

more
than
money



Merchant Agreement

Quick Reference Guide

Contents

1. Introduction	4	16. Motor vehicle rental agencies	12
2. NAB Hive	4	Additional, delayed or amended charges	12
3. Processing transactions	4	17. Subscriptions Transactions	12
What is an authorisation?	4	18. UnionPay International (UPI)	12
Authorisation is not a guarantee of payment	5	19. Contactless-enabled terminals and Merchant Choice Routing	13
Additional security (card not present transactions)	5	20. Stationery	13
Floor limit	5	21. Contact us	13
Transaction splitting	5	Help desk support	13
Manual authorisations	5	Authorisations	13
4. Fallback transactions for EFTPOS terminals	6	Sales enquiries	13
Fallback transactions	6	Merchant fraud team	14
Processing transactions during a system outage	6	22. Complaints	14
5. Pre-authorisations	6		
6. Off-line transactions and pre-authorisation completions	6		
7. Card not present transactions	6		
8. Internet based merchants	7		
Authentication	7		
NAB Transact, NAB Gateway	7		
New NAB Gateway Service	7		
9. Storage of cardholder data	8		
10. Disputed transactions	8		
Fraudulent transactions	8		
Unrecognised transactions	8		
Unauthorised transactions	8		
Duplicate processing	8		
Recurring transactions	8		
Where to go for help	9		
Chargeback contact details	9		
11. The chargeback process	9		
Chargebacks	9		
Retrieval requests	9		
Information you need to supply	9		
Keep your records up to date	9		
Do not re-process charged back transactions	9		
Card not present liability	10		
12. Refunds	10		
Electronic refunds	10		
Manual refunds	10		
13. Fraudulent transactions	10		
Use of counterfeit or stolen cards	10		
Card not present transactions	10		
Third party transactions	10		
Unauthorised refunds	11		
Reducing card fraud	11		
14. Chip enabled EFTPOS terminals	11		
15. Hotel/motel accommodation providers	11		
Additional, delayed or amended charges	12		

1. Introduction

This Quick Reference Guide is intended to assist you and your staff with the important components of the National Australia Bank (NAB) Merchant Agreement General Terms and Conditions.

This is to ensure you have a clear understanding of your rights and obligations as a valued NAB 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 the **Merchant Agreement Quick Reference Guide**. You must also read the supplementary conditions if those provisions apply to you.

In addition you must also read:

- (a) Protect your Business from Card Fraud and Payment Scams information website; and
- (b) Payment Card Industry Data Security Standards brochures; and
- (c) Merchant User Guide for your terminal (where applicable); and
- (d) any other merchant services documentation supplied to you from time to time; and
- (e) 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 on NAB Hive or through our web-site. Information on current standard fees, charges and any interest rates is available on request.

2. NAB Hive

NAB is expanding its merchant services with the addition of an online portal and reporting service. NAB Hive is a cloud-based portal that captures and analyses information about your payments, helping you understand and manage your business. It will enable you to view transactions in near real time and view and download your statements. NAB Hive is being rolled out gradually starting this year. We will contact you when NAB Hive is accessible to you. NAB Hive will be available to you without additional fees.

3. Processing transactions

You must:

- (a) accept all valid cards or card based payments 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:

- (c) request that the cardholder provide you with the cardholder's card and/or pin number to retain; or
- (d) undertake any transaction representing refinancing or transfer of an existing cardholder's financial obligation to you; or
- (e) 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.

You may only retain the customer's card if our operator asks you to do so.

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; some of these have been outlined in the Protect your Business from card Fraud and Payment Scams website. The Australian Payments Network (APN) now requires NAB and other merchant service providers to ensure that card not present fraud is kept at or below specified levels. Fines can be imposed on NAB if these levels are not met. As a result the Merchant agreement allows us to require that you take measures to limit fraud and to pass fines on to you if levels are exceeded.

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 NAB 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. To process a transaction manually, please call NAB KeyAuth service on 13 25 15 and follow the prompts.

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.

Manual authorisations

Whether you are using online or terminal merchant services, most authorisations are obtained electronically. You will need to obtain a manual authorisation if:

- (a) the card is faulty and will not process through your terminal; and/or
- (b) you are suspicious of the transaction for any reason.

To obtain credit card authorisation please call the NAB KeyAuth service. Dial 13 25 15 and follow the prompts. NAB KeyAuth service is provided at no cost to EFTPOS customers.

Where applicable, authorisations for American Express or Diners cards can be obtained by contacting:

American Express 1300 363 614

Diners 1800 331 112

4. Fallback transactions for EFTPOS terminals

We are committed to delivering a continually high level of uninterrupted service to you. However, there may be times when system issues, telecommunications faults or faulty terminals prevent us from doing so. In the event of a system outage, your terminal may function in fallback mode.

Fallback transactions

Fallback transactions are transactions that are processed by an electronic terminal when the terminal is offline. Incorrect processing of a fallback transaction greatly increases the risk of the transaction being charged back. A fallback transaction may occur in the event of the terminal being unable to communicate with NAB.

You should refer to your terminal user guide for instructions on fallback transactions.

Please note that not all terminals operate in fallback mode. If in doubt, refer to your terminal user guide or revert to a manual back-up system to process transactions.

Processing transactions during a system outage

If your terminal is not operating in fallback mode during a system outage, it is necessary to complete and settle the transactions manually. This is done through the Purchase service on the NAB KeyAuth (13 25 15).

If you have chosen to have a manual imprinter, you may use backup stationery to enable you to continue with your normal business transactions.

Manual vouchers are referred to in the stationery brochure as:

Credit Card Merchant Sales vouchers for credit card transactions (Item code 141-153).

Manual transactions must not be used to process transactions on faulty or damaged cards, for declined transactions or for incorrect PIN attempts.

Your terminal user guide provides instructions on when, and when not to process manual transactions.

If your electronic terminal is operating in fallback mode, it will capture cardholder information and you do not need to use the card imprinter.

5. Pre-authorisations

This paragraph 5 only applies where you have been approved for pre-authorisation transactions. Pre-authorisations 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.

6. 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. Your terminal user guide provides instructions for processing off-line transactions.

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

7. 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.

For further information, please review our 'Protect your Business from Card Fraud and Payment Scams website' carefully and follow the guidelines it contains.

8. 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.

Please review our Protect your Business from Card Fraud and Payment Scams website carefully and follow the guidelines. For further advice refer to www.nab.com.au or contact our Merchant Fraud Team on 1300 668 046 or via email at

Merchant.Fraud@nab.com.au

Authentication

Authentication enables you to reduce the risk that the payment you are accepting is being made on a card being used by a person other than the valid cardholder. If you use authentication you can reduce chargebacks significantly, but you must adopt authentication software that has been approved by the card schemes and is up to date. If you continue to use 3-D version 1, after 17 October 2021, fraud **chargeback liability protection for approved Verified by Visa and Mastercard Securecode authenticated transactions will no longer apply**. This means you may receive fraud related chargeback transactions, which you will be expected to pay even though the transactions were authenticated. To read more about it visit this link <https://www.nab.com.au/business/payments-and-merchants/merchant-support-centre/card-not-present-fraud> For advice on how to install an approved authentication service you can contact NAB or your gateway provider.

NAB Transact, NAB Gateway

NAB Transact and NAB Gateway, are electronic payments and receivables channels. They provide you with a centralised technology interface for accessing a range of NAB Products.

In order to access NAB Transact and , NAB Gateway you need to nominate a person to be your Administrator. Your Administrator will be issued with a NAB User ID and a PIN or password.

If you become aware that a PIN, password or User ID has been compromised or divulged, or if you believe there has been unauthorised access to NAB Transact or NAB Gateway, please notify NAB immediately by calling 1300 138 313. You may be required to provide information about how the incident occurred.

New NAB Gateway Service

NAB is in the process of rolling out a new e-commerce payment gateway which will allow its e-commerce customers to accept many more payment types and the benefit of current technology. The merchant agreement has been amended to facilitate the migration of NAB Transact customers to the new channel and we will be contacting those customers to let them know when they are eligible. Work will continue on the gateway service with new functionality from time to time.

9. Storage of cardholder data

If you have access to, or 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.

For further information on these guidelines please email PCI@nab.com.au. 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.

10. 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. For further information, please refer to our Protect your Business from Card Fraud and Payment Scams website.

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 recognise. 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 terminal (where applicable) or contacting the Merchant Service Centre for assistance on **1300 369 852**.

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 NAB in the form of a Chargeback and/or a Retrieval Request (Refer to Section 10 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 NAB on:

Responses – RFI.Responses@nab.com.au

Chargeback Queries – merchantchargebacks@nab.com.au

For Further assistance with the chargeback process you can call us on: 1300 781 935 Option 4. M-F 8am -5pm

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.

If you are not happy with the outcome of a disputed transaction you can contact NAB Merchant Service Centre on 1300 369 852 and we will do our best to resolve the situation.

11. The chargeback process

Once a cardholder disputes a transaction, their bank will contact NAB on their behalf to verify the details of the transaction. NAB 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.

NAB 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 NAB (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 NAB 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 EMV Visa Secure and MasterCard Identity Check.) Refer to paragraph 8 for more details.

12. 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 terminal 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.

Should your terminal allow refunds, the transaction should be refunded to the cardholder through your terminal. Please refer to your individual terminal user guide for instructions on processing refunds.

Manual refunds

If your merchant service is unable to refund transactions electronically, contact the Merchant Service Centre on **1300 369 852** for assistance.

13. 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. For further information, please review the Protect your Business from Card Fraud and Payment Scams website. **Remember, if a sale seems too good to be true or suspicious in any way, it may be fraudulent!**

Use of counterfeit or stolen cards

Always ensure that a card is inserted or swiped through a terminal/PIN pad, a contactless card or device is tapped on or near the terminal or take a manual imprint of the card.

Don't have key-entry switched on unless it is necessary for your business and you have our permission. Key entry can be used by fraudsters who have access to or gain control of your terminal to enter fraudulent transactions. If you are using the terminal in key entry mode make sure it is never left unattended, is password protected and that the password is changed regularly. Be alert to the possibility that customers might be distracting you in order to gain access to your terminal. It is easy to have key entry switched off simply contact the help desk.

By ensuring that every transaction, where possible, is processed via your terminal and an electronic authorisation obtained, you are reducing your potential exposure to the use of stolen or counterfeit cards.

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 transactions where the card is physically present at the time of the transaction:

- (a) for contactless transactions, ask the cardholder to tap the card against the contactless card reader and, if prompted, enter the PIN
- (b) always attempt to swipe or insert the card through your terminal and have the cardholder enter their PIN when prompted, or take an imprint of the card and have the purchaser sign the sales voucher; and
- (c) where prompted to obtain a signature or where using manual vouchers, check the signature and compare the purchaser's signature with the signature on the card; and
- (d) familiarise yourself with built in security features of cards such as holograms and validity dates; make sure these are checked.
- (e) If you have key entry switched on never leave your terminal unattended.

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.

Please review our Protect your Business from Card Fraud and Payment Scams website carefully and follow the guidelines contained.

For further advice refer to www.nab.com.au or contact our Merchant Fraud Team on **1300 668 046** or via email at Merchant.Fraud@nab.com.au

14. Chip enabled EFTPOS terminals

A chip enabled EFTPOS terminal accepts existing magnetic stripe cards and cards carrying an embedded microchip.

Chip cards, also known as smart cards or EMV cards (the global industry standard for chip enabled cards established by 'Europay, MasterCard & Visa') aim to protect merchants and customers from counterfeit cards and fraudulent activity.

Chip cards have the capacity to store information in a very secure way, with greater capability, applications and enhanced security.

When a cardholder makes a purchase with a chip card, the card must be inserted into the card reader on the terminal. Chip enabled terminals will prompt merchants to 'insert' the card if the card has been 'swiped' as the magnetic stripe will detect if the card is a chip card.

The chip card will then remain in the terminal throughout the transaction and send a message for authentication. When the card supports a PIN, the terminal will prompt you for a PIN.

15. Hotel/motel accommodation providers

This Section 15 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.

16. Motor vehicle rental agencies

This Section 16 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.

17. Subscriptions Transactions

This section 17 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 enroll 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.

18. UnionPay International (UPI)

Some NAB terminals 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.

19. Contactless-enabled terminals and Merchant Choice Routing

A contactless-enabled terminal is a NAB EFTPOS terminal which has a NAB Contactless Reader attached to, or embedded within, the terminal. Your contactless-enabled terminal accepts magnetic stripe cards, chip cards and contactless cards and can also process transactions by inserting or swiping a card, including a contactless transaction.

The terminal will prompt you to insert or swipe the card if the NAB Contactless Reader cannot process the contactless transaction. The transaction is then processed as a normal card transaction and a PIN may be required.

Please follow the prompts on the terminal and the reader to complete a transaction and obtain authorisation.

Merchant choice routing is a service that routes contactless scheme debit transactions via the most cost effective network. NAB may automatically enable Merchant Choice Routing on your NAB EFTPOS terminal. It reserves the right to disable it if at any time this is necessary in your interests or for regulatory or other causes.

If NAB has not automatically enabled merchant choice routing on your terminal you may contact the Merchant Service Centre or your Relationship Manager and request it. If you have more than one terminal you may need to accept merchant choice routing across all of your terminals without the ability to select.

Transaction receipts for contactless transactions are optional however you must provide a receipt when asked by the cardholder to do so. A transaction receipt is not automatically generated and the terminal may prompt you to choose whether a transaction receipt is to be issued.

20. Stationery

Some Merchants have the ability to order stationery rolls via their terminal. Please refer to your terminal user guide for instructions. If you have any stationery queries, or to place an order, call our Merchant Service Centre on **1300 369 852** (select Option 5).

Current stationery listing and prices can be obtained from our 'Stationery ordering made easy' brochure, online at www.nab.com.au or by contacting the Merchant Service Centre.

21. Contact us

Help desk support

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

Call the Merchant Service Centre on **1300 369 852**
24 hours a day, 7 days a week or visit www.nab.com.au

NAB Transact Technical Help Desk is available on **1300 369 852**, 8.00am to 8.00pm weekdays.

Authorisations

Credit Card **13 25 15**

American Express **1300 363 614**

Diners Club **1800 331 112**

Authorisation services are available 24 hours a day, 7 days a week.

Sales enquiries

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

Call our sales consultants on 1300 EFTPOS (1300 338 767) 8.00am – 6.00pm AEST/AEDT Monday to Friday.

Ask your relationship manager

Visit us at www.nab.com.au

Merchant fraud team

For fraud related enquiries:

call **1300 622 372** (Option 3)

email **Merchant.Fraud@nab.com.au**

22. Complaints

If you have raised an issue with NAB but do not feel it has been resolved to your satisfaction, you can contact the NAB Resolve team on 1800 152 015. If your concerns still have not been resolved to your satisfaction, you can lodge a complaint with the Australian Financial Complaints Authority (AFCA):

Website: **afca.org.au**

Email: **info@afca.org.au**

Telephone: **1800 931 678** (free call)

In writing to: Australian Financial Complaints Authority, GPO Box 3, Melbourne, VIC 3001

AFCA is an External Dispute Resolution (EDR) scheme to deal with complaints from consumers in the financial system. AFCA provides fair and independent financial services complaint resolution that's free to consumers.

