel the order upon request and process a credit to the cardholder's account
Counterfeit transactions	A counterfeit card was used	Identify the authenticity of the card prior to processing transactions
Credit voucher not processed	A credit/full credit was not issued	Process a credit/full credit to the cardholder account
Defective merchandise or not as described	The merchandise sent to the cardholder was damaged or defective or differs to what they ordered	Resolve the dispute with the cardholder when a call is first initiated to your company
Duplicate processing	A single transaction was processed more than once	Ensure transactions are processed only once
Late presentment	The transaction was not processed within the required time frame	Process sales within 30 days of the transaction date
Fraud – card not present environment or no cardholder authorisation	The cardholder denies participation in this transaction	Identify the authenticity of the cardholder prior to processing transactions

Missing signature	A signature or PIN was not obtained at the time of the sale	Obtain the cardholder's signature/PIN at the time of the sale
Non-receipt of merchandise or services not rendered	The cardholder states they have not received the goods or services they paid for	Ensure that the goods or services are provided to the customer prior to billing
Requested transaction receipt not received	A photocopy of the requested item was not returned to us within the application time frame	Supply a copy of the sales slip as specified in the retrieval request letter within the specified timeframe
No authorisation	The required authorisation was not obtained	Obtain an authorisation on all sales

Preventing card fraud

It is an unfortunate fact that not everyone with a card, or card number, is the card's rightful owner. Card fraud is a reality, especially when the customer is not present, and the order is placed by internet, phone, or mail order. However, there are practical steps you can take to minimise the risk of it happening to you. We recommend that you and your staff read and follow the steps contained in this Merchant Service Guide to prevent you from being a victim to card fraud.

Merchant liability

If you as a merchant accept and process a transaction in a card-not-present environment and it later turns out to be a fraudulent card, under the terms and conditions of your merchant agreement with BNZ, you are liable for the transaction. The transaction can be charged back to you and BNZ may debit your nominated account. When accepting an internet or mail/telephone payment by Visa, Mastercard, or UnionPay, you must obtain authorisation for all transactions regardless of the value.

Minimise your risk

To minimise your risk, you need to identify characteristics that indicate potential fraud. When any of the warning signals listed in this Merchant Service Guide occur and the cardholder is not present, you must take care to avoid becoming a victim of a fraud attack. We recommend you undertake these best practices to protect yourself against losses.

Card Security Code

Always request the three or four-digit Card Security Code when processing a transaction.

- (CVV2) for Visa
- (CVC2) for Mastercard
- (CVN2) for UnionPay
- (CID) for American Express

Never store these numbers for any reason.

Authorisation is not enough

Minimising card fraud means more than just seeking authorisation of a card transaction. Why? Because authorisation does not guarantee payment, and it does not guarantee that your customer is the legitimate owner of the card. It simply confirms that the card is valid, funds are available at the time you obtain an authorisation, and the card hasn't, at that point, been reported as lost or stolen.

Fraud warning signs

Beware of internet and mail/telephone orders with any combination of the following characteristics.

Card number related fraud	Shipping related fraud
The card authorisation is declined, and a second card is readily available.	Orders shipped rush or overnight to deliver items as soon as possible for quick resale.
The card numbers used are strikingly similar or in sequential numbers, e.g. 4557 0220 0000 0010, 4557 0220 0000 1252 and 4557 0220 0000 1562.	Orders shipped to an international address.
Orders are shipped to a single address but billed to multiple cards.	Orders shipped to a country with which you do not normally deal with.
Multiple orders on one card or similar cards with a single billing address but multiple shipping addresses.	Orders shipped to a country where the goods would be readily available in the local market.
Several declined transactions before an approved one.	Orders shipped where the shipping destination country is different than the country where the card is issued.
The total amount is split over numerous cards.	Orders with high shipping charges.

Cardholders details	Transaction amounts/volumes
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.	Large one-off purchases that allow a fraudster to minimise the possibility of identification .
The initiator of the order admits it is not their card being used.	Larger than normal orders that maximise the use of stolen or counterfeit payment card accounts.
Orders where the address the goods are to be sent differs from the cardholder's address.	Orders consisting of multiples of the same item or big-ticket items.
Phone orders, where the cardholder says a friend, relative, employer will come in to pick up the goods.	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 e.g. Western Union, or any other third party.
	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.

Security measures

It is important you follow good business practices when processing sales. Such practices include:

- check that the delivery country of the goods and the issuing country of the card are the same
- develop and maintain a customer database in accordance with Payment Card Industry Data Security Standards, which includes their home address
- never store payment information in a readable form. Card numbers and expiry dates should always be stored securely
  - for physical storage (e.g. paper form), this includes storing in a locked or protected area or facility, with restricted access
  - for electronic storage (e.g. database, system, server, or network drive), this includes encrypting card data, restricting access to servers and logging/monitoring staff activity
- to minimise the risk of chargebacks, 3D Secure will be enabled for e-commerce sites, as it shifts the liability of the transaction from the merchant to the card issuer

Always ask yourself, do I need to keep the card number and expiry date? If the answer is no, the information should be destroyed or deleted. The card security code should never be stored for any reason.

Use this checklist to track buying patterns and identify changes in buyer behaviour:

- identify multiple transactions charged to one card over a very short period
- validate each order ensuring all information is provided, including the customer's full name, full address, and telephone numbers
- arrange for deliveries to be made 'signature required' by your choice of courier, rather than the customer's choice
- limit employee access to sensitive data and payment systems
- consider using a Captcha phrase for e-commerce transactions, to protect against automated programmes that attempt fraudulent transactions on your website.

How we assist

Merchants may be contacted from time to time to be made aware of, and discuss, potentially fraudulent transactions. All merchants should have their own procedures in place to prevent fraudulent transactions being processed and should not rely on us to detect fraud. It is your responsibility to ensure your contact details are up to date with BNZ.

Contact information

If you do experience card fraud, please contact us immediately, and if the goods in question are still in transit, try to stop the delivery and have the goods returned to you. For more information or to discuss card fraud, please contact the Merchant Hub on **0800 737 774**.

UnionPay International

UnionPay International is a major credit and debit card scheme in China. UnionPay cards are accepted at BNZ ATMs throughout New Zealand and at many BNZ EFTPOS and e-commerce merchants.

This Merchant Service Guide will help you and your staff to identify, accept, and process UnionPay transactions. We've produced it to meet the requirements of clause 3.6 of your Merchant Agreement - Master Terms and Conditions.

UnionPay card present transactions

How to identify a UnionPay card

You might not see a cardholder name and valid dates because these are optional. Also, credit cards have a hologram, while debit cards don't.

Dual-branded cards

Some banks issue dual-branded cards, which display a UnionPay International logo, and also a Visa or Mastercard logo. In a card-present or MOTO transaction, if a dual-branded card displays a Visa logo, the card is then processed as a Visa card, or if it displays a Mastercard logo, the card is then processed as a Mastercard. This happens automatically when the card or card number is presented to the terminal. In an e-commerce transaction, the cardholder selects whether a dual-branded card is processed as UnionPay, or as Visa/Mastercard, by selecting UnionPay or Visa/Mastercard as a payment method prior to entering the card details.

Warning signs

Be alert for invalid, fraudulent, or damaged cards. Before accepting a UnionPay card you need to check that:

- the card has a UnionPay logo
- there is no indication of 'Sample Card' or 'Void' on the card
- the card has not been altered or damaged in any way
- if there is a photo on the card, it matches the cardholder
- there is a signature on the signature panel
- the signature panel has not been altered or damaged in any way.

UnionPay card present transaction checklist

- Card and cardholder must be present: a UnionPay Card Present transaction can only be processed when both the cardholder and card are present at the time of the transaction.
- Use the EFTPOS terminal card reader: the UnionPay card must be swiped through or inserted into the EFTPOS terminal card reader to process a transaction.
- Verification for cards: a signature is always required and if the customer has a PIN loaded it must be entered as well.
- All cards with the Visa or Mastercard logo must be processed as credit card transactions, not cheque or savings.

Refunds

- A refund for a card present transaction can only be processed when both the UnionPay cardholder and card are present.
- Multiple refunds can be made, provided the total amount refunded is not more than the original purchase amount.
- A refund can be matched to the original transaction for up to 30 days. Refunds which can't be matched with the original purchase will need to be organised with the customer.

Pre-authorisation and pre-authorisation completions

- The completion amount can't exceed 15% of the pre-authorisation amount.
- If the completed amount exceeds 15% of the pre-authorisation amount, you need to obtain another authorisation for the additional amount.
- Pre-authorisation completion transactions must be processed within 30 days of the pre-authorisation transaction.
- Because UnionPay International gives different authorisation numbers to pre-authorisations and pre-authorisation completion transactions, two different authorisation numbers will display on your terminal receipt.

UnionPay card not present transactions

About UnionPay Online Payment (UPOP)

UnionPay Online Payments (UPOP) is the only electronic commerce gateway that gives merchants the ability to take online payments from UnionPay cardholders. UPOP provides an extra layer of security, with built in authentication of both the cardholder and card information, via SecurePay. An online portal (provided by Windcave) allows you to manage all merchant admin and reporting requirements, including processing purchases, refunds, authorisations, pre-authorisations, and completions.

Benefits

The range of UPOP payment options delivers several benefits, including:

- flexible payments improve the online shopping experience of cardholders, so UPOP helps you attract more customers and promotes your online business
- provides multiple protections for security including static verification, dynamic verification, and a private security key
- provides considerable customer education resources and business opportunities, by enhancing cardholders' confidence and trust in paying online
- offers cardholders' attractive terms for currency conversion of UPOP purchases from international merchants.

How does UPOP work?

Step 1: A cardholder places an order on the website of an online merchant by clicking the "add to cart" or "checkout" button and then choosing UnionPay Online Payments as the payment method, which initiates a transaction.

Step 2: The transaction information is forwarded to the UPOP system through Windcave PXPay2. Meanwhile, the URL of the cardholder's browser is redirected to a UPOP webpage.

Step 3: Multiple payment methods are provided on the UPOP webpage. It is up to the cardholder to choose their preferred payment method. UPOP is responsible for card number collection and facilitates authentication of the transaction once the payment method is selected.

Step 4: UPOP forwards the payment information to the card issuer.

Step 5: The issuer checks the payment information received, and will authorise or decline the transaction.

Step 6: Payment Express is notified by UPOP about the transaction result and the details are passed to the merchant so that the result can be presented to the cardholder by the merchant website.

UPOP business rules

Currency

UPOP operates in New Zealand Dollars (NZD).

Settlement

All transactions are settled to the merchant in NZD.

Refunds

Refunds can be processed for UPOP in the same way as Visa and Mastercard transactions, using the Windcave 'Payline' portal.

Payment gateway integration

BNZ uses the WindcavePXPay2 payment gateway for all UPOP processing, including connectivity to the UPOP payment pages, transaction history, and settlement. This enables our merchants the ability to accept UnionPay as well as other card types using a single integration. If you use another payment gateway already, you may choose to maintain this solution for your existing card acceptance and just add Windcave for UnionPay. Integration documentation for Windcave PXPay2 is available from Windcave.

Website requirements

To ensure that your potential UnionPay customers know that you accept UnionPay, it is important that you display the UnionPay logo in a prominent position on your site, in the same manner that you display Visa and Mastercard logos.

Registration

To access UPOP, BNZ must register your merchant details with UnionPay International and add UnionPay terms to your Letter of Offer. Contact the Merchant Hub if you would like to add UPOP to your existing merchant facility.

Special considerations for UnionPay International transactions

There are some special considerations for UnionPay International transactions, the most notable of these being Tokenisation and Pre-authorisation/completion.

Pre-authorisation/complete

Most UnionPay International cards are debit cards and most banks that issue these debit cards will decline Pre-auth transactions The Pre-auth/complete transactional model, used by many businesses such as car rental and accommodation providers, is therefore not compatible with UPOP. If your business requires the Pre-auth/complete transactional model, we do not recommend adopting the UPOP service.

Alipay

Alipay customers access Alipay via a digital wallet app on their mobile phone. To use Alipay, customers must have a Chinese bank account, so this payment method is used in New Zealand mostly by tourists and Chinese residents.

Alipay Wallet

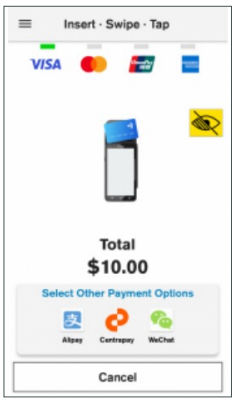
Alipay is a digital wallet app that sits on a customer's phone and replaces the need for a traditional EFTPOS or credit card. Unlike other wallets however, the customer scans a QR code generated by the ETPOS terminal to initiate a transaction. Within their wallet the customer can view the purchase amount in Chinese Yuan and authorise the payment. Alipay utilises dynamic QR codes providing extra security; a unique QR code is generated for each transaction.

Alipay transactions – how does it work?

The Alipay transaction flow uses QR codes during transaction authorisation. QR codes are two-dimensional barcodes capable of containing information.

1. The transaction is initiated in the same way as if it were a debit or credit card transaction, to the point where the payment type is selected.

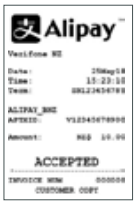
2. The 'Purchase' screen will display on the EFTPOS terminal. Customer selects Alipay logo on present card screen.

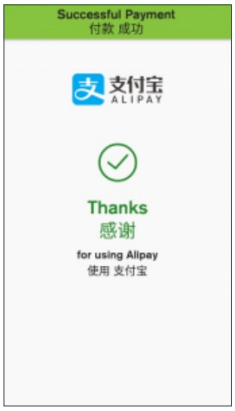


3. A transaction-specific QR code and transaction amount in NZD displays on the terminal screen.

4. Customer scans QR code with mobile device and authorises transaction in-app on their mobile device.

5. Terminal displays Approved or Declined.





If the transaction was not successful, the transaction will time out within one minute and display the Timed Out message. If the Alipay customer doesn't enter their correct PIN to authorise the transaction in their app within one minute, the transaction will time out.

If there's insufficient funds within the Alipay wallet, the Alipay app prompts the customer to top up their account. If this is not done and the transaction is not authorised within one minute, the transaction will time out.

Surcharging

You cannot charge a surcharge fee for Alipay transactions.

Refunds

You can perform Alipay refunds via your EFTPOS terminal.

If you need to refund an Alipay purchase, you will need to know two things:

1. You need to know the transaction reference number of the original purchase transaction. This can be found as the 'ALIPAY_BNZ APTXID' on the purchase transaction receipt.

   The transaction reference can also be viewed by your customer on the Alipay app.

Alipay transaction reference →

2. You need to know your 4-digit Alipay refund passcode. This information is initially given to you by your terminal provider, along with details of the process for changing it.

Here's how to process an Alipay refund via your terminal

1. Enter refund amount, tap Other, then tap Refund.
2. Enter passcode.
3. Refund amount is displayed on the screen. Tap Alipay symbol.
4. Enter 11-digit 'Auth-code' starting with a 'V' which you can find in your Transaction History or on the original transaction receipt as the 'APTXID'.
5. Your terminal processes the refund and then displays Approved or Declined.

Your EFTPOS terminal will only be able to process refunds for transactions that were made at your store and will not allow the refund value to be greater than the original purchase value (even if multiple, partial refunds are processed).

The refund may not be posted immediately to the customer's Alipay app.

Settlement procedures

You can view and access the amount on the day after the transactions were made; 7 days a week, 365 days a year.

The day period for settlement and merchant service fee charges is 4am to 4am NZST. For example transactions made Monday 4am to Tuesday 4am will be paid to your settlement account on Tuesday and the service charge will be charged on Tuesday.

Merchant service fees

All Alipay transactions incur a merchant service fee (MSF). The MSF covers costs incurred by us to process the transactions along with a BNZ margin, and is charged at a fixed rate.

The MSF for sales transactions is calculated and charged daily, on the business day after the transactions were made. It is calculated based on the total value of the transactions for the day and charged by direct debit.

The MSF for refund transactions is calculated and paid to your account for each individual refund transaction processed. This is paid by direct credit.

Merchant statements

As the MSF is charged daily, separate MSF statements will not be produced.

Reconciling POS terminal totals with settlement payments

The 'day' period for Alipay transactions is 4am to 4am NZST, and your EFTPOS terminal can produce a summary of daily settlement totals matching this timeframe. The terminal can produce totals up to 7 days in the past.

1. Swipe down from the top of the Notification bar
2. Tap the App Launcher icon
3. Tap Device Manager app
4. Tap APM Totals report from the Device Manager menu
5. Tap Get Totals to retrieve today's report, or to view any other date tap Change, select date, and then tap Get Totals Report will display count and value of Purchases and Refunds processed for the settlement period for each APM

Information contained within settlement payment transactions

1. The Name of Other party is 'Alipay/BNZ Trans CR'
2. The Particulars show the number of transactions for the day with the text 'Alipay'
3. Code shows the Alipay transaction date in DDMM format
4. Reference contains 'M' and your merchant ID

The deposit amount will match the information from the EFTPOS terminal settlement totals.

Information contained within Merchant Service Fee transactions

1. The Name of Other party is 'BNZ Merch Serv Fee'
2. The Particulars show the merchant service fee rate with the text 'Alipay'. 0150 means 1.50%
3. Code shows the Alipay transaction date in DDMM format
4. Reference contains 'M' and your merchant ID

Glossary

3D Secure means '3 Domain Server'. There are 3 parties that are involved in the 3DSecure process: the merchant the purchase is being made from, the Acquiring institution, and the card issuer.

Card scheme means Visa, Mastercard, American Express, UnionPay International, Alipay, the domestic debit scheme, or any other card scheme with whose card scheme rules we are obliged to comply.

Chargeback means the reversal of a disputed sales transaction to you.

CID means the card identification number for American Express cards. It is the 4-digit, non-embossed number printed above the account number on the face of the card.

CVC2 means the card verification code for Mastercard (3-character code printed on the signature panel of the card).

CVN2 means the card verification number for UnionPay International (3-character code printed on the signature panel of the card).

CVV2 means the card verification value for Visa (3-character code printed on the signature panel of the card).

EFTPOS means 'electronic funds at the point of sale', an electronic payment system involving electronic funds transfers based on the use of payment cards, such as debit or credit cards, at payment terminals located at points of sale.

EMV means Europay, Mastercard and Visa that is a global standard chip card technology.

EOV means 'electronic offline voucher' which is a process in which details of a transaction are read and stored by equipment, but are processed later than would be the case if the equipment were functioning normally and regardless of whether this occurs accidentally or because of a deliberate act or omission.

Interchange fee means a fee set by the card schemes and charged by banks that covers the cost of processing transactions and the credit risk inherent in a card transaction. Interchange fees are paid to the cardholder's issuing bank.

Issuer means a bank or financial institution that issues cards to consumers on behalf of the card schemes.

Letter of Offer means the letter of offer or letter of acceptance (as the case may be) we give you in connection with the merchant services.

MAN-PAN refers to Manual Primary Account Number entry, which allows manual entry of credit card details into equipment.

MOTO means a card transaction involving an order for goods or services received by you by mail, telephone, or email.

MSF means merchant service fee, the fee payable by the merchant to us for processing transactions.

PIN means the personal identification number allocated by a card issuer or personally selected by a cardholder.

QR code means a 2-dimensional bar code that is capable of containing information.

Refund card means a card that is swiped through an EFTPOS terminal to authorise a refund, designed to reduce refund fraud by only being accessible to staff with authority to perform refunds.

bnz.co.nz • bnz_merchantpayments@bnz.co.nz • 0800 737 774

(14040) BNZ191 04-24