



CREDIT CARD FRAUD PROTECTION

how to protect your business
and your customers



nab

INTRODUCTION

It is an unfortunate fact that many businesses will encounter a customer who presents a credit card or a credit card number that is not rightfully theirs.

Credit Card Fraud is a reality and is increasing in the retail market environment, exposing merchants to potential losses that could be damaging to their business.

At NAB, our aim is to assist merchants to minimise fraud through the use of sophisticated fraud detection tools and pro-active merchant education.

Please make the time for you and your staff to review this Credit Card Fraud Protection booklet and the attached DVD.

The more you know about the potential risks, the more you'll be able to protect your business against chargebacks and fraud.

HOW TO BEST PROTECT YOUR BUSINESS

Make sure the sale counts

It is easy to get carried away in the moment when a customer wants to buy large quantities of stock and doesn't try to bargain the price down. The bad news is that when it seems 'too good to be true' it probably is. You should always be on the lookout for any unusual behaviour.

It is important that you train your staff well and teach them to trust their instinct. Being vigilant about suspect behaviour and unusual spending is your first line of defence. If a credit card payment turns out to be fraudulent, it could end up costing you more than the original sale was worth.

Know the consequences

It is important to be aware of how accepting a fraudulent transaction can affect your business.

Some forms of payment carry an increased risk that you, as the merchant could be liable for transactions when the cardholder disputes them.

High-risk transactions

- Card Not Present
- Card number is manually keyed in
- No authorisation obtained
- Card is not swiped through EFTPOS terminal
- Fallback transactions

Lower risk transactions

- Card Present
- Card is swiped through EFTPOS terminal
- Imprint of card obtained with signature and authorisation
- Verified by Visa/MasterCard Securecode Transaction

High chargeback levels and/or the acceptance of excessive fraud could attract penalties from the Card Schemes (Visa or MasterCard) and in some cases, this could even result in the termination of your merchant services by NAB.

RESPONSIBILITIES

Merchants should be aware of their responsibilities under the terms and conditions of the merchant agreement. At all times, it is your responsibility as the merchant, to verify that the purchaser of goods and services is the genuine cardholder.

Your merchant agreement specifies that you are responsible for preventing fraud occurring via your merchant services, ensuring the physical security of your merchant equipment and the protection of cardholder information. For this reason it is essential that you understand:

- How your business can become a target of fraud.
- How fraud can be detected.
- Your liabilities.
- Precautions you need to take.

Third Party Transactions

At no time should a merchant process transactions on behalf of a third party. Not only will you pay the merchant service fee but you will also be liable for any chargebacks that arise from these transactions. Processing transactions on behalf of a third party without prior authority from NAB, is a breach of your merchant agreement and may result in the termination of your merchant services. In addition you may also be open to possible fines for breaching the card scheme rules.

Proprietor Transactions

Funds transferred from a credit card in the proprietor's name via their merchant services to their settlement account are classified as a Proprietor Transaction. Transferring funds in this manner is not only costly (you will be charged a merchant service fee for each transaction) but a breach of your merchant agreement. For

transactions such as transfers and bill payments you will need to utilise other banking services.

Splitting Transactions

If a transaction is declined, it is generally for a good reason. Do not lower the sale amount in an attempt to complete the sale on one card or split the sale over two or more cards. A transaction may be considered invalid and may be charged back if an attempt has been made to split a purchase, effectively avoiding your floor limit.

Securing Your Equipment

You are responsible for the physical security of your merchant services. It is important that you secure your terminal equipment safely and never leave your terminal unattended during trading hours. You should never allow a cardholder to instruct you on how to process a transaction or have access to your terminal.

Fraudsters may approach your business posing as a terminal, electrical or phone line technician advising that they need access to your terminal. They may then process refund transactions or insert card readers into your terminal that will enable them to steal cardholder information whenever the card is swiped.

Always check the identification of technicians attending your premises and never reveal any passwords. If suspicious contact the Merchant Service Centre on **1300 369 852**.

Changes to Your Business

As a merchant, it is also your responsibility to advise NAB of any significant changes to your business. This may include but is not limited to, the business address and location of the EFTPOS equipment or a change in business name. If you would like to change the types of goods and services your business provides, you should obtain prior approval from NAB.

REFUND FRAUD

A common type of fraud involves employees issuing credits (refunds) to their own account via your EFTPOS terminal. To avoid detection they may create a large sale on a fraudulent card then process a refund to their own card. Refunds may also be processed to their own cards without a corresponding sale.

To guard against this type of fraud, we recommend you closely monitor all refunds, checking that all refunds correspond to a legitimate sale and are refunded back to the original purchase card. Particular attention should be paid to large refund amounts.

Ensure only authorised staff are aware of your refund limits and refund password. Your refund password should be changed when your terminal is installed. It should be unique, changed frequently and kept secure.

FALLBACK TRANSACTIONS

Fallback transactions are transactions that are processed when the terminal is offline. A fallback transaction may occur due to a technical reason where the terminal cannot connect with the bank. Incorrect processing of a fallback transaction greatly increases the risk of chargebacks.

A fallback transaction is easy to identify as the transaction receipt has the word 'fallback' or 'offline' printed on it. The terminal will also ask you for an authorisation code to complete the transaction.

Note: The terminal is not asking for your refund password.

To obtain the authorisation code, please call:

For Credit Cards: **13 25 15**

For Debit Cards: **1300 369 852**

Once an authorisation number is received, enter this into your terminal to complete the transaction.

Repeated fallback transactions are uncommon and if this occurs you should seek advice from your terminal supplier or by calling the Merchant Service Centre on **1300 369 852**.

For more information refer to your merchant agreement or your terminal user guide.

CHARGEBACKS

You, as the merchant may be faced with the prospect of incurring chargebacks, which can have a financial impact on your business.

A chargeback occurs when the cardholder (or their bank) raises a dispute in connection with a credit card transaction. If the dispute is resolved in favour of the cardholder, the transaction is 'charged back' and debited to your settlement account. In other words, you as the merchant could possibly lose the value of the sale and incur a chargeback fee.

Common reasons for chargebacks include but are not limited to:

- Cardholder does not recognise the transaction (Business name on statement is not recognised).
- Cardholder did not authorise the transaction (Frequently an indication of fraud).
- Cancelled recurring transaction.
- Goods/services not as described.
- Goods/services not received.
- Goods faulty or defective.
- No authorisation obtained.

Chargebacks can generally be raised by either the cardholder or their bank up to 12 months from the transaction date, or from the date the goods or services should have been provided. For this reason, you are required under your merchant agreement to retain all sales vouchers and information for a minimum of 18 months.

Chargeback Process

Once a transaction is disputed a 'Retrieval Request' will be sent to you, the merchant to request transaction evidence such as a signed transaction receipt to support the sale. You then have ten days from the date of the letter to respond with the relevant information.

Responsibility lies with you, the merchant, to provide satisfactory supporting documentation to prove that a valid transaction occurred and/or that the cardholder authorised the transaction. If you cannot provide evidence to support the sale, liability for the chargeback lies with you.

It is important that you respond to all retrieval requests promptly and within the time frames specified. Late or no response to a retrieval request will result in a chargeback being debited to your settlement account.

Refunds should not be attempted once a retrieval request has been sent or a chargeback has been processed as this may result in your settlement account being debited twice.

Attempting to re-process a transaction once it has been charged back violates card scheme regulations and could lead to the termination of your merchant services.

CARD PRESENT TRANSACTIONS

While trusting your customers is important, this should not be at the expense of good business sense. This means ensuring that whenever the card is present that staff undertake additional security measures to ensure the card is not a counterfeit (fake) and that the purchaser is the genuine cardholder.

When a card is presented at the point of sale hold onto it until the transaction has been completed and always check the following:

Check the card back and front:

- Are all the security features in place?
- Does the card appear to have been tampered with?
- Does the name match the customer?
- Is the card valid?
- Is the magnetic stripe smooth and free of signs of tampering?
- Does the signature panel show any signs of tampering?
- Has the card been signed and does the signature match?
- Is the signature signed in pen and not texta or pre printed on the plastic?

Take note of the embossing:

- Is the embossing clear and well aligned?
(Although most cards are embossed, there are some exceptions).
- Can a ghost image be seen?
(Original embossed details on the card that have been flattened).
- Do the first four digits of the embossed card number match the pre-printed four digits directly below the embossing? (There are some exceptions).

Check the hologram or the holomag:

- Does the image appear three-dimensional and change colour when tilted?
- Can it be scratched or does it lift off?

Check the card number:

- Does the entire or abbreviated (i.e. first six and last three digits) card number match the printed receipt?

While checking the above features, take note of the customer's behaviour. Some of the below situations on their own may not be cause for alarm but in combination they could be an early indicator that something is not quite right.

Be wary in situations where:

- Customers appear nervous or anxious or hurry you at closing time.
- Customers make indiscriminate purchases, possibly with a newly valid card, without regard to size, style, colour or price.
- Customers purchase a large item and insist on taking it with them, refusing delivery.
- You are requested to split transactions over two or more cards and/or a number of cards are presented with multiple declines.
- Customers who are quick to take the card back from you preventing you from checking the security features.
- Customers who choose an item in store and tell you that they will phone through a card number and provide a delivery address.
- Customers who make numerous purchases under your floor limit.
- Customers who ask you to manually key a transaction providing the card number from memory, a slip of paper or an old sales voucher.
- Customers who need to see the card in order to sign the sales receipt.

It pays to swipe the stripe

Always attempt to swipe the card through your terminal or take a manual imprint of the card if given the opportunity. Key entering a card number greatly increases your exposure to chargebacks, as there is no proof that the card was present for the transaction.

Remember, if you are suspicious of a transaction:

- Contact NAB Keyauth on **13 25 15** and go through to 'extension 500'.

If you cannot confirm the transaction beyond your suspicions:

- Decline the transaction or ask for another form of payment.

If you have identified the transaction as fraudulent:

- Contact your local police.
- Attempt to retain the card.

Remember your safety comes first don't take any chances.

CARD NOT PRESENT TRANSACTIONS

Internet and mail order/telephone order (MOTO) transactions are commonly referred to as 'Card Not Present' transactions.

Merchants that accept Card Not Present transactions are at a greater risk of becoming victims of fraud, as fraudsters take advantage of the anonymity Card Not Present purchases provide. Fraudsters are able to make purchases anytime, with or without a physical card, from anywhere in the world making Card Not Present transactions a preferred method of trade.

For this reason it is important you understand the possible warning signals to identify suspicious or unusual transactions for your business. We suggest that you undertake additional security measures whenever you accept a credit card for payment in a Card Not Present environment.

When Taking an Order

- Obtain the credit card number, name of the bank, expiry date, full name, address and contact phone numbers, including landline contacts.
- Conduct a White Pages or Telstra check on the details provided to verify name and telephone number.
- Confirm the order by calling the landline number provided and/or send confirmation of the order to the billing address, not the shipping address.
- Make sure a reputable courier engaged by you makes the delivery. Use a courier that does not allow shipping re-routes.
- Ensure delivery is to a physical address. Never send deliveries to a hotel, motel or GPO Box.
- Ensure that the person making the delivery does in fact deliver the goods to a person inside the premises.
- Obtain a manual imprint of the card and signature wherever possible on delivery.

- Do not continue to attempt authorisation or split a transaction after receiving a decline.

Suspicious Orders – What to Look For

Being vigilant about unusual spending can help you identify early warning signals that something may not be right with an order. While aspects of the following situations may occur during a valid transaction, combinations of these situations may be cause for alarm.

Be wary in situations when:

- You are requested to split transactions over a number of cards.
- Multiple cards are presented with multiple declines within a short period of time generally via your Internet payment page. These cards may have the same BIN (first six digits) or may appear to be sequential with only the last four digits changing.
- Customers who place a number of orders within a short space of time.
- Items that are ordered in unusual quantities and combinations and/or greatly exceed the average order value.
- Orders marked urgent or shipped overnight to deliver fraudulently obtained items as soon as possible for quick resale.
- Orders from Internet addresses using free email services.
- Orders placed where the initiator of the order admits it is not their card being used.
- Orders shipped to international destinations you may not normally deal with.
- Orders received from locations where the goods or services would be readily available locally.
- Orders for additional products you do not normally sell.
- Orders are cancelled and refunds are requested via telegraphic transfer to an account other than the original purchase card.
- Goods or services have been ordered over the phone to be collected in person at a later date. (Make sure you sight the card and swipe or take an imprint with a signature upon collection of the item).

International Orders

We suggest that you express caution when receiving any international orders; particularly from countries you do not normally deal with or if you do not normally trade internationally. While all international orders carry an increased fraud risk, transactions originating from the below locations have shown to generate high levels of credit card fraud:

- Nigeria
- Ghana
- Indonesia
- Singapore
- Eastern Europe

Suspicious of the Transaction?

If you cannot verify that the payment details provided are genuine, or you are suspicious of the purchaser or the transaction, ask for an alternative form of payment such as a telegraphic transfer. If the customer refuses, we recommend that you process a refund to the card and **DO NOT** send the goods.

Remember it is your responsibility to confirm the purchaser is the genuine cardholder before providing the goods and service, as you may be liable for the transaction if it is disputed.

Reducing the Risk of Internet and MOTO Fraud

Now that you are aware of how you can become a target for fraud you may be asking yourself ‘How can I reduce the risk?’ You can minimise the possibility of becoming a target for fraud by implementing the following measures:

1. Develop a standard credit card transaction checklist that all staff must use when taking an order.
2. Create a secure customer database. Include relevant information such as IP addresses, delivery addresses, abbreviated card

numbers etc and link these to transactions marked as suspicious or that have been charged back.

3. Advertise that you will prosecute identified fraudulent activity on your website. This may help in deterring fraud.
4. Discuss additional security with your service provider or an IT expert to help you redevelop your web/payment page. This could include blocking IP addresses, BIN ranges, CVV2 acceptance, Verified by Visa and MasterCard Securecode.

If you suspect that your website has become a target for fraud, we suggest that you shut the site down for a short period of time and conduct an investigation on where the fraud is coming from. If it is possible, block the IP address from which the orders are originating.

Card Verification Value (CVV2/CVC2) or Card Identification Number (CID)

The Card Verification Value or CVV2 is the three-digit number located on the signature panel of the credit card. For AMEX cards the Card Identification Number (CID) is the four-digit number on the front of the card.

If the purchaser cannot provide this number it is likely that they are not in possession of the card and are using card details that they have fraudulently obtained. It is important to note that validation of the CVV2 or CID is not a guarantee of payment or that the card is not a stolen card, it simply confirms that the purchaser has the card in their possession.

To prevent the CVV2/CVC2 or CID data from being compromised or stolen never keep or store the CVV2/CVC2 or CID data once it has been provided and utilised for the original transaction.

Verified by Visa (VbV) and MasterCard Securecode

Verified by Visa (VbV) and MasterCard Securecode are online cardholder authentication programs developed by the card schemes.

VbV and Securecode work in the following way:

- A cardholder registers with their issuing bank.
- The cardholder then creates an authentic password (similar to that of an ATM PIN).
- When a cardholder makes a purchase via your web page they are requested to input their online password.
- The details are then sent through to the cardholder's issuing bank for authentication.
- If the password is incorrect we recommend that you do not proceed with the transaction.

SECURING YOUR CUSTOMER'S DATA

Merchants that do not keep cardholder data safe and secure open themselves up to possible legal action and fines if cardholder data is compromised.

As a merchant you are always dealing with sensitive cardholder information. NAB recommends that you are pro-active in safeguarding all customer data held either electronically (eg a computer database) or manually, (eg manual imprints and transaction receipts).

If data is held electronically, a merchant should comply with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS contains requirements and guidelines and is endorsed by all major credit and charge card payment brands including Visa, MasterCard, American Express, Diners Club and JCB.

It is a requirement that paper records and transaction documentation is stored for 18 months. This information is to be stored securely with restricted access. Any theft must be reported to the NAB immediately.

How do you protect customer information?

- Ensure that all computer systems have a unique password.
- Conduct a network scan on all your external facing IP addresses by visiting ScanAlert.com
- Protect systems that store and/or transmit card data with Anti-Virus software.
- Utilise a firewall with stringent and granular security rules at all entry points. Intrusion Detection Systems should be strategically placed within the network as needed.
- Do not store Card data on Internet facing systems.
- Encrypt data maintained on databases or files, and any data sent across networks.
- Securely destroy data when it is no longer needed for business reasons.
- Limit access by your employees to account data on a need-to-know basis and remove access to your network and premises if an employee leaves your business.
- Ensure files and transaction documentation are kept out of reach of customers.

Do not store the following after authorisation:

- Sensitive cardholder information i.e. full contents of track data from the magnetic stripe of the card.
- Card Verification Numbers (CVV2/CVC2/CID).
(Three digits on the back of the card or four digits on front of card for AMEX).

Remember: Store only the customer's account information that is necessary for your business and only with the cardholder's knowledge and consent (e.g. name, address or email address).

Destroy Cardholder Information After Use

If you are utilising manual paper facilities you must ensure that all carbon copies on manual imprints are destroyed in such a way that the details are unreadable. The same can be said for sales vouchers printed via EFTPOS terminals. This is to ensure that the carbon copies and terminal sales vouchers cannot be retrieved from the rubbish, enabling fraudsters to use the data.

Report All Security Incidents

You are required to immediately notify NAB if it is identified that transaction data has been accessed or retrieved by any unauthorised entity. This allows procedures to be implemented immediately to reduce the usage of compromised data, protecting your customers, but also reducing the potential financial losses for you and others.

For further information on storing electronic data securely, email pci@nab.com.au quoting your merchant number. Or visit:

- <http://www.visa-asia.com/ap/seamerchants/riskmgmt/ais.shtml>
- <http://sdp.mastercardintl.com>
- <http://www.scanalert.com>

Ensure your business complies with the full PCI Standards by completing the SAQ available on any of the websites listed above.

CHINA UNIONPAY

China UnionPay (CUP) is a card scheme that originates from Mainland China & also operates throughout parts of Asia. CUP issues both debit & credit cards that can be accepted at selected merchants across Australia.

When accepting payment on a CUP card remember the following:

- All CUP cards MUST be swiped through your terminal to obtain an online authorisation.

- Neither fallback nor manual processing is allowed.
- CUP cardholders must sign the transaction receipt and enter a PIN for all CUP card types.
- Behaviour and card security checks should always be conducted as per the Card Present section in this booklet and the Card Security Features document.

If a CUP card is presented and the transaction is declined due to incorrect PIN, decline the transaction. Authorisation for CUP card transactions cannot be obtained by contacting NAB KeyAuth. If a transaction declines you cannot accept the card for payment. Advise the cardholder to contact their bank.

Co-Branded CUP Cards

CUP credit cards can also be co-branded with MasterCard or VISA and will display the logos of both schemes ie: CUP and Visa Logo or CUP and MasterCard logo will appear on the front of the card. Co-branded cards can be accepted as per the above procedures and must be authorised with both PIN and signature.

EMV (EUROPAY MASTERCARD VISA) – CHIP CARDS

A chip card is a card containing a smart chip loaded with the information normally contained within the magnetic stripe of a card. The chip also contains further enhanced security features, which may include a PIN to complete the transaction, making the production of counterfeit cards more difficult.

Chip cards have been introduced to limit the impact of counterfeit card activity and will eventually replace magnetic stripe based cards, which are still vulnerable to card skimming. During the transition period, chip cards will also be produced with a magnetic stripe.

AUTHORISATION

An authorisation confirms the following information at the time of the transaction:

- The card has not been reported as lost or stolen.
- There are sufficient funds to cover the purchase.

An authorisation does not confirm payment or that the person providing the card details, is the genuine cardholder. A risk remains that the purchaser has improperly obtained the card or card details. This risk is increased for Card Not Present transactions.

Suspicious Cardholder

If you are suspicious of:

- The cardholder
- The card

Dial NAB KeyAuth on **13 25 15** and go through to 'extension 500'. (You will be transferred to an operator who will assist you).

Remember:

- Only use 'extension 500' if you are suspicious of the transaction. Do not use 'extension 500' if you simply need to obtain an authorisation.
- Authorisation for CUP card transactions cannot be obtained by contacting NAB KeyAuth. If a transaction declines you cannot accept the card for payment. Advise the cardholder to contact their bank.

Debit Cards and Charge Cards

Fraudulent transactions can also occur on Debit and Charge Cards (AMEX, Diners and JCB). Ensure that you apply the pre-cautions enclosed within this booklet to all Debit and Charge Card transactions.

For further enquiries on these types of transactions contact:

Debit Card **1300 369 852**

AMEX/JCB **1300 363 614**

Diners **1800 331 112**

PROTECTING OUR MERCHANTS FROM FRAUD

The NAB Merchant Fraud Team utilises ‘Pro-Active Risk Manager’ or PRM software to monitor irregular trading patterns. When a transaction occurs outside the normal trading behaviour of a merchant, and is identified on PRM, the transaction is brought to the attention of a fraud team member who can assess the transaction and follow-up where necessary.

In many instances, the use of PRM has resulted in NAB alerting a merchant to the use of counterfeit cards or other fraudulent activity in an almost real time environment resulting in a saving to our merchants.

However, PRM is only a component of a good fraud detection and prevention strategy, as PRM cannot always pinpoint every fraudulent transaction. You the merchant are often in the best position to identify suspicious activity and you need to understand your detection and prevention responsibilities.

This fraud education material has been developed to increase your understanding of how fraud can occur, the risks you face and how you can best protect your business.

CONTACT US

For further information on fraud prevention call the Merchant Fraud Team on **1300 668 046**. Or, email us at **Merchant.Fraud@nab.com.au**

Fraud prevention information and educational material is available online at: **national.com.au/merchantfraud**

Merchant services features

Further information on the security features of the merchant services you are currently using can be obtained by contacting your Electronic Banking Consultant or our Merchant Service Centre on **1300 369 852**.

Adopting some or all of these suggestions will not guarantee that you will not be exposed to credit card fraud. Your liability for credit card fraud is detailed in your merchant agreement.

PART 1

credit card fraud

PART 2

skimming

PART 3

chip cards

telephone: 1300 668 046
email: merchant.fraud@nab.com.au
national.com.au/merchantfraud