Protecting your business against card fraud

Merchant Business Solutions.

Effective date: 08 December 2023

In short

Some businesses are more prone to fraudulent purchases than others. Criminals often target businesses that sell over the internet and accept Mail or Telephone Orders. They also target those selling expensive products which can be quickly re-sold.

Getting an authorisation for a card transaction isn't enough. It's your responsibility to make sure that the customer is the genuine cardholder.

Be especially cautious of overseas transactions, international and first-time customers.

If you're suspicious of either the customer or the transaction, don't process the sale – even if the transaction has been authorised.

Don't process transactions on behalf of someone else. Money laundering could impact your business negatively.

You can use online authentication services to help reduce the risk of online transactions.

Always stick to the terms of your merchant agreement and the rules set out by each of the card schemes.

Keep up with the types of scams that could impact your business by visiting the Scam Watch and the Australian Cyber Security Centre (ACSC) websites.

You can find additional fraud and security tips online on our Merchant Support Centre page.

Contents

Protecting your business from Fraud

Today, as a business owner, accepting card payments is a necessary part of running your business. Yet, there are risks you face when accepting card payments. We've created this informative brochure to help you to understand the types of payment risks you may face. It also includes actions that you should take to reduce the risk of fraud and financial loss.

Based on the type of products sold, and the way transactions are processed, some businesses are more prone to fraudulent transactions than others.

What products do fraudsters target?

Criminals generally target high-value products that can be re-sold. These include:

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

If you're selling these types of products, you need to be extremely careful before handing over or shipping the products. Make sure you take all possible steps to confirm that the buyer is the true cardholder. This applies to all merchants – whether you're selling face-to-face or remotely.

Why does the type of transaction increase my risk?

When it comes to card purchases, there are essentially 2 ways a business processes a payment.

'Card Present' transactions

- Those with face-to-face, in-store buyers – such as a retail outlet.

'Card Not Present' transactions

- Those that have Internet purchases (such as online stores); and
- Those that have Mail Order/Telephone Order (MOTO) purchases.

Those using Internet and MOTO transactions are commonly referred to as 'Card Not Present' merchants. Here, the customer and card aren't physically present in the merchant's shop at the time of purchase. Instead, it's when your customer provides their card details over the internet, by phone, or through the mail.

A quick reminder, you should never ask a customer to provide card details in an email.

This rule is part of the Terms and Conditions of your Merchant Agreement.

Why do criminals prefer making Card Not Present purchases?

Many criminals prefer to make Card Not Present purchases as it's easy to remain anonymous and hide their identity.

Also, Card Not Present purchases allow criminals to place orders over the Internet or use MOTO anywhere in the world. If they live overseas, the chance of criminal prosecution is much lower, which is an added incentive to this type of fraudulent behaviour. That's why this type of fraud is increasing at a rapid rate.

Can Authorisation help prevent fraud?

Authorisation is the first step in processing a card transaction and is essential to help reduce fraudulent purchases. That's because it gives the merchant an 'approval' to proceed by confirming crucial must-haves – such as the customer's account number being accurate and adequate funds in the account to pay for the purchase. But there's *still* a risk even after the authorisation is approved.

That's why, to protect your business, it's important to understand the term 'authorisation' fully – mainly, what it means, and what it doesn't mean.

What authorisation **does** mean:

- The account number is valid.
- The card hasn't been reported lost or stolen. However, it may be lost, stolen, or compromised, or the card details have been acquired improperly or copied (and the rightful card owner isn't aware of this).
- 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. For that reason, the risk remains that the person providing the card number has either stolen or acquired the card improperly.

There is also a risk that the person has compromised (improperly acquired) the card number, without possessing the card.

Even though it's essential to get an authorisation for each transaction, it doesn't protect you from the risk of fraud or chargeback (we've explained 'chargebacks' in the next part of this brochure).

The Authorisation wouldn't guarantee payment if the rightful cardholder didn't make the payment.

Can I reduce chargebacks?

A chargeback happens when the cardholder raises a dispute with their financial institution (via the card schemes) for a transaction made through your business.

A cardholder has up to 18 months to dispute a transaction from the transaction date. Alternatively, the cardholder has up to 120 calendar days to dispute a transaction should the business have not delivered the goods and/or services that should have been provided.

Here are the reasons for most chargebacks:

- The cardholder didn't make the transaction (Non-Genuine)
- A cancelled recurring transaction
- Goods were not as described
- Goods were defective
- The goods or services were not received
- The purchase took place without proper authorisation (for an amount exceeding the merchant floor limit). The merchant floor limit is the transaction size after which merchants have to seek an authorisation.

Card Not Present merchants face additional chargeback risks due to the cardholder making the purchase remotely (without the need to enter their PIN or sign the sales receipt). If the cardholder denies having made the transaction later, you'll generally be liable for the chargeback. That's because you can't prove that the cardholder made the purchase.

You can reduce the risk of chargebacks by staying aware of how and why they occur.

Card Not Present merchants need to take extra care to identify customers and ensure that the transaction is legitimate.

Why is it important to verify a customer?

As explained before, authorisation doesn't mean the customer is verified.
The transaction may be fraudulent even after completing the authorisation.

That's why it's your responsibility to check that the customer is the true cardholder. This step applies to all merchants, no matter what method is used to accept card payments.

It's crucial for Internet and MOTO merchants to identify the buyer. However, we strongly recommend that business owners accepting card payments in person (card-present environment) also take steps to verify the customer, especially for large purchases.

At all times, it's your responsibility to check that the buyer is the genuine cardholder.

Detecting and reducing fraud

Card Present businesses.

How do I spot suspicious orders?

Businesses that sell in-store are commonly referred to as Card Present merchants. Although less risky than selling in a Card Not Present environment, face-to-face transactions still pose risks for business owners. If a customer behaves suspiciously, remember that it's better to lose a sale than make a sale and face a loss.

Card Present fraud: early warning signs

- Orders made for highly targeted products (listed earlier in the 'What products do fraudsters target?' section).
- Shoppers that make unusually large purchases. Since stolen cards have a limited life span, fraudsters tend to make the most of this opportunity.
- Customers who purchase large quantities of the same product without showing any interest in picking a particular size, colour, style, or price. Having multiples of the same item increases criminals' profits.
- A large purchase is made on a newly valid card because cards are sometimes stolen in transit (while being sent from the bank to the rightful cardholder).
- Buyers who don't negotiate on price at all where it's usual practice to do so (as they may not have any intention of paying for it).
- Customers who buy large or bulky products but refuse home delivery even if it's free (so the seller won't have any record of their address).
- Buyers wanting to pay with more than one card for a single purchase. Or who make repeated purchases in a short period.
- Shoppers who appear anxious, nervous, or impatient or those who pull their card out of a pocket rather than a wallet.
- Customers who try to distract you at the time of processing the sale, especially when the transaction is large.

How do I reduce card present in-store fraud?

Besides being alert to potentially suspicious transactions, your main defence against criminals is to carefully inspect the card to make sure it's not a counterfeit (fake) and that the customer is the genuine cardholder. Make sure all your staff members are adequately trained to conduct these checks.

The 8-point security check:

- Keep your EFTPOS terminal in a secure location – and don't leave it unattended.
- Always inspect the card carefully to ensure it's genuine. See if the account number matches the card name. Visa® starts with a 4 and Mastercard® (MC) with a 5.
- Make sure the 'valid from' and 'valid through' dates include the current date.

- Check that the card has the appropriate security measures. Security features can include an embedded chip, CVV security code, signature panel, hologram, and account name.
- The hologram on Visa and Mastercard cards should appear three-dimensional or change colour when tilting the card.
- Check that the abbreviated card number on the sales receipt matches the corresponding digits on the card. If the digits don't match, the card is fake.
- Closely inspect both sides of the card to see if the card appears to have been altered. For instance, is the magnetic stripe smooth and free of signs of tampering?
- Ask for an alternative form of payment if the transaction is declined.

Always inspect the card carefully to ensure it's genuine.

What's an example of in-store fraud?

Here's an example of fraudulent activity that may happen when taking a payment in store.

A customer visits a jewellery store to purchase a diamond bracelet. The staff member has trouble with the card during payment and is unable to charge the customer's card when tapping, inserting, or swiping the card. The customer says it's a special gift for a wedding anniversary and coaxes the teller to manually enter the card details into the terminal as they are in a rush. Not wanting to disappoint the customer, the teller manually enters the transaction – and it gets approved. The customer leaves the store with the expensive bracelet.

A few weeks later, the merchant receives a chargeback for the transaction. Unfortunately, the card the customer had given the staff member had been skimmed, and the details were stolen. As a result, the business owner faces considerable losses as they'll need to bear the transaction cost, plus the associated chargeback fee, and won't be able to recover the bracelet.

To prevent these sorts of scams, make sure you or your staff never manually enter transactions if the card is present at the time of transaction. And also keep a watchful eye to make sure the cardholder isn't entering their card details manually in the terminal.

Card Not Present businesses.

How do I spot suspicious orders?

Business owners that sell over the internet or accept MOTO transactions are commonly called Card Not Present merchants. They are at a greater risk of becoming victims of fraud. That's because it's harder to confirm if the cardholder is genuine. So criminals take advantage of the fact that it's easy to remain anonymous and hide their identity.

Card Present fraud: 10 early warning signs

Many of the risks related to suspicious instore purchases are also relevant for MOTO and internet purchases. These include:

- Orders made for highly targeted products (listed earlier in the 'What products do fraudsters target?' section); and shoppers that make unusually large orders or customers who purchase large quantities of the same product.

Besides these, there are also additional risks that you need to be careful of. Very often, it's the presence of more than one of these factors that indicate possible fraud.

- Customers who place multiple orders within a short space of time. And if they use card numbers that are very similar, such as where only the last four digits differ.
- Customers who place orders using multiple cards.
- Customers who use different cards with several declines within a short period.
- Orders requiring urgent shipping. Or orders for goods not usually supplied by your business.
- All international orders, especially where the order is from a country you don't usually receive orders from. 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 card fraud: Nigeria, Indonesia, Ghana and Eastern Europe.
- Orders shipped to a country where the goods could easily be purchased locally. You need to question why the customer is prepared to pay the shipping expense and wait longer for the goods to arrive.
- Orders requesting delivery to a Post Office Box.
- Orders requesting the goods to be shipped to a third party.
- Orders from Internet addresses using free e-mail addresses.

If you're suspicious of the customer or the order, don't ship the products, even if you've completed authorisation.

What's an example of internet fraud?

Card fraud is a real threat in today's eCommerce-based world. And businesses that sell online are more vulnerable than ever before to the risk of card fraud and associated losses. Here's an example.

Cybercriminals purchase or steal cardholder information (including card details). They then use the stolen card numbers to make fraudulent online purchases.

A genuine cardholder receives a statement that shows an unauthorised purchase, and they immediately dispute it. Unfortunately, this results in a chargeback for the business owner. They are left out of pocket due to chargeback costs, plus the loss of the items they've sold. The cost to the business owner for accepting that fraudulent transaction is more than double the cost of the sale.

Make sure you and your staff read the 8-point security check that we've included that could help prevent such losses.

How can I reduce Card Not Present fraud?

The 8-point security check:

- Ask the cardholder to provide the CVV2 (Visa) or CVC2 (Mastercard) three-digit number shown on the card's signature panel (commonly called the card check value). If the buyer doesn't have the card on them, it's unlikely they will know this number – so it could help you stop a potentially fraudulent purchase.
- Ask the cardholder the name of the cardholder's bank. Criminals with compromised account details won't have this information.
- Be cautious when multiple cards are being used for a single purchase. And don't continue to attempt authorisation after receiving a card decline. Try and request another form of payment, such as a bank account transfer.
- Do a web search to verify the name and phone number the customer has provided. Request the customer to send you a copy of their driver's licence as an additional check.
- Be cautious when a customer's billing address and delivery address are different. For example, is it a local billing address with an overseas delivery address?
- Never send parcels to a Post Office Box. And where possible, ask for a signed receipt from the cardholder when they receive the order or delivery confirmation from the delivery provider.
- If it's an order for many different products, call the cardholder after the order is placed to confirm the order. Then, reconfirm the order details with them before shipping it. Frequently, when it's a fraud, the buyer won't be able to confirm these details since they were ordering randomly, with no record of what they had ordered.
- Be extra careful when processing overseas orders. Large orders should not be shipped until you've taken steps to check the legitimacy of the buyer and are satisfied that the purchase is legitimate.

Other risks merchants face

Increase in Mail and Telephone Order fraud.

Criminals are increasingly targeting businesses with MOTO requests. That's because transactions are processed without a physical card or a PIN (Personal Identification Number). MOTO transactions can also take place in-store, as card numbers can be manually entered into the terminal when it's handed over to the customer or left unattended.

What are some real-life examples of MOTO fraud?

Here are a few real-life examples so you can remain aware of how criminals could target your business. These are also worth sharing with your staff members.

MOTO Fraud – remote
A customer calls a tyre company to buy and arrange the delivery of $10,000 worth of new tyres. The delivery address is in a different state from the merchant's business address. The staff member is processing a MOTO transaction by hand-keying in the card number provided over the phone. The customer says that a friend will be collecting the goods on their behalf (since they live interstate). The staff member is unaware that the customer on the phone, making this purchase, is using a stolen card. The tyre company loses money due to a chargeback request from the genuine cardholder's bank (as the purchase was made using a stolen card).

This situation could have been prevented if the staff member had been vigilant and taken time to check the cardholder's authenticity.

MOTO Fraud – in-store
A customer is buying a new $900 smartphone in-store. The staff member enters the sales details then gives the terminal to the customer to enter their PIN. The customer quickly cancels the original transaction and processes a MOTO (keyed) transaction for $9,000 using a card – without the staff member's knowledge. Once this transaction has been processed, the customer claims they've been overcharged. They request the business to refund the difference ($8,100) to an alternative card. The merchant loses money due to a chargeback request being received from the genuine cardholder's bank.

In another instance, a customer wants to purchase two new laptops in-store, one for their use and one as a gift – a total of $3,000. The staff member enters the sales details then gives the terminal to the customer to enter their PIN. The customer then cancels the original transaction and processes a MOTO (keyed) transaction for $3,000 using a stolen card number without the staff member's knowledge. Once this transaction has been processed, the customer leaves the store with the new laptops. The merchant loses money due to a chargeback request being received from the genuine cardholder's bank.

These examples of fraud could be prevented if business owners and staff members remain vigilant and double-check transactions before completing them.

How do I reduce the growing risk of MOTO fraud?

Be mindful when an unusual or high-value MOTO request is made. It includes any unusual requests from the cardholder regarding the collection or delivery of the order, such as agreeing to pay for relevant freight or postage costs when it isn't usual practice.

Especially when it comes to international or interstate orders, ask the cardholder why they've selected your business instead of sourcing products or services available locally.

Be cautious of international cards being utilised for domestic use.

If the products are being delivered, you can request the cardholder to show a Photo ID, and the original card used for the transaction to confirm the identity matches the name on the physical card.

Any sales through the terminal need to be processed carefully; you can identify a MOTO transaction by the terminal sales receipt, which will show 'MOTO' or 'MOTO PURCH'.

Make sure you can see your terminal at all times. In addition, be aware of cardholder behaviour – entering a PIN shouldn't take more than a few seconds. If you think the cardholder is behaving suspiciously, request a Photo ID to confirm that their identity matches the name on the card.

If a signature is required, check that the numbers on the terminal sales receipt matches the last four digits on the card.

Any refund requests must be processed to the same card as the original transaction and should never exceed the original transaction amount. You can ensure you're processing a refund to the same card by comparing the last four digits on the 'Merchant Copy' receipt with the last four digits on the card.

For assistance, contact our 24/7 Merchant Helpdesk on 1800 029 749.

Laundering of sales (3rd Party Processing).

When it comes to merchants, the term 'laundering' refers to a situation where a business with a valid merchant facility accepts transactions on behalf of another company.

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.

Criminals sometimes approach legitimate merchants to process their card transactions, generally paying the merchant a percentage of the amount processed. Apart from constituting a serious breach of our terms and conditions, it is also an extremely dangerous practice that makes a merchant's business vulnerable to a significant loss.

Merchants engaging in laundering or processing transactions on behalf of another business will face chargebacks arising from these illegal transactions. In many cases, the person approaching the merchant to process their transactions is unable to secure a merchant facility of their own – possibly due to previous improper merchant practices. That's why the chance of fraudulent transactions processed using your merchant facility is extremely high.

As a merchant, laundering is an extremely dangerous practice that could impact your business.

Fraudulent refund transactions.

A common type of fraud involves employees issuing refunds to their own account. To avoid detection, they may process a large transaction on a fraudulent card and refund the amount on their own card. Unfortunately, it often takes weeks, even months, before the fraud is detected. To guard against this, it's important to closely monitor all refunds. In addition, check that all credits and corresponding debits relate to the same card number – especially when it involves large amounts.

Another way merchants can protect themselves from this type of fraud is by regularly changing passwords (like their terminal and user passwords), especially after an employee has left.

Change your passwords regularly to prevent unauthorised use of your merchant facility.

Safety for Online Merchants

How Online Authentication – 3D Secure can help.

One of the problems merchants face in accepting Internet-based transactions is the difficulty of confirming if the buyer is the genuine cardholder. This means that if a cardholder disputes an online purchase, the merchant may be liable for the chargeback.

3D Secure^ is a service that provides an extra layer of protection to our merchants and their customers for their online purchases and may deter unauthorised transactions. This additional layer of authentication gives business owners protection because it shifts the liability away from them and to the cardholder's bank for fraudulent chargebacks. The service is called Visa Secure (previously Verified by Visa), Mastercard ID Check™ (formerly Mastercard Secure Code) and eftpos Secure.

Here's how the Visa Secure, Mastercard ID Check™ and eftpos Secure works:

Step 1. A customer visits the merchant's online store and buys the products or services they want.

Step 2. The payment gateway exchanges all the necessary information in the background.

Step 3. The merchant performs a regular transaction which is 3D Secure authenticated in the background.

Step 4. Based on the customer's issuing bank limits, the customer may either be asked to provide two-factor authentication, or the transaction is approved. For example, a one-time PIN is sent either via email or SMS. The cardholder's issuing bank bears responsibility for that transaction – and so the merchant is protected.

How do I enable 3D Secure?

The first step is to talk to your payment gateway service provider about enabling 3D Secure.

Whether you're 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 3D Secure.

3D Secure will assist your business with reducing the risk of online transactions.

^3D Secure is a security service offered by third parties (e.g. Visa, Mastercard and eftpos). Westpac does not guarantee or endorse the services. 3D Secure is only available for schemes including Visa, Mastercard and eftpos when enabled on your payment gateway.

Securing your customers' payment information.

We're committed to helping our merchants 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 businesses today.

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

You must understand the measures you need to maintain the security of highly sensitive personal financial information.

That's why we have created a handy brochure called 'Your Guide to the Payment Card Industry Data Security Standard (PCI DSS)'. It's designed to provide you with the information that will help protect your business against potential financial losses, investigative costs, and the risk of unwanted media attention.

If you don't have a copy of this guide, you can:

- Visit westpac.com.au/merchant-terms to view it online
- Call our Merchant Helpdesk on 1800 029 749 for a copy
- Email us at pci@westpac.com.au with the subject heading of 'PCI DSS Enquiry'.

Be aware of the importance of data security and your responsibility to ensure that your customers' data remains secure.

We're here to help

1800 029 749 – Available 24/7

westpac.com.au/merchantsupport

Accessibility support.

At any time, you can inform us how you would prefer to be contacted. If you are deaf and/or find it hard hearing or speaking with people who use a phone, you can reach us through the National Relay Service (NRS). To use the NRS you can register by visiting **accesshub.gov.au/about-the-nrs**

Visit **westpac.com.au/web-accessibility** for further information on our accessible products and services for people with disability.

Westpac acknowledges the traditional owners as the custodians of this land, recognising their connection to land, waters and community. We pay our respects to Australia's First Peoples, and to their Elders, past and present.