PROTECT YOUR BUSINESS FROM CREDIT CARD FRAUD.

CAN

Protect your business from credit card fraud

Credit cards are a secure and convenient way for your customers to pay. They're also a great way to get money into your business account faster, without the hassle of handling cash or cheques. But credit card fraud is a serious issue and there are some risks you may need to manage. We suggest that you follow these easy tips for safer card transactions. Staying wise to credit card fraud protects your customers, revenue and reputation.

W	**Watch out**	**Watch out** for suspicious behaviour, such as: ◆ customers who tell you how to process a transaction or hesitate when you ask them for personal details ◆ significant transactions (in terms of cost and/or volume) where all the information is provided by unfamiliar buyers or sellers.
I	**Identify**	**Identify** your customer to make sure they're the true cardholder. You can do this by: ◆ asking customers for additional forms of identification if they are requesting large orders or appear suspicious ◆ comparing a customer's card number and type of card to the one printed on the receipt – if they don't match, the customer is using a counterfeit card. ◆ obtaining a card imprint for 'card not present' transactions by phone, mail or online, if the customer picks up their goods in person ◆ checking for fake addresses before you ship by using a Google map search to check that the address is real.
S	**Signature**	**Prioritise security** in your payment processes. Signatures are being phased out from the 1 August 2014 and customers will be required to enter their PIN for many transactions. In addition, you should: ◆ train your staff to ask customers to enter their PIN for transactions, rather than signing. This request could be framed in terms of making payments quicker and more convenient. ◆ ask customers to provide their card CVV number for phone and online transactions. ◆ consider using fraud prevention & monitoring tools for online transactions to prevent, detect and help combat fraud.
E	**Educate**	**Educate** your staff about fraud by: ◆ training them to look out for suspicious transactions ◆ giving them these simple hints so they know what to look for. ◆ visit the APCA website www.apca.com.au/getsmart/online-card-fraud/ and complete the training module.
R	**Remember**	**Remember** common signs of fraud. This includes customers who: ◆ place orders using multiple cards that have similar or sequential numbers ◆ make many purchases with the same card over short periods of time ◆ ask you to pay for shipping costs (see case studies for examples) ◆ order several of the same item, or who don't care about the colour or size they receive ◆ request funds be deposited thorough money transfer agencies such as Western Union (see case studies for more information).

REMEMBER! **We suggest that you treat credit card sales just like cash. Ask yourself: would I be happy to hand over my own money in this situation? If the answer is no, think carefully about accepting the payment.**

Warning signs to look out for

These case studies, based on real life situations, show just how much fraud can cost your business. Watch out for the warning signs to avoid becoming a victim.

CASE STUDY 1: If it's too good to be true...

What happened	A cosmetic manufacturer received an email from a potential client who wanted to buy large quantities of the company's newly released product and have the order shipped overseas. After corresponding with the client, the manufacturer agreed to fill the order. The client sent multiple credit card numbers to pay for the goods.
The scam	The client asked the manufacturer to use these credit cards to pay a shipping company to deliver the products overseas. The manufacturer agreed, and arranged for multiple transactions totalling $27,000 to be remitted through Western Union to the shipping company.
The result	After 10 days, the manufacturer's bank contacted them with bad news: they'd been the victim of a scam. The merchant lost the $27,000 in non-existent shipping fees and was left with a storeroom full of unsold cosmetics it had produced to fill the order.
What to watch for	◆ Complicated or unlikely orders. Are your products freely available? If so, why would someone from overseas or interstate choose your site to make large purchases? ◆ Customers who try to use multiple card numbers to complete transactions. ◆ Huge orders from previously unknown buyers out of the blue. If a deal seems too good to be true, it probably is.

CASE STUDY 2: The function that never was

What happened	A client contacted a restaurant wanting to book a function for 300 people. To pay for the function, the client provided a number of different MasterCard card numbers, which the restaurant owner manually entered into the terminal.
The scam	A few days later, the customer cancelled the function due to a family illness. They asked the restaurant to refund the money through Western Union instead of processing a credit card refund. The restaurant owner followed these instructions. However, shortly afterwards, the restaurant discovered the payments were fraudulent. The restaurant had to pay chargebacks to the true cardholders for the full amounts.
The result	Because it didn't have physical imprints of the cards, the restaurant couldn't prove the sale. As a result, it lost the money it had to refund, and was significantly out of pocket.
What to watch for	◆ Customers who ask you to send funds through Western Union or other money transfer agencies to pay for courier costs. ◆ Customers that offer multiple credit cards to complete transactions.

CASE STUDY 3: Orders across borders

What happened	Another restaurant received an email request to prepare $3,000 worth of food. The customer provided several credit card numbers to pay for the order.
The scam	Later, the customer asked the restaurant to courier the food to Penrith in New South Wales. They offered to pay for courier fees using the credit cards they'd already provided. Soon after this request, the restaurant's bank warned the owner not to process the card transactions or to send the goods, as the credit cards used for the order had been compromised.
The result	Unfortunately, the restaurant's owner had already used the credit cards to pay the courier company $1,200. As it did not have physical imprints for the cards, the restaurant was liable for this payment. Furthermore, the restaurant was left with the perishable food it had bought to fulfil the order.
What to watch for	◆ Customers who ask you to pay for shipping or courier costs. ◆ Unusual purchases. For instance, if you're a restaurant based in Queensland, and you offer products that are generally available elsewhere, why would a customer want to have your perishable goods transported interstate?

CASE STUDY 4: Free parts

What happened	An automotive parts supplier received a phone order from an unknown customer wanting to buy expensive performance parts. The customer provided credit card details over the phone, and the company manually entered them into its EFTPOS machine.
The scam	The card authorisation was approved and the supplier prepared the order as normal. The customer then told the supplier that they would send a courier to the site to collect and deliver the goods. The courier took the goods and the transaction was complete.
The result	Later, the supplier's bank called with bad news: the credit card used in the transaction was fraudulent. Because the supplier had manually entered the credit card details, it was liable for the chargebacks.
What to watch for	◆ Expensive and unusual orders. ◆ Couriers that have been booked by customers. Ask the courier for identification before handing over any goods. ◆ Mail and telephone orders. These are potentially risky, as your business will be liable for any disputed transactions. Take extra care when dealing with customers through these channels.

We're here to help

1800 230 177 24 hours a day, 365 days a year
www.commbank.com.au/business/merchant-services