BNZ Merchant service guide

Your guide to using your BNZ Merchant facility

December 2025

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.

This guide operates alongside other documents

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

You can contact our Merchant Hub by:

- Calling 0800 737 774 Mon–Fri, 8.30am–5pm, except national public holidays
- Emailing bnz_merchantpayments@bnz.co.nz
- Mailing us at:

  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 – 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
- Ensure that all internet transactions are authenticated by the cardholder through biometrics, two-factor authentication, or 3D Secure
- 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 or refunds
- Do not impose a minimum or maximum amount on transactions
- Retain paper or electronic records of all transactions in a secure place for a minimum of 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 a cardholder's card security code
- 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 same card that was used in the original sales transaction
- If a card is left on your premises, you must retain the card in a safe place for two business days. If the card is claimed within that time, you must only hand the card to the claimant after establishing their identity. If the card is not claimed, either contact the issuing bank or destroy and securely dispose of the card.

Settlement, Merchant Service Fees, and statements

Settlement procedures

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

For information on settlement procedures, visit 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, 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.

Examples of statements showing split pricing

The following table shows the abbreviations used for transactions.

Your Bill for February 2027

The total you need to pay is:

$108.53 (1)

This amount will be debited to your account number 02-0000-0000000-000. Unless advice to the contrary is received from you by 12 March 2027 the amount of $108.53 will be directly debited to your bank account on 15 March 2027.

Volume summary

	(3) No. of transactions	(4) Sales value	(5) No. of refunds	(6) Refund amount	Net value of transactions	(7) Rate	(8) Service charges
(2) 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

(9) **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

(10) **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**

Key:

- (1) Total charge/s payable
- (2) The type of card accepted
- (3) Number of sales processed
- (4) Value of sales processed
- (5) Number of refunds processed
- (6) Value of refunds processed
- (7) Rate of service charge
- (8) Amount of service charge
- (9) Daily transaction summary
- (10) Breakdown of number and value of sales processed by card type

Your bill for February 2027

Total service charge for this period is NZD $87.90. Unless advice to the contrary is received from you by 12 March 2027, this amount will be directly debited from your nominated bank account on 15 March 2027.

Charges Summary

Account Currency: NZD	1
Service Fee	$87.90
Total NZD	**$87.90**

Processing summary

Card scheme	3 Sales transactions	4 Sales value	5 Refunds	6 Refunds value	Net sales value
Account currency: NZD					
Mastercard	39	$1,243.00	0	$0.00	$1,243.00
Visa	261	$7,863.20	0	$0.00	$7,863.20
Total NZD	**300**	**$9,106.20**	**0**	**$0.00**	**$9,106.20**

Transaction summary

Date	Amount
Account currency: NZD	
01 September	$2,488.20
06 September	$685.50
07 September	$1,046.00
08 September	$1,360.50
13 September	$1,222.00
14 September	$1,242.00
15 September	$1,062.00

9

Summary of card transactions

2 10

Area	Card scheme description	No. of transactions	Total value
Account currency: NZD			
Domestic	MC-CR PayPass	13	$487.00
	MC-CR Tokenized Contactless	3	$99.00
	MC-DR PayPass	13	$434.00
	MC-DR PayPass Micro	3	$30.00
	MC-DR Tokenized Contactless	7	$193.00
	VISA-CR Contactless	1	$22.00
	VISA-CR Standard	24	$884.00
	VISA-Contactless	47	$1,390.00
	VISA-DR Commercial Premium	1	$17.00
	VISA-DR Consumer Electronic	151	$4,282.50
	VISA-DR Standard	34	$1,208.70
	VISA-PP Consumer Electronic	1	$10.00
International	Visa	2	$49.00
Total NZD		**300**	**$9,106.20**

Service fee

7 8

Area	Card scheme	Net sales	Rate	Total fee
Account currency: NZD				
Domestic Debit Contactless	Mastercard	$657.00	0.70%	$4.60
	Visa	$5,518.20	0.70%	$38.63
Domestic Standard	Mastercard	$586.00	1.50%	$8.79
	Visa	$2,296.00	1.50%	$34.44
International	Visa	$49.00	2.95%	$1.44
Total NZD		**$9,106.20**		**$87.90**

Figure 2: Rates are indicative and subject to change

Key:

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

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

Accepting and validating cards

Cards you can accept

You must accept all valid nominated payment types your facility has been approved for. Appropriate industry limits may apply. For more information, contact our Merchant Hub. If you wish to accept Japanese Credit Bureau (JCB) cards, you will need to speak directly with JCB to set this up.

Card number identifiers:

Different card schemes have cards that begin with different numbers.

Card number	Card scheme
2	Mastercard
3	American Express
4	Visa
5	Mastercard
6	UnionPay

Getting paid

Processing transactions

Payments can be taken in person, on the go, or online depending on your business needs. 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 (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 can 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 MSF.

Taking payments in person

In a 'card present' transaction, the cardholder is physically present during the transaction. These transactions are processed via a point-of-sale terminal, for example an EFTPOS terminal, PayClip terminal, or BNZ Pay device, 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 of the card.

Contactless transactions

A contactless transaction is a form of card payment. The cardholder must hold their card over the payment device until the transaction has been processed. If the value of the transaction is less than $200, authentication is not required and an 'accepted or declined' message will appear on the payment device. If the value of the transaction is more than $200, the payment device will ask for biometric identification, PIN or a signature to authorise the transaction. All contactless transactions incur a MSF, as set out in your Letter of Offer.

Electronic Offline Voucher (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 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. If the terminal ceases 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.

While in EOV mode, the following limits and restrictions apply.

- 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

While in EOV mode, you cannot process the following:

- UnionPay International, American Express cards, Alipay+ payments or proprietary cards (e.g. giftcards)
- Contactless
- Refunds, cash advances, or cash out
- Internationally issued cards

Card issuers may also apply other EOV limits and restrictions on their cardholders.

Manual primary account number entry

If you would like to take orders via phone or mail for your goods or services, you can ask for MAN-PAN functionality to be added to your EFTPOS or PayClip terminal. MAN-PAN allows manual entry of card details into the EFTPOS or PayClip terminal when the cardholder and card are not present.

Mail order or Telephone order (MOTO)

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. All EFTPOS or PayClip terminals are capable of processing MOTO transactions – some may require the use of a password to confirm the transaction. It is your responsibility to ensure that this functionality is only accessible by authorised staff with permission to perform MOTO transactions on your behalf. We must approve your ability to accept Card Not Present (CNP) transactions first, including MOTO.

Taking payments online

A CNP transaction occurs when the cardholder, and their card, are in a different location to you. CNP transactions can be initiated by either the cardholder or you. These transactions are authorised electronically in real time. They are usually processed via a payment gateway or can be manually entered by the merchant into an EFTPOS terminal using the manual primary account number (MAN-PAN) entry function if your business has been approved for these types of transactions.

E-commerce transactions

E-commerce transactions are used for taking customer payments online through a website, using a payment gateway. We must specifically approve your ability to accept e-commence transactions first.

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

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

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

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

Other transaction types

Pre-authorisations

A pre-authorisation allows you to place a hold on funds on a customer's card until the good or service is provided, at which point you 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.

It is a requirement to finalise a pre-authorisation you initiate. Pre-authorisations for the purpose of checking the status of a customer's card 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.

We must specifically approve your ability to process pre-authorisation transactions 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-authorisation transactions are stored securely in the terminal memory, or via your payment gateway; however, merchants must retain their pre-authorisation EFTPOS receipts in case of unforeseen hardware or software issues.

Step 2

Completion: A completion transaction is the completion of a stored pre-authorisation 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-authorisation 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-authorisation 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

Account-on-file and recurring transactions allow you to securely store a customer's payment details for future use.

Account on file transactions

An account on file payment can be used in cases where a cardholder agrees to a payment gateway retaining their card information online, for future use. This will help speed up the check-out process for any future purchases made by the cardholder.

Recurring transactions:

In a recurring payment arrangement, the cardholder authorises a merchant, either electronically or in writing, to automatically charge their card on a recurring basis to pay for future purchases of goods or services – for example, paying a monthly subscription. Payments can be made periodically at any fixed, regular interval – up to one year – depending on what the card holder and the merchant agree. Recurring payments can be a fixed dollar amount, or they can vary. They are initiated by you as a CNP transaction, either through a payment gateway or MAN-PAN 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, visit bnz.co.nz/interchangefees

For recurring transactions, you must ensure that you:

- Disclose to the cardholder a simple cancellation procedure
- Disclose to the cardholder an online cancellation procedure if the order was accepted online
- Disclose to the cardholder the dates and frequency at which transactions will be processed
- Provide a transaction receipt to the cardholder at the time of transaction
- Do not include any finance charges or interest
- Do not charge any convenience fees

Recurring and account-on-file transactions offer you and your customers the following benefits.

For cardholders

- Earn rewards on eligible transactions by paying monthly bills
- Avoid late payment fees
- Set-and-forget recurring payments speed up the check-out process for future payments

For merchants

- Processing is easy, with fewer errors

Identifying transactions at the payment gateway

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, letting your customers know your refund policy at the time of purchase can avoid questions and disputes later. Refunds must be returned to the same card or digital wallet 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 – they 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.

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.

Most payment gateways have refund capability via an online merchant portal. When you are processing a refund, an authorisation may be sent to the issuer of the card you are submitting the refund to. The transaction could decline based on issuer response – for instance, 'card closed'.

Fallback mode

Fallback occurs when your terminal does not read a Europay, Mastercard and Visa (EMV) chip card correctly and the customer must swipe their 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 regularly there could be a problem with the terminal, and you should contact your terminal provider for assistance.

Transactions in fallback mode carry higher risk for merchants, including a higher risk of chargebacks. Processing these payments uses lower security – so, if the cardholder challenges the validity of the transaction, you are liable.

Surcharging

Surcharging can be applied to your terminal or website to recover the cost of your MSF, 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 some payment options, surcharging is not permitted. For information on surcharging, 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 our Merchant Hub on **0800 737 774**.

Tipping

Some terminals allow customers to add a tip to 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 (NZD) 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)	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, which may 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 NZD. Settlement will be made to your nominated Bank of New Zealand account in NZD.

Benefits for merchants

- CurrencySelect EFTPOS merchants receive a MSF 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 at the time of transaction - compared to CurrencySelect online transactions, where you must set 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, which 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 indicative CurrencySelect foreign exchange rates, visit bnz.co.nz/personal-banking/international/exchange-rates
You can also see the exchange rate applied in your settlement transaction details.

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

Receipt requirements

You must retain the 'merchant copy' of all transaction receipts in a secure location for at least 18 months.

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.

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 that includes the business name, company number, the date of supply, the product or service, the price, and clearly outlines your returns process and any other terms and conditions.

Business protection

Chargebacks and disputed transactions

Sometimes we must 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.

Depending on the card scheme, chargeback reason, and business, chargebacks can occur between 60 and 540 days after the date of the transaction, or the date the goods or service were expected to be received by the cardholder. Chargebacks are the reason you must retain receipts for 18 months, as described in the previous section.

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 accounts. As the merchant, you could possibly lose the value of the sale as well as incur a chargeback.

Your Merchant Agreement Master Terms and Conditions covers this type of transaction. We have also included a list of common chargeback reasons and recommended actions below.

We may sometimes ask you for documentation to support transactions you have processed. 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.

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.

Always 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**.

Avoiding common chargeback situations

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 part or full credit was not issued.	Process a part or 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 or 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

Unfortunately, the person who presents a card or card number is not always its 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 Visa, Mastercard, American Express or UnionPay payments by internet, mail, or telephone, you must obtain authorisation for all transactions regardless of the value.

Ask for card security codes

Always request the three or four-digit card security code when processing a transaction.

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

Never store these numbers for any reason.

Know the warning signals

To minimise your risk, you need to identify characteristics that indicate potential fraud. Minimising card fraud means more than just seeking authorisation of a card transaction. This is because authorisation does not guarantee payment. It simply confirms that the card is valid, funds are available at the time you obtain authorisation, and the card hasn't, at that point, been reported as lost or stolen. We recommend you undertake these best practices to protect yourself against losses.

Fraud warning signs

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

Card number related fraud

- The card authorisation is declined, and a second card readily available
- The card numbers used are strikingly similar or in sequential numbers, e.g. 4557 02xx xxxx 001x; 4557 02xx xxxx 002x; 4557 02xx xxxx 003x
- The order is shipped to a single address but billed to multiple cards
- There are multiple orders on one card or similar cards with a single billing address but multiple shipping addresses
- There are several declined transactions before an approved transaction
- The total amount is split over numerous cards

Shipping related fraud

- The order shipping is rushed or overnight to deliver items as soon as possible for quick resale
- The order is shipped to an international address
- The order is shipped to a country you do not normally deal with
- The order is shipped to a country where the goods would be readily available in the local market
- The order is shipped to a destination country that is different than the country where the card is issued
- The order has a high shipping charge

Cardholder's details

- The order is from an internet address using free email services – for example, Hotmail, Yahoo, Gmail – or with domain names that can be set up by anyone
- The initiator of the order admits it is not their card being used
- The address for the order differs to the cardholder's address
- The order is via phone order, and the cardholder says a friend, relative or employer will come in to pick up the goods

Transaction amounts or volumes

- The order is a large one-off purchase which allows a fraudster to minimise possibility of identification
- Order is larger than normal, maximising the use of a stolen or counterfeit payment card
- An order 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 e.g. Western Union, or any other third party
- Orders where the transaction is cancelled and the cardholder request the refund be processed to another card, bank account, or via a money transfer service. Always process refunds to the card number the original purchase was charged to

Security measures

Always follow good business practice when processing sales, using security measures like the following.

- 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
- Always ask yourself if you 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
- To minimise the risk of chargebacks 3DS will be enabled for e-commerce sites. This shifts the liability of the transaction from you to the card issuer. 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 programs that attempt fraudulent transactions on your website

How we help

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.

How to contact us about security issues

If you experience card fraud, contact us immediately. 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, contact our Merchant Hub on **0800 737 774**.

Payap

Payap is a payment app held on your customer's phone, which enables them to pay you from their linked account. Similar to Alipay+, your customer uses Payap to scan a QR code generated by your EFTPOS terminal or Point of Sale (POS) system. Within their app, they check the details and authorise the payment.

Payap is brought to you by BNZ and Centrapay. To use Payap, you'll need to have a compatible terminal model. Check if your terminal model is compatible at centrapay.com

Business Portal

When you accept Payap transactions, you get access to Centrapay's Business Portal. To start you will need to set up a Payap profile. From the portal, you can manage your Payap profile and can easily:

- View transactions
- View settlements
- Initiate refunds
- Manage your Payap business profile information.

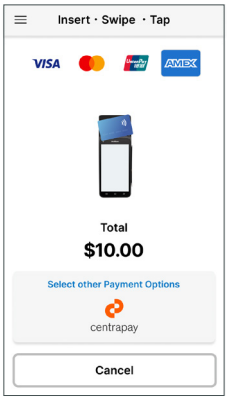
How Payap transactions work

On your EFTPOS terminal:

1. Create the transaction on your EFTPOS terminal in the same way you do for debit or credit card transactions.

2. The 'Purchase' screen is displayed. Your customer selects the Centrapay option on the EFTPOS terminal screen.

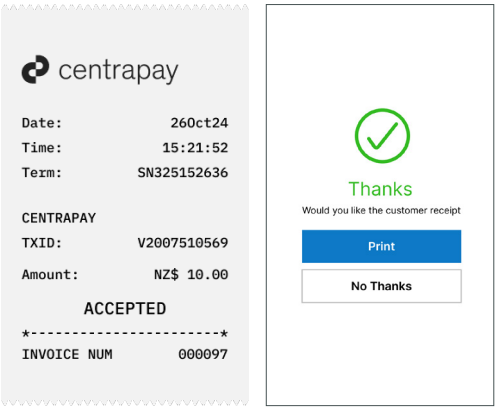
   The Centrapay option may look different, depending on your EFTPOS terminal.



3. A QR code and transaction amount is presented on the EFTPOS terminal screen.

4. Your customer uses their phone to open the Payap app and scan the QR code, then authorises the transaction from their Payap app.

5. Approved or Declined response shows on their phone and your EFTPOS terminal.



If your customer doesn't authorise the transaction in their Payap app within two minutes, the QR code will time-out on your EFTPOS terminal.

Surcharging

You cannot charge a surcharge fee for Payap transactions.

Refunds

You can perform Payap refunds via your EFTPOS terminal or via the Centrapay Business Portal. If the Payap refund is declined, the transactions you have processed so far that day are not sufficient to cover the refund. You will need to perform the refund in another way.

Settlement procedures

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

The day period for settlement and MSF charges is 00:00:00 to 23:59:59 New Zealand time. For example, transactions made Monday 00:00:00 to Monday 23:59:59 will be paid to your settlement account on Tuesday morning.

Payment processing fee

All Payap transactions incur a payment processing fee.

The payment processing fee for sales transactions is calculated monthly at the end of each calendar month and is payable by you on the 15th of the subsequent calendar month. It is calculated based on the net value of the sales transactions for the month – purchases less refunds – and the fee is debited from your nominated fees account.

Payap records

Digital records of your transaction history, daily settlements, and monthly payment processing fees can be found under your Payap profile in the Centrapay Business Portal.

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 this guide to meet the requirements of clause 3.6 of your Merchant Agreement – Master Terms and Conditions.

Checklist for UnionPay card present transactions

- 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 can be swiped, inserted, or used contactlessly on the terminal.
- 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.

UnionPay card not present transactions

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.

The range of UPOP payment options delivers several benefits.

- Cardholders are provided with flexible payment options for their online shopping experience, so UPOP helps you attract more customers and promotes your online business.
- UPOP provides multiple security methods including static verification, dynamic verification, and a private security key.
- Cardholders are offered attractive terms for currency conversion of UPOP purchases from international merchants.

Warning signs of card fraud

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

- the card has a UnionPay logo
- there is no sign 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.

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 processed as a Visa card.
- If a dual-branded card displays a Mastercard logo, the card is processed as a Mastercard card.

This happens automatically when the card or card number is presented to the terminal.

For e-commerce transactions, using a dual-branded card, the cardholder selects whether they want the transaction processed as UnionPay, or as Visa, or Mastercard, before they enter the card details.

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 that can't be matched with the original purchase will need to be organised with the customer.

Pre-authorisation and completions

- The completion amount can't exceed 15% of the pre-authorisation amount.
- If the completed amount would exceed 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.

How UnionPay Online Payments work

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.

2. The transaction information is forwarded to the UPOP system through your e-commerce gateway. Meanwhile, the cardholder's browser is redirected to a UPOP webpage.

3. Multiple payment methods are provided on the UPOP webpage, where the cardholder chooses their preferred method. UPOP is responsible for card number collection and facilitates authentication of the transaction once the payment method is selected.

4. UPOP collects the card number and authenticates the transaction.

5. UPOP forwards the payment information to the card issuer.

6. The issuer checks the payment information received and authorises or declines the transaction.

7. The e-commerce gateway 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.

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 – the same way 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. If you would like to add UPOP to your existing merchant facility, contact our Merchant Hub.

Pre-authorisation/completion

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

Alipay+

Alipay+ is a payment solution that enables the acceptance of multiple global digital wallets such as Alipay, ezlink, MPay, Touch 'n Go, GCash, and others. Customers who wish to pay using these digital wallets select the Alipay+ logo on the enabled payment terminal, scan the QR code, and then authorise the payment in their app. For a full list of Alipay+ enabled wallets, visit alipayplus.com

How Alipay+ transactions work

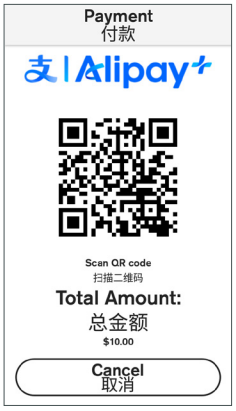
The Alipay+ transaction flow uses QR codes during transaction authorisation.

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.

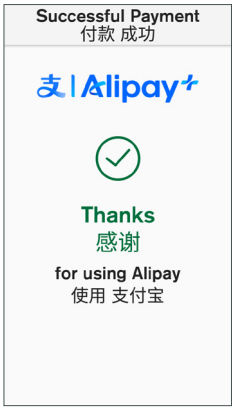
2. The 'Purchase' screen displays on the EFTPOS terminal. Customer selects Alipay+ logo on present card screen.

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 your customer doesn't authorise the transaction in their app within two minutes, the QR code will time-out on your EFTPOS terminal. If your customer doesn't enter the correct PIN in their app within one minute, the transaction will time out.

If your customer has insufficient funds in their digital wallet, they will be prompted to top up their wallet. If your customer does not top up and authorise the transaction 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.

You need the following details to refund a purchase through Alipay+.

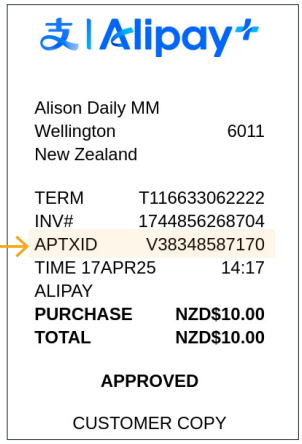
- Find the Reference number for the original purchase transaction on the receipt, or ask the customer to find it on their app.
- Find your 4-digit refund passcode that your terminal provider gave you, or that you've updated it to since then.

1. You need to know the transaction reference (APTXID) of the original purchase transaction.

   This can be found on the purchase transaction receipt.

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

Alipay transaction reference →


Alipay+

Alison Daily MM
Wellington 6011
New Zealand

TERM T116633062222
INV# 1744856268704
APTXID V38348587170
TIME 17APR25 14:17
ALIPAY
PURCHASE NZD$10.00
TOTAL NZD$10.00

APPROVED

CUSTOMER COPY

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

Follow these steps to process an Alipay+ refund using 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 the 11-digit APTXID.
5. Your terminal processes the refund and then displays Approved or Declined.

Your EFTPOS terminal can only process refunds for transactions that were made at your store. The refund value cannot be more than the original purchase value, even if you process this as multiple partial refunds.

The refund may not be posted immediately to the customer's e-wallet.

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 MSF charges is 4am to 4am in New Zealand Standard time. 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 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 daily, based on the total value of transactions for the day. The MSF is charged by direct debit on the business day after the transactions were made.

The MSF for any 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

Your EFTPOS terminal can produce a summary of daily totals. Maximum retrieval periods are terminal dependent.

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

- The Name of Other party is 'Alipay/BNZ Trans CR'.
- The Particulars show the number of transactions for the day with the text 'Alipay'.
- Code shows the Alipay transaction date in DDMM format.
- 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

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

Meanings of specific terms

APM means any alternative payment method besides cash, debit or credit cards.

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 card scheme sales transaction to you.

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.

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 – whichever applies – that we give you in connection with the merchant services.

MOTO means 'mail order or telephone order', 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 barcode that contains encoded data, and is designed to be scanned by devices like smartphone cameras.

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

(15088) BNZ191 03-25