Transaction Talk

SUNCORP BANK
Business

Issue 18 | Autumn 2015

10 tips for managing card-present fraud in 2015

There's nothing like a fraudulent transaction to take the shine off an otherwise successful day of sales. Most of the time, you'll know instinctively when something's not quite right. But there are still times when fraudsters can get the better of you.

The good news is, by following these tips, you'll be able to stay one step ahead:

1. Be wary of customers who purchase a lot of stuff without asking any questions. It's always nice to have a big sale, but not when you've got to foot the bill.
2. Think twice if someone's buying your products without regard to size, style, colour or price. People who steal cards will want to buy as much as they can before the card gets cancelled.
3. When a customer is trying to rush you or distract you during the sale, be careful not to let your guard down. It's a common tactic used by fraudsters.
4. Look extra carefully at big purchases that come in just after you've opened, or just before you're about to close up for the day.
5. If a customer is coming back repeatedly to your store to make credit card purchases, it's probably just because they love what you sell. But be careful, it's also a sign of fraud.
6. Most people won't refuse free delivery for large items, unless someone else is paying the bill. So when this happens, think twice.
7. Check the card's security features. If it's been altered in any way, there's a chance it's been stolen.
8. Make sure the card is electronically read, and check the authorisation response and take whatever action is appropriate. If the card fails to read, never enter the card number manually into the terminal.
9. Check the embossed number on the card against the four digits of the account number displayed on the terminal. If the two don't match, you're probably dealing with a fraudster.
10. For pre-paid and cards issued overseas, get the cardholder to sign the transaction receipt. If it looks different from the signature on the card, you know something's up.

How to avoid card-not-present fraud? It helps to understand how fraudsters work.

When you're taking orders by phone, email or over the web, you need to be extra careful to avoid fraud.

By understanding a bit about the way fraudsters work, you'll be better placed to identify when you're on the wrong end of a criminal transaction.

Fraudsters are usually looking to re-sell the items they buy from you

So they'll be after items that are easy to sell quickly, for the biggest amount.

Having multiples of the same items (with different colours, sizes, model types etc), or lots of big ticket items, increases a criminal's profits – so be wary of those sorts of orders.

Fraudsters usually don't have long to use a credit card before it's cancelled

So they'll try to get as much out of it as quickly as possible. Look closely at larger-than-normal orders, "rush" or "overnight" shipping orders (people aren't concerned about additional shipping charges if they're not paying), multiple orders on one card in a short period of time, or even just first-time orders (fraudsters are always looking for new merchants to scam).

Fraudsters will often work across borders

So be on the look out for transactions where the IP address, the shipping address, and the billing address are not from the same country, or when the country or regional code for the phone number doesn't match where the goods are headed.

Fraudsters often use technology to help cover their tracks

If you get multiple orders on different cards, all shipping to the same address, it could well be fraudsters using an account number generated using special software, or a stolen batch of card numbers.

Likewise, if there's a batch of transactions with similar (but not identical) account numbers, it could be a software system at work.

Lower tech services can help fraudsters too. They might use free email services (that often don't have billing relationships or audit trails), and email addresses that use numbers or letters that don't make sense (and don't have any relationship to the cardholder's name).

Fraud is often highly organised

Multiple transactions on one card (or a similar card) with a single billing address, but multiple shipping addresses, are likely the work of an organised fraud group or scheme. So too multiple cards used from a single IP address.

So be wary of transactions that ship to hotels, empty buildings, or mail forwarding companies.

How to properly identify a cardholder's identity

Whether you're selling by mail order, telephone, internet or in person, it's up to you to verify the cardholder's identity and the validity of the transaction. Here are some things you can do:

- Ask the customer for the card expiration date – an incorrect or missing expiration date is an indicator that the purchaser doesn't have the card in hand.
- Undertake internal screening, or use a third-party tool to screen for questionable transaction data or other warning signs that might indicate 'out of pattern' orders. Then route transactions with higher risk characteristics for fraud review.

Getting ready for EFTPOS chip cards

It's become an integral part of the way we shop. Every day, Australians make more than 6 million EFTPOS transactions on 820,000 terminals across the country.

Some changes are being made to EFTPOS card technology, to give consumers even more choice and to make the systems more secure particularly against card skimming.

Cash in your chips

As a result of four years of research, development and testing, EFTPOS chip technology is being added to all cards that can process EFTPOS transactions including EFTPOS only cash cards and credit cards with linked transaction accounts.

Why the changes?

As well as being more secure, the new EFTPOS chip will be able to carry multiple applications, so it'll be ready for a range of new possibilities in the future.

Things will start to look a little different

As the new cards roll out, the way customer accounts are displayed on point of sale terminals will change slightly from the current "CHQ, SAV, CR" options. In most cases, the new displays will read "EFTPOS CHQ, EFTPOS SAV, VISA or Mastercard Debit".

In some cases the order in which the customer accounts are displayed may also change. Specifically, some multi-network cards may display the Issuer brand name first – e.g. "SUN EFTPOS CHQ, SUN EFTPOS SAV".

From now on, we suggest you turn the EFTPOS terminal around and encourage customers to choose their account themselves.

The changes are already underway

The terminal upgrades are tipped to be complete by the end of this year (with the exception of some end-of-life terminals which will be replaced). The card rollout should be complete by the end of 2017.

How will it affect you as a merchant?

If you have a VX680 or VX520 contactless terminal …

- Your software will be remotely updated overnight during the first half of 2015, so there's nothing you need to do.
- Once your terminal has been updated, it'll ask the customer to select the account type whenever a card with a chip is presented. The options will depend on what accounts have been loaded on the card, but it could be:
  - EFTPOS Chq
  - EFTPOS Sav
  - VISA or Mastercard Debit
- Some financial institutions may choose to place their name in front of the options, so it will read "SUN EFTPOS SAV", for example.
- When a customer uses Tap and Go with a Visa or Mastercard Debit, the account type will automatically be Visa or Mastercard Debit. If they want to select Chq or Sav, they'll need to insert their card.
- Contactless payment is only available on a purchase transaction. Customers will need to insert their card for all other transaction types.
- If a customer swipes a new EFTPOS chip card using the traditional magstripe, the terminal will request that they insert their card.

If a new EFTPOS chip card is presented at your EFTPOS terminal prior to the terminal receiving the software update, you can still process the card. If you insert the card your terminal will request that you swipe the card and process the transaction in that manner.

If you have a T4220 or a M4230 terminal …

- The customer will need to first insert their card into the EFTPOS terminal.
- The screen will flash 'Card Reader Error' and then 'Please remove the Card'.
- Once the customer has removed the card, they'll be prompted to 'Swipe Customer card'.
- Once they've swiped, the terminal will prompt them to select an account type: 1. Savings, 2. Cheque.
- The customer should select their account type and then proceed with the transaction as normal.

‘Why Leave Town’ gift cards

Recently a gift card supplier launched a new gift card scheme called ‘Why Leave Town’. We’re not supporting this card. In fact, we’re advising merchants not to sell or load the cards using their Suncorp Terminal.

The scheme asks merchants to sell EFTPOS gift cards to their customers, to be used at other participating outlets in the area. It requires merchants to load the cards using a refund from the merchant terminal onto the card.

At this stage, the scheme is targeting merchants in small towns – it’s yet to hit the metro areas.

If you have any questions or concerns about the scheme, you can get in touch with us on 13 11 75.

Talk to us today

www **suncorpbank.com.au/merchanthelp**

For merchant account enquiries, call us on 13 11 75

For technical support from the EFTPOS Terminal helpdesk, call 1800 836 055

SUNCORP BANK
Business

Suncorp-Metway Ltd ABN 66 010 831 722.
12189 13/02/15 A