

Merchant Business Solutions.

Protecting business against credit card fraud.

Version 5.0 August 2017

200



200 years proudly supporting Australia

Contents

Protect your business	4
Authorisation	5
Chargebacks	6
Verification of Purchaser	7
Types of goods fraudsters target	8
Detecting suspicious orders	9
Card present merchants.....	9
Internet and MOTO merchants.....	10
Reducing fraud	11
How to reduce card present fraud.....	11
How to reduce Internet and MOTO fraud.....	12
Other risks merchants face	13
Laundering of sales (3rd Party Processing).....	13
Fraudulent refund transactions.....	13
Online authentication of purchasers.....	14
Risk Mitigation for Online Merchants	15
How to enable Verified by Visa and Mastercard® SecureCode.....	15
Secure your customers' data.....	15
Website requirements.....	16

Protect your business

Merchants face various risks when accepting credit card transactions. This brochure has been developed to assist you to understand the types of risks you face and actions that should be taken to reduce the risk of loss.

One of the greatest risks to merchants is that of fraudulent transactions.

If you are not careful, fraud can cost your business significant amounts of money. Certain types of merchants – based on the type of goods sold – are more prone to fraudulent transactions than others. Merchants should understand their likelihood of being targeted by fraud.

It is essential for merchants to have a sound understanding of credit card fraud, how it can be detected and how it can be prevented. These concepts are discussed below for the three broad types of credit card transactions:

- Card present (face-to-face) merchants;
- Internet merchants; and
- Mail Order/Telephone Order (MOTO) merchants.

Internet and MOTO merchants are commonly referred to as “Card Not Present” merchants where the credit card and purchaser are not physically present in the merchant’s shop at the time of purchase.

Examples include purchases where your customer provides their credit card details over the Internet, by fax, phone, or through the mail.

Note: Under no circumstances should you request that a customer provide Credit Card details via email for payment of the provision of goods and/or services, as per section 4.14 of the Terms and Conditions of your Merchant Agreement.

Many fraudsters prefer to make Card Not Present purchases due to the anonymity afforded by these payment methods. Also, Card Not Present situations enable fraudsters to place orders over the Internet or via MOTO all over the world.

If they reside overseas, the chance of criminal prosecution is much lower, which is an added incentive to this type of fraudulent behaviour. A large amount of credit card fraud is committed in Card Not Present situations and the volume of this type of fraud is increasing at a rapid rate.

HINT: Always adhere to the Terms and Conditions of your merchant agreement and to the Card Scheme rules.

Authorisation

It is essential that you understand the term 'authorisation' – what it means, and what it does not mean.

What authorisation **does** mean:

- The account number is valid.
- The card has not been reported lost or stolen (although it may in fact be lost, stolen or compromised [card details improperly obtained or copied] and the card owner is unaware).
- There are sufficient funds available to cover the transaction.

What authorisation **does not** mean:

- An authorisation does NOT confirm that the person providing the card number is the legitimate cardholder. The risk remains that the person providing the credit card number has either stolen or improperly obtained the card.
- There is also the risk that the purchaser has compromised (improperly obtained) the card number, without being in possession of the card.

Although it is important to obtain an authorisation for each transaction, it does not protect you from the risk of fraud or chargeback. Risk of fraud remains even though authorisation has been obtained.

HINT: Authorisation will not guarantee payment if the transaction is not made by the rightful cardholder.

Chargebacks

As a merchant, you face the prospect of receiving chargebacks. A chargeback occurs where the cardholder (or their bank) raises a dispute in connection with a transaction made through your business. If the dispute is resolved in favour of the cardholder, the transaction is charged back (debited) to your account. In other words, you lose the full sale proceeds.

Common reasons for chargebacks are as follows:

- Cardholder did not make the transaction (frequently an indication of fraud)
- Cancelled recurring transaction
- Goods not as described
- Goods faulty or defective
- Failure to respond to voucher requests

Chargebacks may also be made for a number of other reasons, including, but not limited to:

- Goods/services not received
- Exceeding merchant floor limit without obtaining authorisation

Chargebacks can generally be made by either the cardholder or their bank up to a maximum of 12 months from the transaction date, or from the date the goods or services should have been provided, where delivery was expected subsequent to payment.

Card Not Present merchants face additional chargeback risks that do not apply to merchants transacting in a card present environment. Specifically, due to the purchaser not signing a sales voucher, if the cardholder subsequently denies having made the transaction, you will generally be liable for the chargeback. This follows from the fact that you are unable to prove that the cardholder made the purchase.

For this reason, it is essential that Card Not Present merchants take steps to identify the purchaser, and ensure that the transaction is legitimate. The ways in which you can do this are discussed over.

HINT: Minimise the risk of chargebacks by becoming aware of how and why they occur.

Verification of Purchaser

At all times, the onus is on you to verify the purchaser is the genuine cardholder. This applies to all merchants irrespective of the method by which credit card payments are accepted.

It is particularly important for Internet and MOTO merchants to identify the purchaser however Westpac recommends that merchants accepting credit card payment in a card present environment also take steps to verify the purchaser, especially for large purchases.

If you sell goods to a purchaser who is not the genuine cardholder, you may be liable for the chargeback.

It is emphasised that authorisation does NOT constitute verification of the purchaser – the transaction may be fraudulent even though authorisation is obtained.

HINT: Remember that the onus is on you to verify that the purchaser is the genuine cardholder.

Types of goods fraudsters target

Due to their high value and ability to be re-sold, the following types of goods are frequently targeted by fraudsters:

- Electrical goods
- Household appliances
- Jewellery
- Computers
- Furniture
- Goods which are easily disposed of for cash

If you are selling any of these types of goods, we urge you to be extremely careful before handing over/shipping goods. In particular, take all possible steps to confirm that the purchaser is the genuine cardholder. This applies to all merchants whether selling in a face to face or card not present environment.

HINT: Fraudsters often target high value goods which are easily re-saleable.

Detecting suspicious orders

Card present merchants

Although less risky than selling in a Card Not Present environment, face-to-face transactions still pose risks to merchants. The indicators below are useful to detect potentially suspicious purchases:

- Orders for the types of goods detailed in the “Types of goods fraudsters target” section.
- Unusually large orders.
- Customers who purchase multiple numbers of the same item without regard to size, colour, style or price. Merchants should ask themselves whether it is likely that an individual would purchase a large number of a particular item.
- Customers who don't negotiate on price where it is customary to do so. The possibility exists that the person isn't concerned about the price because they have no intention of actually paying.
- Customers purchasing large or bulky items, but refusing home delivery despite its inclusion in the price. It may be that the customer doesn't want the merchant to know their address due to the purchase being fraudulent.
- Customers offering more than one credit card in connection with a single purchase.
- Customers who make repeated purchases in a short period of time.
- Customers who pull their credit card out of a pocket rather than a wallet.
- Customers who appear anxious, nervous or impatient.
- Customers who try to distract you at the time of processing the transaction, especially where the transaction is large.
- Where a large purchase is made on a newly valid card. The reason is that credit cards are sometimes stolen while being sent from the bank to the rightful cardholder.

HINT: If your customer behaves in a suspicious manner, remember that it is better to lose a sale than to lose the sale and the proceeds.

Internet and MOTO merchants

The following are indicators of potentially suspicious Internet and MOTO transactions. Frequently, it is the presence of more than one of these factors that indicates possible fraudulent activity:

- Orders for the types of goods detailed in the “Types of goods fraudsters target” section.
- Unusually large orders.
- Orders for multiple quantities of the same item.
- Customers who place a number of orders within a short space of time.
- Customers who place orders using multiple credit cards.
- Orders placed where the first card offered is declined, and a second card is immediately offered.
- Orders requiring urgent shipping.
- All overseas orders, especially where the order is from a country from which you don't usually receive orders.
- Orders shipped to a country where the goods could easily be purchased locally. The question must be asked why the purchaser is prepared to pay the shipping expense, and wait longer for the goods to arrive.
- Orders from Internet addresses using free e-mail addresses.
- Orders requesting delivery to a Post Office Box.
- Orders requesting the goods to be shipped to a third party.
- Orders where the only contact number provided is a mobile phone.
- Orders made within a short period of time on credit card numbers that are very similar, such as where only the last four digits differ.
- Orders for goods not normally supplied by your business.

While all orders from overseas countries represent an increased fraud risk, transactions originating from the following countries have been identified as generating a disproportionate level of credit card fraud:

- Nigeria
- Indonesia
- Eastern Europe

HINT: Merchants suspicious of either the purchaser or the transaction are recommended not to ship the goods, even though the transaction has been authorised.

Reducing fraud

Merchants are frequently targeted by fraudsters who process fraudulent transactions and subsequently request that refunds be paid by other means such as a wire or telegraphic transfer.

These fraudsters approach a merchant (often in the hospitality industry to book accommodation or purchase services) and provide fraudulent credit cards. The booking or service is then cancelled and the merchant is asked to make a refund to another account (often via a money transfer solution).

In some instances the merchant is offered an “incentive” to comply with this request, such as a specific amount of money or a percentage of the total value of the transaction.

Invariably the initial transaction is fraudulent and is charged back by the cardholder, and as the merchant has already remitted the funds they have to accept the chargeback as a loss.

You are reminded that you must comply with section 5.2 of the Terms & Conditions of your Merchant Agreement, which states, in part:

“You shall not process any refund to a Card account unless the original transaction between you and that Cardholder was paid for by the Cardholder using the relevant Card”.

HINT: By always processing refunds only to the card on which the initial sale was made, you will protect yourself against this type of fraud.

How to reduce card present fraud

Apart from being alert to potentially suspicious transactions, merchants’ main defence against fraud in card present situations is to carefully inspect the card to ensure it is genuine, and check that the signature on the back of the card matches the purchaser’s signature on the sales voucher.

The following security checks should also be performed:

- Closely inspect the card. Check that the “valid from” and “valid through” dates include the current date.
- Check that the card has the appropriate security measures.
- Check that the first four digits of the embossed account number match the four digits printed immediately above or below the embossed number.
- When tilting the card, the hologram on Visa and Mastercard® credit cards should move and/or change colour.
- On the signature panel on the back of the card, check that the words “Visa” and “Mastercard” appear repeatedly at a 45 degree angle.

- Check that the abbreviated credit card number on the sales receipt matches the corresponding digits on the card. If the digits don't match, this is a clear indication the card is counterfeit.
- Closely inspect both the front and back of the card to determine whether any part of the card appears to have been altered.

HINT: Remember to inspect the card to ensure it is genuine.

How to reduce Internet and MOTO fraud

Merchants can minimise the possibility of fraudulent purchases and chargebacks from Internet and MOTO transactions by implementing the following measures:

- Request the purchaser to provide the CVV2 (Visa) or CVC2 (Mastercard®) three digit number located on the signature panel of the credit card. If the purchaser is not in possession of the card, it is unlikely they will know this number.
- Request the name of the cardholder's bank. Fraudsters who have compromised account details will not have this information. If the purchaser hesitates in advising the name of their bank, caution should be exercised.
- Request the purchaser to provide a fax copy of their driver's license.
- Ensure the customer's billing address and delivery address is consistent.
- Check the telephone book to verify address and phone numbers provided.
- Never forward goods to a Post Office Box.
- Obtain a signed receipt from the cardholder when the goods are delivered.
- In the case of orders for a large number of different goods, telephone the cardholder after the order is placed to confirm the order. Also, have the purchaser read back all details of the order. Frequently, where an order is fraudulent, the purchaser will be unable to confirm these details, as they were ordering at random, with no record of what they ordered.
- Be suspicious where multiple cards are used for a single purchase.
- Don't continue to attempt authorisation after receiving a decline.
- Exercise particular caution in relation to overseas orders. Large orders should in all cases be held back for shipping while the above enquiries are made into the legitimacy of the purchaser. Merchants should not ship goods until satisfied that the purchase is legitimate.

HINT: Be especially cautious of overseas transactions.

Other risks merchants face

Laundering of sales (3rd Party Processing)

The term “laundering”, in a merchant context, refers to a situation, such as, where a business with a valid merchant facility accepts transactions on behalf of another business. Disreputable individuals sometimes approach legitimate merchants to process their credit card transactions, generally paying the merchant a percentage of the amount processed. Apart from constituting a serious breach of Westpac’s terms and conditions it is also an extremely dangerous practice opening up a merchant’s business to significant risk of loss.

Merchants engaging in laundering/processing transactions on behalf of another business are liable for all chargebacks arising from these transactions. In many cases, the individual approaching the merchant to process their transactions is unable to obtain a merchant facility of their own, possibly due to previous improper merchant practices. Consequently, the chance of fraudulent transactions being processed is extremely high.

A merchant **must not**, process transactions on behalf of someone else or in connection with a transaction that did not involve them directly selling goods or services to their customer.

HINT: Laundering, in a merchant context, is an extremely dangerous practice which may lead to significant loss.

Fraudulent refund transactions

A common type of fraud involves employees issuing credits (refunds) to their own account. To avoid detection, they may create a large debit transaction on a fraudulent card and an offsetting credit on their own card. In this type of situation, it is likely to take weeks, even months, before the fraud is detected. To guard against this type of fraud, we recommend that merchants closely monitor all credits, and check that all credits and corresponding debits relate to the same card number. Particular attention should be paid to large credits.

Another way in which merchants can protect themselves from this type of fraud is by regularly changing their terminal or user password(s), especially after an employee has left.

HINT: Ensure your password is changed regularly to prevent unauthorised use.

Online authentication of purchasers

The primary risk facing merchants accepting Internet transactions is the difficulty faced confirming the purchaser is the genuine cardholder. Where a cardholder disputes having made an online purchase, irrespective of whether this is actually the case, the merchant is generally liable for the chargeback.

Visa and Mastercard® have jointly attempted to overcome this burden placed on Internet merchants by developing an online cardholder authentication service known as 'Verified by Visa' and 'Mastercard SecureCode'. A term called '3D Secure' refers to the technology platform through which this service is offered.

Verified by Visa and Mastercard SecureCode works as follows:

- A cardholder registers with their bank
- The cardholder creates a password (similar to an ATM pin number)
- Cardholder browses merchant website and selects goods/services to purchase
- When a cardholder attempts to make a purchase, the cardholder is asked to enter the password they previously created when registering with their bank. The 3D Secure software can detect if a card is enrolled or needs to be enrolled. The standard authorisation process is followed for cards that are not able to support this service
- When the cardholder enters the password, the information is routed to the cardholder's bank for verification. The result of the password verification check is then sent to the merchant, advising whether the purchaser entered the correct password. If the wrong password is entered, it is likely that the purchaser is not the rightful cardholder and the merchant should not proceed with the transaction as liability then shifts back to the merchant.

The primary benefit to merchants of these verification processes is the chargeback liability shift that occurs. Subject to a few exceptions, if a merchant attempts to authenticate a purchaser using 3D Secure, both the cardholder and their bank lose the right to make a chargeback claiming the cardholder did not make the transaction. This is irrespective of whether the cardholder or their bank subscribe to 3D Secure - all that matters is that the merchant has implemented 3D Secure, and attempted to verify the cardholder's password.

Of course, if the password verification check fails (the purchaser entered the wrong password), you should not proceed with the transaction. If you proceed with the transaction after a cardholder has failed the verification check, you will incur the liability should a chargeback result.

HINT: Never process a transaction after a cardholder has failed the verification check.

Risk Mitigation for Online Merchants

How to enable Verified by Visa and Mastercard® SecureCode

3D Secure is compulsory for merchants operating in industries that Westpac considers risky from the perspective of being targeted by fraudsters. Please phone the Merchant Help Desk on 1800 029 749 if you are unsure whether 3D Secure is compulsory for your business.

Where 3D secure is not compulsory, you may still elect to install it.

Whether you are using a Hosted Payment Solution or your own Payment Solution, you must first contact your Gateway Service Provider to arrange for a demonstration and an assessment of the costs and processes involved in implementing Verified by Visa and Mastercard SecureCode. Depending on your business activity, an e-mail will be forwarded to you by emercantssupport@westpac.com.au within one week of merchant facility approval, containing information and enrolment forms.

HINT: 3D Secure will assist your business with risk mitigation for online transactions.

Secure your customers' data

At Westpac we are committed to providing our merchants with every assistance to help protect their business, and their customers, from the growing threat posed by high-tech criminals. Without a doubt this is one of the biggest challenges faced by business today.

If you are a merchant who has access to, or stores credit card details in any format, **or if you use a service provider who does**, it is your responsibility to ensure that your customers' payment details remain secure.

It is important that you understand the measures which need to be taken to ensure the security of highly sensitive personal financial information.

Westpac is dedicated to assisting you to make it as easy, convenient and secure as possible for you to do so.

That is why we have developed a booklet entitled "*Your Guide to the Payment Card Industry Data Security Standards (PCIDSS)*". It is designed to provide you with the information which will assist in protecting your business against potential financial liability, investigative costs and the risk of unwanted media attention.

If you do not have a copy of this brochure, please telephone our Merchant Business Solutions Help Desk on 1800 029 749.

Alternatively, you may wish to email us at emercantssupport@westpac.com.au with the subject heading of "PCIDSS Enquiry".

HINT: Be aware of the importance of data security and your responsibility to ensure that your customer's data remains secure.

Website requirements

All merchants using an Internet Merchant Facility must comply with Westpac's website standards.

Westpac reserves the right to decline, deactivate access or terminate merchants who do not comply with these requirements for the duration of the facility.

1. Your website must satisfy all of the following criteria:
 - The trading name and the URL must not have any substantial differences in wording. This will maintain consistency and reduce any potential cardholder confusion.
 - A clear description of the goods and services offered for sale.
 - Contact information – trading name, Australian Business Number (where required), address.
 - Telephone number and fax number where available.
 - A clear explanation of shipping practices and delivery policy/timeframe.
 - Transaction currency: Westpac merchants can process AUD amounts only and may settle into AUD accounts only.
 - Total cost of the goods or services purchased, inclusive of all shipping charges.
 - Card scheme brand marks are displayed wherever payment options are presented.
 - Export restrictions (if any) – countries to which the merchant does not ship.
 - A clear refund/return policy.
 - Consumer data privacy policy – advises what you plan to do with information collected from your customers.
 - Security capabilities and policy for transmission of payment card details.
 - Each merchant domain name must utilise separate payment pages. It is necessary to check that website links do not go to another domain name from which payments can be made in relation to goods or services offered through the first website.
 - All information must be accurate in all respects.

2. Your website must not:
 - Contain anything that constitutes or encourages a violation of any applicable law or regulations, including but not limited to the sale of illegal goods or the violation of export controls, obscenity laws or gambling laws.
 - Contain any adult or pornographic content.
 - Offer for sale goods or services, or use to display materials, that may be considered by a reasonable person to be obscene, vulgar, offensive, dangerous, or are otherwise inappropriate.
 - Fail to use digital certificates to establish a secure browser session.
3. Payment pages must be accredited by Westpac or a Westpac accredited service provider and must adhere to our security requirements.
4. You must use digital certificates to establish a secure browser session between you and your customer.
5. You should not change the types of goods or services sold through your merchant facility without first providing Westpac with written notice, and then receiving written consent from Westpac confirming the change has been approved.



200 years proudly supporting Australia

Things you should know: 1. Some accredited Gateways can offer a Currency Converter tool. This is helpful to identify to the customer a rough approximation of how much, in his or her currency, their bill is. However, additional fees will be incurred when international conversions take place, and your customers must be made aware that the final amount billed to them will reflect conversion fees as well as payment made to your business, if applicable. Information is current as at August 2016.

Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated.

©2017 Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714.

WBC228296 0817