BNZ **Merchant**
Service Guide

Your guide to using your credit and debit card facility

October 2018

Table of contents

Welcome to the Bank for 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 in regards to the acceptance of credit and debit cards.

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 - General 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 general merchant sales and service enquiries call the merchant helpdesk on **0800 737 774**, or send an email to bnz_merchantpayments@bnz.co.nz. They're available Monday–Friday, from 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 if you see any irregularities

› Accept and validate all nominated cards presented for payment – see page 9 for more information

› Follow the correct authorisation procedures for manual transactions – see page 10 for more information

› Ensure that the customer authorises all transactions by using a PIN or signature, unless the transaction is a contactless transaction less than $80.00, or is a mail, telephone, or internet transaction

› Do not split the cost of a single transaction between two or more sales receipts using a single cardholder account to avoid authorisation limits

› Do not give cash out with credit card transactions (including refunds)

› Do not impose a minimum or maximum amount on card transactions

› Retain paper or electronic records of all transactions in a secure place for 13 months and then securely destroy

› Be alert to possible card fraud and report all instances to us

› For card not present transactions, never store the card security code (the 3-digit security codes on the reverse of the Visa, Mastercard, and UnionPay International credit and debit cards)

› Never use your own credit or debit 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 more than the value of the goods or service you are providing

› Always process refunds to the original card used for the transaction

› If a card is accidentally left behind in 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 by comparing signatures with another card in the claimant's possession. If the card is not claimed within two business days, cut the card in half and send it to: Fraud Department, Bank of New Zealand, PO Box 2295, Wellington.

Settlement, service fees and statements for scheme debit and credit card processing

Settlement procedures

If your daily card processing settlement payment is made to a BNZ account, you can view and access the amount as soon as it has been processed. Processing card transaction settlements daily means you'll have your day's card payment amount in your BNZ account around 11.00pm every day – 7 days a week, 365 days a year.

If you have your card processing settlement payment made to an account at another bank, your payments will be received on business days only. Settlement of card processing on weekends or public holidays will be made the next business day. The other bank determines when you can view the payment and access the funds.

Merchant service fees (MSF)

All credit card transactions, and contactless, card not present (e.g. online), pre-paid and international debit card transactions, incur a merchant service fee (MSF). The MSF is made up by the interchange fee set by the card schemes, and costs incurred by us to process the transactions. The rate we charge depends on several factors such as the type of business you have, your transaction volumes, and the mix of domestic and International card types you accept.

BNZ merchant service fees are calculated monthly at the end of each calendar month, and are debited from your nominated account on the 15th of the subsequent calendar month. Should the 15th of the month fall on a day which is not a banking day, the fees will be payable on the next banking day. BNZ offers several pricing methods depending on your requirements and preferences.

Blended (Fixed)

We charge you the same fixed rate for all Visa, Mastercard, and UnionPay International card transactions.

Unblended (Fixed)

We charge you separate fixed rates for Visa, Mastercard, and UnionPay International card transactions.

Interchange plus

With this option, you'll be charged the actual Interchange costs applicable for each type of Visa and Mastercard transaction, plus a margin applied by us to process the transaction. Note: Interchange Plus is not available for UnionPay International or American Express transactions.

Interchange is a fee set by the card schemes for every card transaction. The fee is paid by the acquiring bank to the issuing bank for the transactions accepted at the merchant's facility. Interchange rates vary based on the type of card your customer is using and the transaction method, e.g. card present or card not present. The benefit of interchange plus pricing is that it is straightforward and clear - you can see exactly what rates you are paying for each type of card accepted. You can see the interchange rates on our website by searching 'interchange fees'. Some customers prefer a simple fixed rate for all card transactions, but interchange plus is the most transparent pricing option available.

Variable (Matrix)

If you're a new business with no transacting history, you might initially be priced on a variable matrix, which enables us to assess your sales limits to determine an appropriate pricing structure in the future, for example, fixed, or interchange plus pricing.

Association pricing

If you're a member of an association you could be eligible for special group pricing. Contact our merchant helpdesk on **0800 737 774** for more information.

Merchant statements

Your merchant statement is sent out monthly at the beginning of the month. The statement details all credit card and scheme debit card transactions you've processed in the previous month, and shows the amount of the merchant service fee due. It is your responsibility to check your statement regularly and contact us if you see any irregularities.

Merchant statement example, fixed pricing

Summary of Credit Card Transactions

Total service charge for this period is $1,803.78 which will be processed to your bank account number
_____ Unless advice to the contrary is received from you by 11 March 2016, the amount of $1,803.78 will be directly debited to your bank account on 15 March 2016.

Card	Sales	Returns	Amount Sales	Amount Returns	Net Sales	Rate	Service Charges
VISA	330	1	37,068.70	35.00	37,033.70	3.01	1,114.71
MCRD	160	1	17,435.40	41.40	17,394.00	3.01	523.56
CUP	43	1	8,393.20	117.80	8,275.40	2.00	165.51
TOTAL	533	3	62,897.30	194.20	62,703.10		1,803.78
YTD (Oct-Sep)	1786	8	138,837.00	368.10	138,468.90		3,920.40

Date	Card	Reference	Amount		Date	Card	Reference	Amount
01 February	V	76554056	82.10		09 February	V	76554056	839.90
01 February	M	76554056	1,856.20		09 February	M	76554056	740.80
01 February	V	76554056	161.40		09 February	C	76554056	165.00
01 February	M	76554056	276.10		09 February	V	76554056	654.70
01 February	C	76554056	332.70		09 February	M	76554056	915.10

1. The type of card accepted

2. The number of sales by card type

3. The total value of transactions by card type

4. The fixed rate (MSF) by card scheme

5. The total service charge (MSF) payable by you

6. Daily summary of card transactions (usually over more than 1 page).

Merchant statement example, fixed pricing, page 2

VISA **MasterCard** **UnionPay 银联**   **bnz**

BNZ MERCHANT

All enquiries to:
Payments Division
Phone 0800-737-774
Fax 04-474 9177

Summary of Credit Card Transactions - continued

Merchant Number:
000000000

Statement date:
31 July 2018

Domestic Transactions

	No. of Transactions	Value of Transactions
M CR Consumer Premium	14	5,055.36
M CR Consumer Super Premium 1	16	652.00
M CR Commercial	3	5,264.35
M CR Consumer Electronic	2	2,698.55
M CR PayPass	4	8,446.89
M DR PayPass	1	9,856.21
M DR PayPass Micro	15	18,560.96
M PP Consumer Prepaid Premium	5	1,136.76
V CR Contactless Credit Program - Platinum	5	6,520.36
V CR Contactless Credit Program - Classic/Gol	3	4,526.57
V CR Electronic - Classic/Gold	12	5,269.02
V CR Standard - Commercial	1	6,247.89
V CR Standard - Platinum	5	2,651.91
V DR Electronic	6	10,560.32
V PP Electronic	3	468.64
Total Domestic	95	87,915.79

International Transactions

	No. of Transactions	Value of Transactions
MasterCard	5	2,568.32
Visa	3	304.28
Total International	8	2,872.60

Summary

	No. of Transactions	Value of Transactions
MasterCard Domestic	60	51,671.08
MasterCard International	5	2,568.32
MasterCard Total	65	54,239.40
Visa Domestic	35	36,244.71
Visa International	3	304.28
Visa Total	38	36,548.99
Total	103	90,788.39

1. Card and transaction type

2. The number of transactions for each card type

3. The dollar value of transactions by card type

Merchant statement example, interchange plus pricing, front page

Summary of Credit Card Transactions

Total service charge for this period is $496.41 which will be processed to your bank account number _____ Unless advice to the contrary is received from you by 11 August 2017, the amount of $496.41 will be directly debited to your bank account on 15 August 2017.

Card	Sales	Returns	Amount Sales	Amount Returns	Net Sales	Rate	Service Charges
VISA	31	0	13,805.44	0.00	13,805.44	1.95	269.80
MCRD	16	0	8,352.50	0.00	8,352.50	2.71	226.61
TOTAL	47	0	22,157.94	0.00	22,157.94		496.41
YTD (Oct-Sep)	217	1	126,281.56	261.00	126,020.56		2,711.88

With interchange plus pricing you pay the cost of delivery for each card type, set by the card schemes, plus a margin applied by us to process the transactions. The rate (1) on the front page of an interchange plus statement is not the margin, it is an average of service charges divided by net sales, to show you an equivalent fixed rate.

Interchange plus statement example, page 2

All enquiries to:
Payments Division
Phone 0800-737-774
Fax 04-474 9177

Merchant Number:

Statement date:
31 July 2017

Summary of Credit Card Transactions - continued

Domestic Transactions

	No. of Transactions	Value of Transactions	Interchange Rate/Fee/Cost	Margin	Cost
M CR Consumer Premium	7	2,548.00	2.15%	0.52%	68.03
M CR Consumer Super Premium 1	2	3,749.00	2.35%	0.52%	107.59
M CR Commercial	4	1,186.50	2.00%	0.52%	29.90
M CR Consumer Standard	1	234.00	1.40%	0.52%	4.50
V CR Electronic - Platinum	4	601.50	2.10%	0.35%	14.74
V CR Electronic - Classic/Gold	4	4,145.00	0.85%	0.35%	49.74
V CR Standard - Commercial	8	4,481.94	2.00%	0.35%	105.33
V CR Standard - Platinum	8	2,450.50	2.10%	0.35%	60.04
V CR Standard - Classic/Gold	5	1,343.50	1.25%	0.35%	21.49
V DR Standard	1	93.00	1.25%	0.35%	1.49
Total Domestic	44	20,832.94			462.85

Summary

	No. of Transactions	Value of Transactions		Cost
MasterCard Domestic	14	7,717.50		210.02
MasterCard International	2	635.00		16.59
MasterCard Total	16	8,352.50		226.61
Visa Domestic	30	13,115.44		252.83
Visa International	1	690.00		16.97
Visa Total	31	13,805.44		269.80
Total	47	22,157.94		496.41

1. Card type

2. The number of transactions for each card type

3. The dollar value of transactions by card type

4. The interchange fee set by the card scheme for each card type

5. The margin set by us to process the transactions

6. The total cost for each card type

7. The total merchant service fee payable by you.

Accepting and validating cards

Which cards can I accept?

Your BNZ merchant facility gives you the ability to accept all Visa, Mastercard, UnionPay International, Alipay, and New Zealand issued debit cards, as payment for your goods and services. In addition to Visa, Mastercard, UnionPay and Alipay, a BNZ merchant facility enables you to accept American Express, JCB, and Diners Club cards; however, you will need to make separate arrangements with those schemes before you can accept those cards. When you receive your merchant number from the scheme, contact our merchant help desk on **0800 737 774** to have it enabled at BNZ. American Express and Diners Club credit card transactions will be settled directly by those schemes into your account.

You must accept all valid nominated cards bearing any of these logos without restriction on the amount of the transaction. If you are applying a surcharge fee you must advise the cardholder and give them a chance to opt-out before processing the transaction. You must also follow the procedures set out in Clause 3.9 of the Merchant Agreement General-Terms and Conditions.

Validating cards when the customer is present

We recommend the following checks to ensure a card is valid and can be accepted for payment. Most cards have the card details embossed on them. The embossing on the card should be even with all numbers the same size and shape.

› Check the expiry date on the card (1)

› Check the cardholder name on the card and that it matches any other information provided (2)

› Check the four-digit number printed below the account number is the same as the first four digits of the account number (3)

› Check for the three-digit card security code next to the signature panel on the reverse of the card. These numbers are required for card not present transactions (mail, telephone order, or online transactions) (4)

› A magnetic stripe is on the reverse of the card (5)

› The card has been signed by the cardholder (6).

Getting paid

Processing transactions

Transactions can be processed as either card present or card not present. This will be discussed with you during the application process and your facility approval confirmation will identify the types of transactions and card types you have approval to process.

Authorisation

All transactions must be authorised. An authorisation is our 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 19 for more information on chargebacks. To seek authorisation of manual credit card transactions call the authorisation centre on **0800 266 565**.

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 smartphones, like Google Pay and Apple Pay. Mobile wallets provide a convenient way for customers to make in-store payments and can be used anywhere that accepts contactless transactions via an EFTPOS terminal. Some mobile wallets can also be used for making purchases online, although most merchants will experience these transaction types when the customer is present at the time of purchase.

If your EFTPOS terminal accepts contactless transactions you're all set up and ready to accept transactions from mobile wallets. Card present transactions from mobile wallets work just like a standard contactless transaction which only requires a PIN for purchases of $80.00 or more. When a customer uses this technology to pay, they hold their phone against the terminal and their phone will vibrate after the transaction and show an 'accepted' or 'declined' message. All transactions accepted using Google Pay and Apple Pay incur a merchant service fee as it is a contactless transaction.

Alipay Wallet

An Alipay wallet also works like a physical wallet, but rather than containing digitised plastic card numbers it holds stored value. Alipay customers can use a variety of funding sources to load stored value into the wallet.

Alipay transactions are not contactless transactions - they use QR codes that are displayed on the EFTPOS terminal screen and are scanned by the Alipay customer using the Alipay app. The terminal will show an 'accepted' message when the transaction is approved. Refer to Appendix A on page 44 for a full list of products that are prohibited from being sold via Alipay.

Card present (CP) transactions

A card present transaction is one where the cardholder is present during the transaction at your place of business. These transactions are processed via an EFTPOS terminal and authorised in real time, usually with a PIN. For credit card transactions, only, if you get an 'accept with signature' terminal message, the cardholder can 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 terminal until the transaction has been processed. If the value of the transaction is less than $80.00 (e.g. $79.99), a PIN or signature is not required and an 'accepted or declined' message will appear on the EFTPOS terminal once the card has been tapped on the card reader.

If the value of the transaction is $80.00 or more, a PIN or signature is required to authorise the transaction. You will need to have an EFTPOS terminal that accepts this kind of payment. Ask your terminal provider for more information or call our merchant helpdesk on **0800 737 774** to turn on contactless acceptance on your terminal.

Contactless transaction fees

Although EFTPOS transactions are free of charge, all contactless transactions incur a merchant service fee. If you are on a fixed rate it will be the same rate as you are charged for Visa and Mastercard credit card transactions. If you are on interchange plus pricing you will pay the contactless interchange fee, plus a margin for us to process the transaction.

Electronic offline vouchers (EOV)

Electronic offline vouchers enable your business to continue processing transactions if your EFTPOS terminal loses its connection to the network. Connectivity can be lost for several reasons, such as telecommunication faults and power outages. With EOV enabled, even while you're offline, transactions can still be processed through your terminal in a safe and secure manner, making zip-zap machines a thing of the past.

On most terminals, EOV is set up by default and 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. Contactless transactions and Alipay transactions do not work in EOV mode. Refunds and cash advances are not available in EOV mode. The cardholder will be required to sign the receipt instead of entering a PIN and you will need to validate the signature against that displayed on the card, and keep hold of the receipt for 13 months. Once connectivity has been restored, your terminal will upload the stored transactions to the network for processing.

Until the stored EOV transactions have uploaded, you must ensure no changes are made to your terminal, such as unplugging it. There are several limits and restrictions applied when a terminal is in EOV mode, these include:

› The maximum dollar amount allowed per EOV transaction is $300

› The maximum number of EOV transactions allowed per day is 99

› Only one EOV transaction per card, per EOV session, is permitted on each terminal.

Finally, EOV limits and restrictions are governed by the card issuer and they may impose different restrictions on their cardholders from time to time. If you have any questions about electronic offline vouchers, contact our merchant helpdesk on **0800 737 774**.

Card not present (CNP) transactions

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

Mail-order/telephone order (MOTO)

If you would like to take mail-order and telephone orders for your goods and services, you can apply 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 credit card details into the EFTPOS or PayClip terminal when the cardholder and card is not present. MOTO transactions can also be processed using BNZ's Buy-Line+ Online product, and similar products supplied by independent internet payment gateway providers, which enable merchants to manually key cardholder details into a secure online portal for processing payments. If you want the ability to accept card not present transactions, including MOTO, you need to be approved by us first. Just call our merchant helpdesk on **0800 737 774** for more information.

E-commerce transactions

E-commerce transactions are used for taking one off customer payments that are usually initiated in real time. These are generally through a web site with an internet payment gateway. BNZ offers several e-commerce solutions including BNZ Securit-E, and the BNZ Buy-Line+ suite of products. E-commerce transactions are governed by strict data security standards, see page 25 for more information.

Other transaction types

Pre-authorisations (Pre-auths)

A pre-authorisation allows a merchant to hold a specific amount of money from a customer's card until the goods or service is provided, at which point the merchant can finalise the transaction for the full amount. These types of transactions are common for hotels, rental car companies, and any business that needs to hold funds from a customer's card.

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

Note: rules for pre-authorisation transactions are changing. It will soon be a requirement to clear/complete the authorisation, and $1 authorisations will not be permitted. Instead, we recommend a verification check on the customer's card. We 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 finalised or the hold on the funds has exceeded its expiry period. This period is set by the card issuing bank. Pre-auth functionality must be authorised by both the merchant's bank and Paymark before it can be enabled on your EFTPOS terminal or e-commerce site. 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

Finalise/complete: A finalise/complete transaction is the completion of a stored pre-auth transaction. To receive payment, the merchant must complete the transaction (finalise) once the goods or service is provided. Pre-auth funds are generally held for up to 14 days, but the hold period can be less or more and is dependent on the card issuer and acquirer. The finalise amount can be different to the original pre-auth amount, but merchants should be aware that if the finalise amount is higher, there is no guarantee that the bank will approve the higher amount. Contact our merchant helpdesk on **0800 737 774** for further information about pre-authorisations.

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 it can fluctuate.

They are initiated by the merchant as a card not present 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. Recurring transactions on domestically issued cards incur the domestic recurring interchange rate, and international cards can be used for recurring payments, however a higher international interchange fee will apply. Check our website for more information about interchange rates.

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 (like a Trade Me account top up). While technically it is still a card not present 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 for paying monthly bills with their credit card

› Avoid late payment fees

› Set and forget payment for regular bills.

For merchants

› Increased approval rates as expiry dates on domestically issued cards aren't validated by issuers on recurring transactions, meaning when new cards are issued they continue to be honoured

› There's a reduced merchant service fee as recurring payments incur a lower interchange fee

› Ease of processing and less errors.

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

Refunds

Returns and refunds are part of the shopping experience. Whether a return is necessary or not, customers find comfort in knowing what to do if they need to return a purchase. 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 credit 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 a refund card, contact our merchant helpdesk on **0800 737 774** for more information about obtaining one.

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

Fallback mode

Fallback occurs when a card that is EMV (chip & PIN) enabled 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:

› Higher risk of chargebacks for merchants. As a lower form of security has been used for processing the payment, the merchant has more liability for any transactions which are challenged by cardholders as being incorrectly charged

› Fines from schemes (Visa, Mastercard, and UnionPay) or disconnection. For example, if a merchant continues to process high levels of fall-back transactions, they could incur penalties of up to US$1 per transaction, charged to us by the card schemes and on-charged to merchants.

We will contact you if you are processing higher than acceptable levels of fallback transactions. If you continue to process high levels of fallback transactions, your terminal may be disconnected.

Surcharging

You can apply a surcharge fee to some or all Visa, Mastercard, and UnionPay International credit card transactions. You cannot apply a surcharge for Alipay transactions. If applying a surcharge fee, you must advise the cardholder and give them a chance to opt-out before processing the transaction, and you must comply with the procedures set out in clause 3.9 of the BNZ Merchant Agreement – General Terms and Conditions. Please contact our merchant helpdesk on **0800 737 774** for more information about this.

Tipping

Some terminals allow customers to add a tip on top of the transaction amount. This transaction is a combination of an authorisation, which requests approval for a purchase to proceed, and a purchase completion, which provides notification that the authorised purchase has completed. By utilising this combination of transactions, the merchant is provided with the ability to add a tip to a credit card transaction after having presented the cardholder with the transaction record. Contact your terminal provider for more information about tipping.

CurrencySelect Eftpos, and CurrencySelect Online transactions

CurrencySelect makes it easier for you to sell your goods and services to the world – online, in-store, over the phone, and by mail order, by converting your New Zealand Dollar sale price to your cardholder's home currency at the time of sale. Used in conjunction with an EFTPOS terminal, Buy-Line+ services, BNZ Securit-E, BNZ's Credit Batch product, or the NAB Transact payment gateway, it 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 New Zealand dollars. 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 cardholder's home currency – payable as a lump sum payment or rebated against your merchant service fee

› Improved customer service, experience & 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 credit card account.

To see CurrencySelect foreign exchange rates, just 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.

CurrencySelect Eftpos merchant service fee rebate

When you process an approved card present transaction using an EFTPOS terminal, where the cardholder has selected to be charged in their home currency, you will receive a rebate. The rebate is currently 0.8% of the total monthly NZD amount credited to you. There are two options you can choose to how you receive your rebate.

1. Rebate paid into a nominated bank account on the 15th of every month

2. Rebate deducted from the monthly merchant service fee.

If you're interested in getting CurrencySelect for your business, just call our merchant helpdesk 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 from the EFTPOS 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 13 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, facsimile, or by 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 should include 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

Suspicious sales

If you are suspicious about a card or cardholder, ring the authorisation centre on **0800 266 565** and they will advise the steps you should take, including retaining the card if possible.

Chargebacks and disputed transactions

There may be times when it is necessary for us to reverse a previous credit card transaction to your nominated bank account. This is referred to as a chargeback. A chargeback occurs when a cardholder (or their bank) raises a dispute about a credit card transaction processed by you. 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 incurring a chargeback fee.

Information regarding this type of transaction is covered in your Merchant Agreement - General Terms and Conditions. We have also included a list of common chargeback reasons and recommended action, on page 20.

There are times when the bank requests documentation to support credit card transactions banked by you. Please respond 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 Visa and Mastercard 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
Alteration of amount	The amount on the sales voucher was altered without the cardholder's permission	Process the amount the cardholder signed for
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 credit 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
Declined authorisation	Transaction completed after receiving a declined response	Accept the original authorisation response. Once a decline response is received, no further authorisation should be attempted Another form of payment should be requested
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
Illegible amount	The amount written on the sales voucher was illegible	Record the amount of the transaction clearly on the sales voucher or credit voucher
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-matching account number	The account number was not recorded or the account number on the sales voucher was incorrect	Ensure that the account number recorded on the sales voucher is correct (i.e. swiped or imprinted)
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 copy voucher is Illegible	The copy of the sales voucher which we received from you was illegible	Supply a legible copy of the item at the time of request. Card number and amount must be clearly readable
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

Chargeback reason	Reason chargeback occurred	How to avoid future chargebacks
Sales voucher not imprinted with card	The credit card was not imprinted at the time of sale	Ensure that all sales vouchers are imprinted at the time of sale
Sales voucher split to avoid authorisation	Two or more sales vouchers were created to avoid calling for an authorisation on a sale over your floor limit	Include all purchases on one sales voucher. Also, an authorisation must be obtained for the full amount if over your floor limit
Signature on sales voucher	The signature on the sales voucher was not compared to the signature panel on the card	Always compare the signature on the sales voucher to the signature on the card
No authorisation	The sales amount was over the floor limit and the required authorisation was not obtained	Obtain an authorisation on all sales which exceed your floor limit

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. That's where we would like to help, by recommending that you and your staff read and take the steps contained in this guide, which is based on the latest international information and experience.

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 advice occur and the cardholder is not present, you must take care to avoid becoming a victim of a fraud attack. We strongly recommend you undertake these best practices to protect yourself against losses.

Secure ID (CVC2, CVV2, CVN2 & CID)

Always request the Secure ID/Card Security Code when processing the transaction

› (CVC2) for Mastercard

› (CVV2) for Visa

› (CVN2) for UnionPay

› (CID) for American Express.

This will tell you that the person using the card is in possession of the card at the time of the transaction. 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	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

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 on your own computer server. Card numbers and expiry dates should always be stored securely. Always ask yourself, do I need to keep the card number and expiry date? The Secure ID/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

› Never deliver goods to unattended premises

› 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, however all merchants should have their own procedures in place to prevent these transactions being processed and should not rely on us to detect fraud.

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 helpdesk on **0800 737 774**.

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.

To minimise the risk of chargebacks, consider 3D Secure for e-commerce sites, as it shifts the liability of the transaction from the merchant to the cardholder.

3D Secure for e-commerce websites

3D Secure is an additional layer of security to make online shopping transactions safer, by authenticating a cardholder's identity at the time of purchase. It's provided by Visa as 'Verified by Visa', and by Mastercard as 'Mastercard SecureCode'. In addition, UnionPay International uses a proprietary authentication service called 'SecurePay'.

How 3D Secure works

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

Benefits of 3D Secure

› Block fraudulent transactions at the online checkout, before you send any goods or provide services

› Help protect against chargebacks claimed as unauthorised by the cardholder

› Increase customer confidence in the safety of your e-commerce site.

Even with the added protection of 3D Secure, it's important to have strategies in place to prevent fraud and chargebacks. If these levels become too high, it is possible that you could lose the liability protection that 3D Secure authentication provides.

Requirements for 3D Secure on your e-commerce site

To enable 3D Secure on your e-commerce site you'll need to have:

› An approved BNZ merchant facility

› An e-commerce site that meets BNZ's minimum requirements

› A payment option that supports 3D Secure, such as Payment Express or BNZ Securit-e.

Enabling 3D Secure

We may require you to use 3D Secure on your e-commerce site, however in most cases it is your choice whether you want to utilise it or not. If you want to enable 3D Secure, contact our merchant helpdesk on **0800 737 774** to get things started. We'll let you know what the next steps are, depending on whether your payment page is hosted by your payment gateway, or if you host your own.

Payment Card Industry Data Security Standards (PCI-DSS)

The growth of e-commerce has seen an increase in electronic fraudulent activity – such as hacking and redirecting payment full stop after information. This means any device or payment system storing, processing, and/or transmitting card data, is increasingly vulnerable to compromise.

In response to this threat, the Payment Card Industry (PCI) has developed the Payment Card Industry Data Security Standards (PCI-DSS) and all merchants are required to comply with these internationally recognised security standards. The intent of PCI-DSS is to protect stored cardholder data. PCI-DSS applies to both electronic and manually recorded information, e.g. paper vouchers, and will assist in preventing a data compromise.

How do I minimise my PCI-DSS risk?

The best way to lower your reporting obligations is to remove the presence of credit card numbers from your business. PCI approved, fully hosted solutions (usually provided by internet payment gateways) will capture the credit card numbers and process this information for you. This prevents any card numbers or other details contacting your IT systems, being available to staff within your business, and lowers risk of card numbers being stolen via web and IT attacks.

As a merchant accepting card payments, you must not store or retain any sensitive data after authorisation, which includes but is not limited to: Primary account number, secure ID, card security code, customer PIN number, and magnetic stripe data.

Benefits of PCI-DSS include:

› Reducing the risk of card fraud

› Avoiding fines, penalties and costs related to card security breaches and non-compliance by merchants

› Increasing consumer confidence in card payments

› Reducing your business' exposure to potential lost revenue because of fraud.

Help whenever you need it

If you ever need any assistance, you can contact us at pcidss@bnz.co.nz

Disclaimer

PCI-DSS defines a minimum data security standard to help secure sensitive cardholder data. BNZ, the Payment Card Industry Security Standards Council, and the card schemes do not guarantee that these standards will prevent security breaches or losses.

UnionPay International

UnionPay International is the 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 guide will help you and your staff to identify, accept and process UnionPay transactions. We've produced it to meet the requirements of section 3.6 of your Merchant Agreement - General 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.

Credit cards

- **A** Issuer's logo
- **B** Embossed card number
- **C** Expiry date (optional)
- **D** Embossed cardholder's name (optional)
- **E** Issuer's name in Chinese and English
- **F** UnionPay hologram
- **G** UnionPay logo
- **H** Magnetic stripe
- **I** Cardholder signature panel
- **J** Issuer's statement and service hotline (optional)

Debit cards

- **A** Issuer's logo
- **B** Name of the debit card
- **C** Valid issue or expiry date
- **D** Issuer's name in Chinese and English
- **E** Card number
- **F** UnionPay logo
- **G** Cardholder signature panel
- **H** Issuer's statement and service hotline (optional)
- **I** Magnetic stripe

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 electronic 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 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 by the customer.

Pre-authorisation and pre-authorisation completions

› The completion amount can't exceed 115% of the pre-authorisation amount

› If the finalise amount exceeds 115% 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 finalise 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 (UnionPay version of 3D Secure). An online portal (provided by Payment Express) allows you to manage all merchant admin and reporting requirements, including processing purchases, refunds, authorisations, pre-authorisations & completions.

Benefits

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

› Convenience: flexible payments improve the online shopping experience of cardholders, so UPOP helps you attract more customers and promotes your online business

› Security: provides multiple protections for security including static verification, dynamic verification, and a private security key.

Advantages for you

› With the powerful brand support of UnionPay, UPOP provides considerable customer education resources and business opportunities, by enhancing cardholders' confidence and trust in paying online

› UPOP provides a secure transaction environment based on the strong electronic payment service capability of UnionPay International.

Advantages for your customers

› UPOP provides cardholders with secure, convenient Internet payment services, through a wide range of participating banks

› UPOP offers various payment methods for cardholders to choose from, plus an extensive acceptance network both at home and abroad, strict merchant credit certification, and financial-level credit guarantee

› UnionPay International 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 Payment Express 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. UPOP settlement is aligned to the UnionPay International settlement cut-off of 11.00pm Beijing time. Funds will be credited to your nominated account overnight the following business day.

Transaction Amount Limit

To reduce potential fraud risks, UnionPay International imposes limits for online transactions:

Business type	Transaction limit (CNY)	Debit card daily limit (CNY)
Airline, Hotel, Education and Government related services	300,000	200,000
Luxury goods, wedding services, beauty products, duty free shops	30,000	50,000
Electronic Goods, Gifts	15,000	30,000
General Business, Department store, Car Rental & Maintenance and Miscellaneous	20,000	20,000
Courier Services, Telecommunications, Games top-up	500	2,000
Other Merchants	5,000	5,000

Prohibited businesses

UnionPay International does not support the following business types (merchant category codes in parentheses):

› Agricultural co-operatives (0763)

› Financial institutions - manual cash disbursements (6012)

› Non-financial institutions - foreign currency, money orders (not wire transfer), scrip, and travellers' checks (6051)

› Securities - brokers and dealers (6211)

› Payment transactions - Customer Financial Institution (6529)

› Payment transactions - merchant (6530)

› Betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at race tracks (7995)

› Firearms and ammunition (5999).

For a full list of prohibited business types speak to our merchant services team on **0800 737 774.**

Refunds

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

Payment gateway integration

BNZ is using the Payment Express PXPay2 payment gateway for all UnionPay Online Payment processing, including connectivity to the UPOP payment pages, transaction history, and settlement, so that our merchants have the ability to accept UnionPay as well as other card types using a single integration. However, if you use another payment gateway already, you may choose to maintain this solution for your existing card acceptance and just add Payment Express for UnionPay. Over time, other payment gateways may opt to add UnionPay acceptance. Integration documentation for Payment Express PXPay2 is available from Payment Express.

Website requirements

To ensure that your potential UnionPay customers know that you accept UnionPay and therefore feel confident to shop on your site, 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 Merchant Agreement – General Terms and Conditions. Please contact BNZ 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-auth/finalise).

Tokenisation

UPOP does not currently support tokenisation of card numbers. If your business requires tokenisation of card numbers (for example for recurring payments or card on file applications), we do not recommend adopting the UPOP service.

Pre-auth/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.
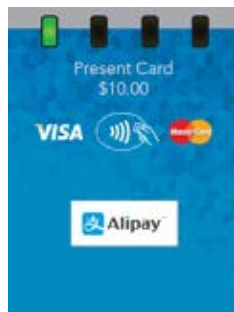
Alipay

Alipay is the world's largest digital payment and lifestyle platform. 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 transactions – how does it work?

The Alipay transaction flow uses QR codes during transaction authorisation. QR codes (or Quick Response 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 'Present card' screen will display on the EFTPOS terminal. To pay with Alipay, the Alipay customer would press the Alipay button.

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

4. The Alipay customer scans the QR code using the Alipay app on their mobile phone.

5. The Alipay app converts the transaction amount to Chinese Yuan. The Alipay customer can then confirm the transaction and enter their PIN to authenticate.

6. If the transaction was successful, the terminal will display an Accepted message, and a terminal receipt will print out

   The Alipay customer will also be able to access details of the transaction from within the Alipay app.
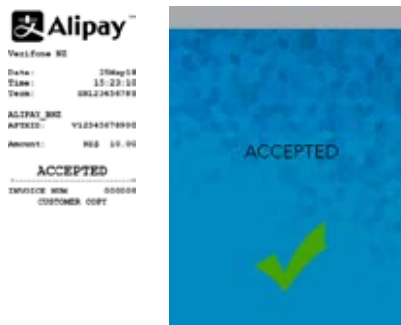
7. If the transaction was not successful, the transaction will time out within one minute and display the Timed Out message.

   If the Alipay customer doesn't enter their correct PIN to authorise the transaction 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 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 2 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
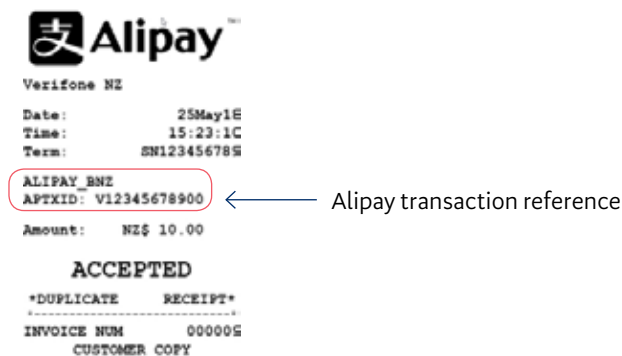
2. You need to know your 4-digit Alipay refund passcode. This information is initially given to you by your terminal provider, along with details of the process for changing it.
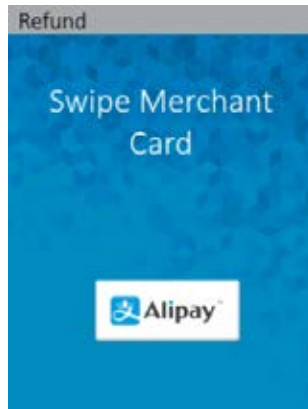
Here's how to process an Alipay refund via your terminal

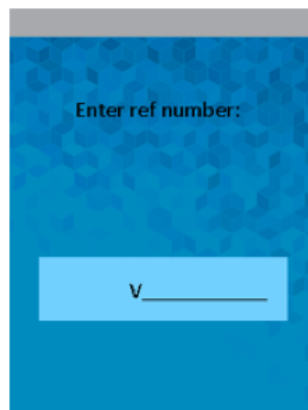1. Select the standard Refund option on your terminal.
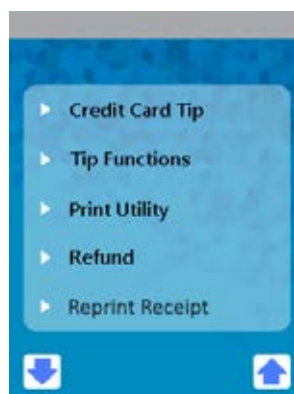
2. Select the Alipay button.

Refund

Swipe Merchant Card

Alipay

3. Enter the transaction reference from the original purchase transaction. This always starts with V.

Enter ref number:

V_____
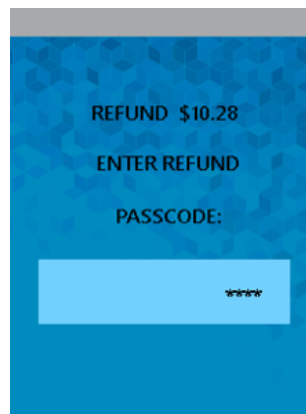
4. The terminal will then show:

› The original purchase transaction amount.

› Any amounts previously refunded by you.

› An entry box for the refund amount to be refunded now – this will default to the full amount available to be refunded, but can be overtyped if you are doing a partial refund.

Original amount $20.00

Total refunded $9.72

Refund amount:

$10.28

5. Enter your Alipay refund passcode.

REFUND $10.28

ENTER REFUND

PASSCODE:

****

6. The request will be processed through to Alipay who will check that the amount is available to be refunded and approve.

   If the refund was successful, the terminal will display an Accepted message, and a terminal receipt will print out.

ACCEPTED
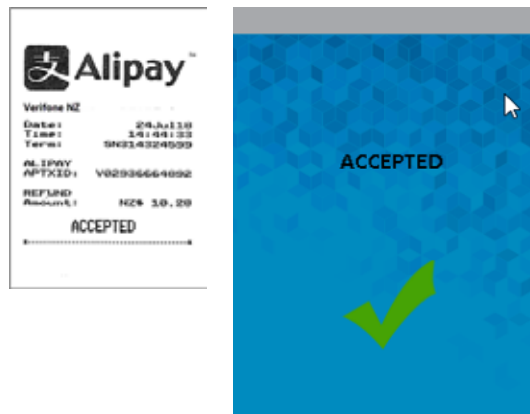
7. It is possible for a refund to fail. In this case, refer to your terminal provider.

ERROR

Refund failed
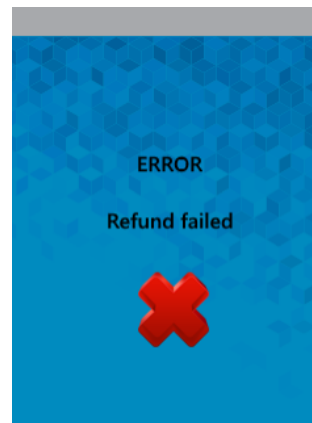
Your EFTPOS terminal will only be able to process refunds for transactions that were made at your store, and will not allow the refund value to be greater than the original purchase value (even if multiple, partial refunds are processed).
The refund may not be posted immediately to the customer's Alipay app.

Prohibited Businesses

Please refer to Appendix A on page 44 for a full list of prohibited products and business types.

Settlement procedures

If your card processing settlement payment is made to a BNZ account, you can view and access the amount as soon as it has been processed on the day after the transactions were made – 7 days a week, 365 days a year.

If you have your card processing settlement payment made to an account at another bank, your payments will be received on business days only, on the business day after the transactions were made.

The day period for settlement and merchant service fee charges is 4am to 4am NZST e.g. 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 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 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

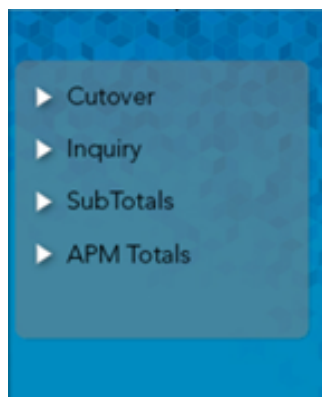As the MSF is charged daily, separate MSF statements will not be produced.

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.
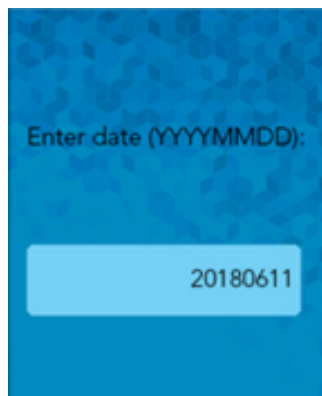
1. Select the Settlement option from the terminal.

> Purchase
> Purchase/Cash
> Cash Out
> Log On
> Settlement
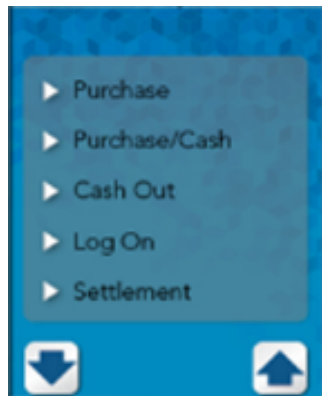
2. Select the APM Totals option.

> Cutover
> Inquiry
> SubTotals
> APM Totals

3. Enter the date on the screen in YYYYMMDD format and press the green [enter] button.

Enter date (YYYYMMDD):

20180611

4. Your terminal will print the Alipay totals receipt, and you can identify the expected settlement payment from here.

```
APM Totals
*------------------------*
TIME:       14JUN2018   15:23
TERM:              SN123456789
TOTALS FOR:         20180611

alipay_BNZ
PURCHASE
15                NZ$ 396.00
REFUNDS
0                 NZ$ 0.00
*------------------------*
```

Information contained within the settlement payment transaction can be used to reconcile the EFPOS totals

Date	Name of Other Party	Type	Particulars	Code	Reference	Withdrawals	Deposits
15 Jun	Alipay/BNZ Trans CR	DC	0015 Alipay	TRANS 1406	M24965527		396.00
15 Jun	BNZ Merch Serv Fee	DD	Alipay 0175	TRANS 1406	M24965527	6.93	

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'. 0175 means 1.75%

3. Code shows the Aipay transaction date in DDMM format

4. Reference contains 'M' and your merchant ID

Alipay Marketing Partners

To maximise your business opportunity in accepting Alipay payments, you can share a description of your products and services within the Alipay app. From within the app, Alipay customers can identify what merchants accept Alipay payments at different locations, which will help drive customers to your business.

To have a marketing presence in the Alipay app, you will need an agreement with an Alipay Marketing Partner. Alipay Marketing Partners provide varying levels of marketing services, covering 2 key areas:

1. Creating and managing your listing. This covers the basic listing of your business, product/services descriptions and location information. This can include videos and photos, and relevant content is translated into Mandarin by the Marketing Partner for you.

2. Creating special offers. This allows you to run campaigns via the Alipay app.

BNZ have agreed with an Alipay Marketing Partner to provide marketing services to create and manage your listing free of charge to you. BNZ can refer you to an Alipay Marketing Partner.

BNZ Frequently asked questions

What does the monthly merchant service fee cover?

The Merchant Service Fee (MSF) is paid to cover our costs for authorising and processing your transactions and crediting the funds to your Nominated Account. The Merchant Service Fee also covers costs for our Merchant helpdesk to answer any queries you may have.

How is the merchant service fee calculated?

The Merchant Service Fee is normally calculated as a percentage of the total dollar value of transactions processed for your business during the month and the average ticket size (sale). Fixed rates may be provided on request. A minimum monthly fee will generally apply. See page 5 for more information about merchant service fees.

Are the funds credited to our account guaranteed?

If the Transaction has been properly authorised and the transaction successfully completed, we will credit cleared funds to your Nominated Account. However, this payment may still be reversed later if a chargeback event occurs or the transaction is later discovered to be an invalid transaction. For details, refer to the section on chargebacks on page 19.

How do I change my merchant facility information? e.g. change of address, new owner etc.

If you need to change any of the information that you initially provided to us, call our merchant helpdesk on **0800 737 774**.

Who pays the cost if one of our employees uses a card fraudulently?

Your business is financially responsible for all card fraud, whether carried out by an employee, a cardholder, or both in collusion. To reduce the risk, ensure the rules outlined in this guide are explained to staff, and follow the tips for detection in the Business Protection section on page 20.

Can I charge for processing credit cards?

You can apply a Surcharge Fee to some or all Visa and Mastercard credit card transactions. If applying a surcharge see, you must comply with the procedures set out in Clause 3.9 of the Merchant Agreement - General Terms and Conditions.

Can I give cash out with a credit card transaction?

You must not provide cash to a customer on a Credit Card transaction under any circumstances. Cash can only be provided to customers making debit card transactions. It is recommended that the customer signs the receipt as proof of receiving the cash.

I have a problem with my EFTPOS terminal, who do I call?

In the first instance you should contact your terminal provider.

I don't know my Merchant ID, where can I find it?

You can find your Merchant ID on the top right hand corner of your merchant statement.

Where can I find my EFTPOS Terminal ID?

You can usually find your terminal ID on any EFTPOS receipt.

What happens if I sell my business?

If you sell your business and the new owner wants to retain your EFTPOS terminals you can do a 'change of ownership' process. Just contact our merchant helpdesk on **0800 737 774** for more information about this process.

Glossary

3D Secure means '3 Domain Server'. There are 3 parties that are involved in the 3DSecure process: The company the purchase is being made from, the Acquiring Bank (the bank of the company), and the card issuer.

Acquirer means a bank or financial institution that processes credit or debit card payments on behalf of a merchant

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

Certified Solutions provider (CSP) means a payment company accredited by Paymark to process transactions on the Paymark network

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

CID/card security code means the 3 or 4-character code on the signature panel of a 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 a global standard for credit and debit payment cards based on chip card technology

EOV means electronic offline voucher, a method of processing transactions on an EFTPOS terminal when there is no internet connectivity

Floor limit means the maximum dollar amount known as a 'floor limit' for manual transactions, notified by us to you from time to time

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 usually paid to the bank funding a transaction and thus bearing the risk

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

Letter of offer means the letter of offer or letter of acceptance that we give you about your merchant facility

MAN-PAN means manual primary account number entry, which allows manual entry of credit card details into an EFTPOS terminal

Matrix means a variable merchant service fee, determined based on a combination of the value and volume of card transactions you process

MCC means 'merchant category code', a 3 or 4-digit numerical code used by the card schemes to classify the type of goods or services a merchant supplies

MOTO means mail-order or telephone order, a method of card not present transaction

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

PAN means primary account number, the numbers embossed on the front of a card

PIN means the personal identification number allocated by a card issuer or 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

Scheme debit means a debit/EFTPOS card showing the logo of the card schemes, e.g. Visa and Mastercard, and containing a chip.

Appendix A - Alipay Prohibited products list.

1. Illegal political audio visual products and publications

2. Illegal political program channels

3. State secret documents and information

4. Pornographic and vulgar audio visual products, channels and publications

5. Pornographic and vulgar erotic services

6. Gambling devices and accessories

7. Lottery

8. Gambling service

9. Narcotics and related accessories

10. Weapons of all types (including daggers, firearms and accessories), replica weapons, ammunitions and explosives)

11. Military or police equipment

12. Illegally obtained proceeds or properties as result of crime

13. Poisonous or hazardous chemicals prohibited by Applicable Law and/or the laws of the People's Republic of China

14. Batons and electric batons

15. Lock picking tools and accessories

16. Anesthetic, psychotropic or prescription medicine prohibited by the People's Republic of China; illegal unregistered medicine

17. Fetal gender determination

18. Aphrodisiac

19. Medical services, including medical consulting, hypnotherapy, plastic surgery

20. Hacking services or accessories

21. Malwares

22. Software or services that may jeopardize the reputation and goodwill Alipay or any of its Affiliates or related party

23. Illegal publication of certificates issuing or carving of stamps

24. Crowd funding

25. Video chatting services

26. All religious websites, publication or accessories

27. Online cemeteries and ancestor worshipping

28. Sales of personal information (e.g. identity card information)

29. Espionage equipment and accessories

30. Services or products that infringe on personal privacy (e.g. online activity monitoring)

31. Pyramid schemes and multi-level marketing

32. Gold investment

33. Cash disbursement from credit funding sources (e.g. credit cards)

34. Counterfeit currency

35. Illegal sale of financial information (e.g. bank accounts, bank cards)

36. Stock and securities

37. Mutual Funds

38. Insurance products and platforms

39. Financial products and services

40. Rebate or cashback services

41. Software or products related to trading of financial products and information

42. Single-purpose prepaid cards (including gift cards and other stored value cards)

43. Illegal or un-registered fund-raising activities

44. Foreign exchange services

45. Peer to peer (P2P) lending services

46. Payment by instalments service

47. Trading in invoices issued within the Peoples' Republic of China

48. Trading or sale of virtual currencies (e.g. Bitcoin, Litecoin)

49. Satellites and antennas

50. Archaeological and cultural relics

51. Trading or distribution of currency (both RMB and foreign currencies)

52. Counterfeit or replica food products

53. Online sale of tobaccos and cigarettes

54. Fireworks and firecrackers

55. Crude oil

56. Human organs

57. Surrogacy services

58. Services to facilitate plagiarism and examination fraud

59. Protected species

60. Smuggled goods

61. Sales of distribution of event tickets without license
    (e.g. Olympic Games or World Expo tickets)

62. Seeds

63. Real estates

64. Charitable Organisations

65. Auction sites and services

66. Pawn services

67. Lucky draw

68. Sale of animals, plants or products with contagious and hazardous diseases

69. Sale of animals, plants or products originating from areas declared with
    an epidemic outbreak of contagious diseases

70. Services or products facilitating unlawful public gathering.