Merchant Agreement General Terms - NZ

Section 1: Quick Reference Guide

1. Introduction

This Quick Reference Guide is intended to assist you and your staff with the important components of the Latitude Technologies Limited (Latipay) Merchant Agreement General Terms and Conditions.

This is to ensure you have a clear understanding of your rights and obligations as a valued Latipay merchant.

The first section of the guide outlines key issues and procedures. This section will help you understand important issues and explain how we can work together to ensure your merchant facility helps meet the needs of your business. Although there are requirements in this guide that you must comply with, it is not a replacement for your Merchant Agreement General Terms and Conditions or the supplementary conditions. It is important that you read the letter of offer and Section 2 of this booklet which sets out the Merchant Agreement General Terms and Conditions. You must also read the supplementary conditions if those provisions apply to you.

In addition you must also read:

a) Payment Card Industry Data Security Standards brochures; and

b) any other merchant services documentation supplied to you from time to time; and

c) your merchant statement.

You are required under the terms of your Merchant Agreement to comply with terms, conditions and procedures identified in the documents referred to above. We may vary or replace this booklet at any time by written notification, which may be provided by mail, email or through our website. Information on current standard fees, charges and any interest rates is available on request.

2. Processing transactions

You must:
(a) accept all valid Cards and process all transactions in accordance with this document and any other practical operating instructions we provide to you; and
(b) make every effort to verify the identity of the Cardholder, and ensure any Cardholder authorisation is not forged, obtained by fraud or deception, unauthorised or that the transaction is not otherwise invalid.

You must not:

(a) request that the cardholder provide you with the cardholder’s card and/or pin number to retain; or
(b) undertake any transaction representing refinancing or transfer of an existing Cardholder’s financial obligation to you; or

(c) request that a customer provide card details via email for payment of the provision of goods and/or services. Should such details be provided to you, you must not use this information to provide goods and/or services, and must immediately securely destroy these details.

What is an authorisation?
An authorisation is confirmation that:

a) the number on the card exists and is valid; and

b) the card has not been reported lost or stolen at the time of the transaction; and

c) sufficient funds are available at the time of the authorisation request.

Authorisation occurs when the cardholder's bank or financial institution confirms these details.

Authorisation is not a guarantee of payment
Obtaining an authorisation does not guarantee payment or protect you from disputed transactions. An authorisation does not, and cannot, guarantee that:

(a) the legitimate cardholder is using the card; and/or
(b) the person using the card is authorised to do so by the account holder; or

(c) that the card has not been compromised (card details improperly obtained or copied).

Additional security (card not present transactions)
If the card and purchaser are not physically present at the time of purchase, there is an increased risk of liability for transactions that are disputed.

To help reduce your exposure to card fraud, we suggest you undertake additional security measures whenever you accept a Card not present transaction.

Floor limit
A floor limit is an amount allocated to merchants individually. The default floor limit is zero. The floor limit represents the maximum transaction in Australian dollar value that you can process without obtaining an authorisation. Floor limits are set and changed by Latipay from time to time to align with the requirements of the card schemes.

All transactions must be processed electronically and are automatically provided with a real time authorisation.

Transaction splitting
Under no circumstances should a sale be 'split' by completing two or more transactions, except in the following instances:

(a) when the cardholder bills a portion of the transaction to a card and pays the remaining balance by cash, voucher or cheque only; or
(b) when the goods or services will be delivered or performed after the transaction date, where one voucher represents a deposit and the second voucher represents payment of the remaining balance. The second voucher is conditional upon the delivery or performance of the goods or services.

If you split a transaction to avoid having to obtain authorisation, this action may result in the transaction being charged back.

3. Pre-authorisations

This paragraph 3 only applies where you have been approved for pre-authorisation transactions. Pre-authorizations are not available for cheque and savings transactions.

A pre-authorisation is used to place a hold on the cardholders' funds to the value of the transaction to be processed at a later time, for example, a hotel may reserve funds to pay the final bill upon checkout.

The pre-authorisation confirms that sufficient funds are available to cover the cost of the transaction and a hold is placed on the funds for approximately 5 to 7 days for domestically issued debit and credit cards. The matching transaction value should be processed within this time period. A pre-authorisation transaction supplies you with an authorisation number that must be recorded for processing of the final transaction.

Please ensure you advise the customer of the pre-authorisation amount.

4. Off-line transactions and pre-authorisation completions

An off-line transaction or pre-authorisation completion is used to process the value transaction relating to a previously obtained pre-authorisation.

You must not use the off-line function for any other purpose than as authorised by us.

5. Card not present transactions

(For merchants processing card not present transactions)

As sales activity via the internet and other remote channels is increasing, merchants need to ensure that they are familiar with the increased risks of accepting payments when the card is not physically present for verification.

Any transaction conducted via the telephone, email, mail or internet is known as a 'card not present' transaction and carries additional risks.

If a cardholder disputes a 'card not present' or Mail order/Telephone order (MOTO) transaction, the merchant is at risk of having that transaction charged back. The risk of almost all 'card not present' transactions resides with the merchant NOT the bank or the cardholder.

Once you have obtained our approval to process 'card not present' transactions, it is important to have policies and procedures in place to verify the identity of the purchaser before allowing the transaction to go ahead.

Some suggestions to assist you in verifying the cardholder's identity include:

(a) obtaining full name, address and landline telephone number details;

(b) conducting a white pages or Telstra check on the address and phone number provided;

(c) confirming the order by calling the landline number provided; and

(d) ensuring all deliveries are conducted by a reputable courier and made to verifiable residential or business addresses only.

Note: Always be wary of large or suspicious orders.

6. Internet based merchants

For internet based merchants, you must comply with clauses 4.5 to 4.10 (inclusive) of your Merchant Agreement General Terms and Conditions to enable you to accept payments through your website.
If transactions conducted by cardholders on your website are processed automatically through your merchant service, you are responsible for ensuring that this is operational.

7. Storage of cardholder data

If you have access to, or if you store card details in any format, or if you use a service provider who does, you are responsible for ensuring the security of your customers' payment details.

Storage of electronic card details on all systems is governed by strict guidelines that aim to protect this information from unauthorised access.

Data storage also includes physical storage and security of cardholder data. Some examples of other data storage which must be secured include an Access or Excel database and hard copy files.

Payment Card Industry Data Security Standards (PCIDSS) refers to the data security standards which have been mandated by Visa and MasterCard to facilitate protection of cardholder data from unauthorised access.

The Schemes may issue heavy penalties if your business experiences a card data compromise and you are non-compliant.

Storage of paper records is also regulated by your Merchant Agreement General Terms and Conditions.
You must not, under any circumstances, request that the cardholder provide you with the cardholder's card and/or pin number to retain.

8. Disputed transactions

A 'disputed transaction' can arise for a variety of reasons; the most common is when a cardholder cannot identify a transaction or claims not to have authorised a transaction on their credit or debit card.
A cardholder can lodge a dispute and, once a transaction is disputed by the cardholder, it may be debited to your account.

This process is known as a 'chargeback'. It is up to you to provide proof that the transaction is legitimate by providing evidence of the transaction as requested.

Failure to respond to requests for information/vouchers within specified timeframes may result in chargebacks.

Common types of disputed transactions include fraudulent transactions, unrecognised transactions, unauthorised transactions, duplicate processing and recurring transactions.

Fraudulent transactions
You should always be aware of the potential for fraudulent transactions and have policies and procedures in place to deal with suspicious transactions.

Unrecognised transactions
An "unrecognised transaction" occurs when a cardholder cannot reconcile the transaction appearing on their card

statement with the payment to your business. To avoid this situation you must ensure that your merchant facility name is also your trading name or a name that your customers will easily recognize. Encourage your customers to retain their receipts for reconciliation.

Unauthorised transactions
Unauthorised transactions occur when the cardholder denies conducting a transaction. Ensure you keep all receipts and signed card vouchers. Always check the signature on card vouchers against the signature on the card. In the case of mail order, telephone order or internet transactions, special care should be taken to establish cardholder's identity.

Duplicate processing
This occurs when a transaction is charged to the cardholder's account two or more times. Should you notice this has occurred, you can avoid a chargeback of this type by crediting the cardholder through your payment gateway (where applicable).

Recurring transactions
This happens when a cardholder has cancelled a recurring transaction authority but is still being debited. You can avoid future chargebacks of this type by updating your records as soon as the cancellation/alteration request is received.

Where to go for help
Should a transaction be disputed by the cardholder, you will receive a formal notification from Latipay in the form of a Chargeback and/or a Retrieval Request (Refer to Section 9 of this guide for further information). It is important for you to read these notices and respond to the request within 10 calendar days. Failure to do so may result in a legitimate transaction being charged back to your settlement account.

Chargeback contact details
In the event of a dispute, all documentation we request should be returned to Latipay via email on:

Telephone 09 930 0600
Chargeback Queries – customerservice@Latipay.net
Should a cardholder contact you directly regarding a disputed transaction and you believe the transaction to be legitimate, refer the cardholder back to their bank.

9. The chargeback process

Once a cardholder disputes a transaction, their bank will contact Latipay on their behalf to verify the details of the transaction. Latipay will then contact you to assist with this process.

Chargebacks
A chargeback occurs when the cardholder (or their bank/financial institution) raises a dispute in connection with a card transaction. If the dispute is resolved in favour of the cardholder, the transaction will be debited (charged back) to your account.

Latipay also has the ability to raise a chargeback on a transaction should it be invalid or unacceptable. This would result in the loss of the full sale proceeds of the transaction and a chargeback fee will also be applicable.

Retrieval requests

In some cases you will receive a request for transaction information from Latipay (known as a “Retrieval Request”). This process may allow you to verify the transaction for the cardholder prior to the transaction being charged back.

Should you receive such a request, please respond within 10 calendar days. Failure to do so may result in a legitimate transaction being charged back to your settlement account.

Information you need to supply
Your response should include all details relevant to the transaction and any verification of the cardholder.

These details may include:
a) a signed copy of the transaction voucher or receipt; and/or

b) a copy of the order or invoice; and/or

c) a copy of any correspondence received by you from the cardholder. Please keep a copy of all documentation you forward to us.

Keep your records up to date
It is important to retain all documentation relating to transactions. This will assist you in responding to ‘Retrieval Requests’ should a transaction be disputed.

Do not re-process charged back transactions
You must not re-process a transaction that has previously been charged back. This violates card scheme regulations (and could lead to the termination of your merchant services).

Do not process a refund to a cardholder after you have received chargeback notification from Latipay as this may result in you being debited twice for the transaction.

Card not present liability
Visa and MasterCard rules request that a PIN or ‘signature’ be obtained during a transaction, except for some transactions performed by tapping a card near a contactless card reader. Therefore, for a Card Not Present transaction ‘You’, the merchant will always be liable for a chargeback. (Please note for electronic commerce transactions, this liability can be reduced by implementing Visa Secure and MasterCard Identity Check.)

10. Refunds

A refund occurs when a merchant agrees to pay money back to a customer for goods that have been returned or services not received. You should establish a fair policy for the return or exchange of merchandise. Refunds may only be processed to a card where there was an initial valid transaction on that card. Do not refund cash under any circumstances.
If you have an electronic gateway supplied with an initial password, you should immediately change the refund password to a unique code for your business. This refund password should be changed on a regular basis and should only be disclosed to those who process refunds, reducing the risk of refund fraud by staff. You should change the password immediately after a staff member has left your employ.

Electronic refunds
If a cardholder returns goods that have been purchased with a card, you must refund the transaction back to that card and NOT provide the refund to a different card, or in cash or cheque. If you do not follow this procedure you may be exposed to fraudulent transactions. Following correct refund procedures will also provide you with proof that the

transaction has been refunded if a dispute arises.

11. Fraudulent transactions

Fraud is an issue for many merchants and can have a substantial impact on your business.

You should have policies and procedures in place to handle irregular or suspicious transactions and to detect suspicious cardholder behaviour. You should ensure that all your staff understands the built in security features of the legitimate cards and can identify these. Remember, if a sale seems too good to be true or suspicious in any way, it may be fraudulent!

Card not present transactions
There is a significantly higher risk of fraudulent transactions where a transaction is processed without the card being electronically swiped, inserted or manually imprinted by the merchant (e.g. Mail order, telephone order, internet based or manually keyed transactions).

Third party transactions
You must not process transactions on behalf of any other person or business or in connection with any transaction which is not directly related to the sale of goods or services to your customer. Processing such transactions would be a serious breach of your merchant agreement and you will incur any losses (i.e. chargebacks) associated with these invalid transactions.

Unauthorised refunds
You should ensure you have adequate security provisions to prevent unauthorised processing of refunds through your merchant services or terminal.

Reducing card fraud
Listed below are just some of the steps you can take to help avoid card fraud for your business.

For ‘card not present’ transactions:

(a) obtain full name, address and landline telephone number details; and
(b) conduct a white pages or Telstra check on the address and phone number provided; and

(c) confirm the order by calling the landline number provided; and

(d) ensure all deliveries are conducted by a reputable courier and are made to verifiable residential or business addresses only.

Note: Extra care should be taken when providing goods or services to international destinations.

We recommend caution when dealing with international orders, particularly from countries you do not normally deal with or if you do not normally trade internationally. Whilst all international orders carry an increased fraud risk, transactions originating from African or Eastern European countries have been shown to generate a disproportionate level of card fraud.

12. Hotel/motel accommodation providers

This Section 12 only applies to businesses that have been authorised to accept credit card transactions to

guarantee hotel, motel or accommodation reservations or advance deposits.

If you have been approved to accept pre-authorisations, the amount may be based on the customer's intended length of stay at check in, the room rate, any applicable taxes, service charge rates and other allowable charges such as meals, phone calls, etc.

For instructions on processing a pre-authorisation, please refer to your terminal user guide.

For prepaid transactions or transactions which originate via the internet your business should participate in CVV (Card Verification Value) which is an anti-fraud security feature. This will assist in verifying that the cardholder is in fact, in possession of the credit card and that the card account is legitimate.

Additional, delayed or amended charges

You must obtain authorisation from the cardholder to process additional or amended charges such as the cost of food, beverages, tax or dry-cleaning amounts that were not available at the time the pre-authorisation was obtained.

Card scheme rules state that charges for damages, theft, cleaning, etc. are not considered to be legitimate delayed or amended charges, therefore you must obtain prior written consent from the cardholder to process these additional charges to their credit card or seek another form of payment (cash, cheque).

In order to reduce the risk of chargebacks you should process any additional, delayed or amended charges as a separate transaction.

13. Motor vehicle rental agencies

This Section 13 only applies to businesses that provide vehicle rental services.

You may not process transactions which include charges representing either the vehicle insurance deductible amount or an amount to cover potential damages when the cardholder waives insurance coverage.

Charges for damages must be processed as a separate transaction. You must provide a reasonable estimate of the cost to repair the damages and obtain agreement from the cardholder.

Where you have been approved for pre-authorisation transactions the pre-authorisation amount may be based on the customer's intended length of vehicle rental, insurance and tax.

For instructions on processing a pre-authorisation, please refer to your terminal user guide.

Additional, delayed or amended charges

You must obtain prior written consent from the cardholder to process additional charges to their credit card or seek another form of payment (cash, cheque).

In order to reduce the risk of chargebacks you should process any additional, delayed or amended charges as a separate transaction.

Additional charges may relate to traffic or parking infringements or damage to the vehicle.

14. Subscriptions Transactions

This section 14 only applies to Merchants who provide subscriptions services

If you offer introductory free trials or promotional discounts as part of an ongoing subscription service we recommend you make the following disclosures when you enrol a cardholder, in order to increase your chances of resolving a chargeback dispute in your favour:

(a) Provide a digital receipt, even if no payment is yet due, confirming your cardholder's consent to the subscription or free trial, providing terms and conditions, the amount and frequency of future payment obligations, and a link to a cancellation page

(b) A reminder email or text message advising that the trial period is over, including a link to a cancellation page, at least 7 days before processing the first transaction after the end of the trial period

(c) A clear message that the trial has ended. For example, "End Trial" in the merchant descriptor that appears on the cardholder's statement

You must provide cardholders with a simple way to cancel their subscriptions eg over the internet, even if the cardholder signed up for the trial offer over the phone or in person.

15. UnionPay International (UPI)

Some Latipay merchants may choose to also accept UnionPay International (UPI) cards.

If you wish to process UPI transactions, you should know that special terms and conditions apply. These are set out in full in your Merchant Agreement General Terms and Conditions. You will need to read these special terms and conditions carefully and ensure you understand the special processing requirements:

(a) UPI cards are subject to special conditions relating to refunds and pre-authorisations;

(b) all UPI card transactions must be authorised online and can only be processed through certain terminals;

(c) manual or fallback processing is not permitted;

(d) UPI cardholders must sign the transaction receipt for all UPI card types; and

(e) a PIN must be entered for both UPI debit card transactions and UPI credit card transactions.

If you have been authorised to process UPI transactions, please refer to your Terminal User Guide for instructions on how to complete these transactions.

16. Contact us

Help desk support

For customer assistance, to report system faults or failures, how to close your facility and for general enquiries regarding Latipay's Payment Solutions contact the Merchant Service Centre.

Call the Merchant Service Centre on 09 930 0600

24 hours, 7 days a week or visit www.Latipay.net

Sales enquiries

For all enquiries or information requests on Latipay's range of payment solutions for your business:

Call our sales consultants on 09 930 0600 8.00am – 6.00pm AEST/AEDT Monday to Friday, ask your Account Manager or visit us at www.Latipay.net

Merchant fraud team

For fraud related enquiries:

Call 09 930 0600
fraud@latipay.net

17. Complaints

Latipay has internal and external dispute resolution processes in place. If you have a complaint about the services or products provided to you by Latipay, you should take the following steps:

a) Contact your Latipay Representative and discuss your concerns.

b) If your complaint is not satisfactorily resolved, contact Latipay to inform us about your complaint. You may do this by telephone, facsimile, email or letter.

c) If you are dissatisfied with the outcome, you have the right to complain to an external complaint scheme such as the Commerce Commission New Zealand

PO Box 2351 Wellington 6140 New Zealand
Freephone 0800 943 600 Email: contact@comcom.govt.nz
Web www.comcom.govt.nz