Checking your security at the checkout.

Strategies for safely accepting and storing cardholder data.

"In the future, our banking and payments trends are going to be heavily influenced by the customer's need to be able to transact anywhere, any time. And preferably – seamlessly. As a merchant, your customers will expect you to provide the facilities that allow them to use faster, better, innovative payment experiences. But it's important that you understand how to keep your customers' cardholder data – and your business – safe while enabling these new ways to pay."

Meagan Arderne, Senior Risk and Scheme Compliance Manager, Westpac New Zealand

No cash. No card. No problem.

The payments landscape is evolving rapidly. One of the factors driving this evolution is the customer's expectation that they can get everything done in an instant – and that includes making payments. So what does this mean for you?

You may already be aware that contactless payments are growing in popularity. Customers can now choose to use their mobile phones or other devices like smart watches and wearables to pay for whatever they want, whenever they want. No need to carry a card or cash – thanks to technology like Near Field Communication (NFC), they can simply hover their mobile phone or device over the terminal to pay and go. At Westpac, we've helped many businesses switch on their contactless facilities to meet customer demand for this service.

But that's just the beginning.

Imagine a customer coming into your store, choosing an item and leaving your store knowing that the payment will be made automatically – without having to deal with the usual technological hurdles or mundane task of queuing at a checkout.

Advancements like artificial intelligence, biometrics and open banking will pave the way for these new types of payment experiences. Why will your customers bother trying to remember a PIN or password when they can simply use their fingerprints, face or eyes to identify themselves through biometric authentication? With open banking, soon customers will be able to give their bank permission to share their financial information across platforms with multiple approved organisations. Imagine giving your customers the ability to buy products online seamlessly and securely by using these advancements.

Soon we'll all be able to transact anywhere, any time – and eventually we won't even know we're doing it.

Delivering that great customer experience starts with security.

There's no doubt these innovative payment channels can help to improve your customer experience. But it's important to remember that a great experience is not just about fewer clicks on your website to get to the check out, or less time in the queue at your store – it's also about making sure you protect your customer's data throughout the entire transaction process. Understanding what we do to protect you, and how you need to protect yourself, will help you keep your customers safe – however they decide to transact with you.

Fraud doesn't ask for your size.

One of the things we keep emphasising is it doesn't matter if you are a big, international retailer or the 'mum and dad' store around the corner, fraudsters will look for your vulnerabilities then use these to try and exploit you. To them, money is money. It doesn't matter where they get it from. With every new payment channel and platform that's developed, fraudsters quickly evolve to the new payment landscape. Which means if you don't understand how to protect your business you're not only running the risk of losing money, you are also running the risk of brand damage, reputational damage and losing consumer trust.

How you can remove risks in your business.

Know your MCCFA.

When we start working with you, we provide you with a legal document called a Merchant Credit Card Facility Agreement (MCCFA). This gives you a detailed overview of your responsibilities as a merchant and includes requirements designed to protect your business and your customers against fraud. We keep an updated version on our website **westpac.co.nz/mccfa** so it's easy for you and your staff to refer to at any time. It's important to review this agreement and let us know if you have any questions, because there can be serious consequences for breaching the agreement.

Comply with PCI.

If you want to have a merchant facility, you need to be Payment Card Industry Data Security Standard (PCI DSS) compliant.

PCI DSS is the global information security standard set by the card schemes for all organisations that store, process or transmit card payment data. Making sure your business meets this standard is one of your requirements outlined in the MCCFA. It's important to know that whatever your size or transaction volume, if you accept or process scheme payment cards then PCI DSS applies to you (even if you are a small merchant that processes 100 transactions in a 12 month period). This requirement is designed to protect cardholder data regardless of the payment channel.

As a bank, we can't provide any guidance or consulting around PCI DSS but the official website **pcisecuritystandards.org** has some useful information. If you need more advice, you may consult a Qualified Security Assessor (QSA). You can find a list of approved QSAs on **pcisecuritystandards.org**

BIG LOSS FOR A SMALL BUSINESS.

A small e-commerce merchant that processes less than 300 transactions in a 12 month period was breached because the software on their website and shopping cart was not kept up-to-date. Fraudsters exploited the vulnerabilities and injected a line of malicious code into the merchant's website. When customers went to enter their details, it made the purchase but also sent a copy of the customer's card details to other fraudsters. This is known as scraping or skimming.

As a result, 35 card numbers were compromised. One of the cards was a Westpac card. And the very next transaction (once the card number was stolen) was for an amount in excess of $5000. As soon as the breach was detected, we contacted the merchant and asked them to shut down their e-commerce payments page and website until remediation to remove vulnerabilities was completed.

Enable 3-D Secure.

The highest risk for fraud is through card not present transactions – research from Mastercard indicates that this represents around 90% of all fraud losses in New Zealand. In our present landscape, card not present channels are predominantly mail order/ telephone order (MOTO) and e-commerce. While there's not much authentication available for MOTO processing, 3-D Secure is the most effective tool available to protect you against e-commerce fraud and associated losses. It is designed to confirm the authenticity of a transaction when a credit or debit card is used online.

How does 3-D Secure work?

- Your customer enters their card details on your e-commerce site.
- If required, your customer is redirected to their issuing bank's 3-D secure page (the bank who issued your customer with their debit or credit card is known as an 'issuing bank').
- Your customer then needs to enter the authentication details requested by their issuing bank.

- After your customer has provided the correct details, the payment is authenticated by their issuing bank and your customer is directed back to your e-commerce site.
- You can then make an informed decision whether to submit or decline the transaction.

Monitor your MOTO processing.

Today, mail order or telephone order (MOTO) is the only channel that doesn't have authentication built into it. Your card present has your chip and PIN. Your e-commerce has 3-D Secure as authentication. Even your mobile wallet acceptance has two factor authentication on it – this is built into the card stored on your device and your actual device. And then there's MOTO which currently has no protection.

What makes MOTO so risky? The collection, storage and usage of card numbers. We have seen merchants write these down on the back of an envelope or put them up on a whiteboard for processing at the end of the day. Even capturing the data in a spreadsheet and saving it to a desktop in an encrypted file isn't safe – what happens if that data lands up in the wrong hands?

A data breach could impact your business in two ways. If those card numbers have been obtained from your unsecure environment, you'll be considered the source of the breach and you could be held liable for financial penalties and need to complete remediation steps outlined by the scheme. If you process transactions via MOTO using those stolen card numbers, you'll be liable for that transaction – regardless of whether it was a legitimate transaction that was later charged back under a fraud related code.

That's why, even if you have asked for a small facility to allow just 1 or 2% of your volume to be MOTO, we monitor that strictly – and you'll need to make sure you understand your PCI compliance obligation around this channel. So if you wonder why our team discourage you to accept MOTO, it is because of the risk to us and your business.

FRAUD THROUGH A PHONE CALL.

In a recent case, fraudsters identified a vulnerability with our merchant and started testing stolen cards with them on their MOTO facility. These fraudsters called up requesting services that this particular merchant delivered, provided the stolen card payment details and then collected on the services.

In accordance with scheme rules, a cardholder has 120 days to dispute a fraudulent transaction. In this instance, the cardholder whose card number had been stolen exercised that right. This meant the merchant had to refund the original amount to the cardholder even though they could prove that the services were delivered. The end result is that the merchant is out of pocket because they had to reimburse the cardholder in full.

Check your third party's security.

Fraudsters can infiltrate your third party suppliers too – in fact, there have been several cases where these data breaches have cost businesses millions of dollars. In a recent case, a company which sells tickets online to events experienced a breach caused by malicious software on their third-party customer support product, which affected up to 40,000 UK customers and an undisclosed number of NZ customers. So if you are using any external software or hardware to process your payments or rely on service providers during any part of your transaction processing, it is vital that you ensure they are compliant with PCI requirements.

How we protect your business.

Develop our fraud knowledge through partnerships.

We work with our industry partners, schemes and even other banks across the world to stay up-to-date on international trends, experience and tools to combat fraudsters.

This kind of collaboration helps us to make informed decisions when we're faced with assessing risk and exposure to you. Recently we had a request from a merchant to use a service provider whose PCI compliance status was unknown. There was no obvious reason to decline the service provider's application, but we put in a call to an industry partner to find out whether they had vetted this service provider from a security perspective at any stage in the prior 12 months. We were informed that the service provider suffered a breach within the past five years and their PCI compliance status was still unknown. We referred the merchant to a PCI compliant service provider and asked them to resubmit their application. This is just one way we're able to use our partnerships to conduct our due diligence, and provide our merchant base with a preapproved list of service providers they can use and trust.

Report and block fraudsters through international databases.

Another way we share information is through the international merchant databases set up by Mastercard® and Visa® – two of the card schemes we work with. This gives us the ability to see if a merchant has been terminated by another bank so that we can make a risk-based decision whether or not we will work with them. If we choose to terminate a merchant facility for any of the reasons determined by the schemes, we have to register these merchants in their database and every bank in the world has access to that information. This is a requirement from Mastercard® and Visa®.

Monitor for fraud and report it.

Our fraud team conducts fraud monitoring on our merchants in near real time as well as reviewing daily trends. The team look for unusual activity as well as high decline rates. Anything out of the ordinary will be reported to our merchant team for further investigation.

What to do if there's a data breach.

If you suspect there may have been a data breach within your organisation, contact the Westpac Merchant Assist team immediately – whatever the size or nature of the breach. Talk to us before trying to contact your cardholders. Don't change anything (such as reloading your environment) because we won't be able to trace anything. Take a snapshot of your environment, make a copy of it and if you can switch over to a more secure environment then do that. We will talk you through the next steps.

Tips to protect your business.

- Don't allow any unauthorised access to your terminal, website or payment page.
- For card present electronic transactions, ensure the cardholder authorises all card transactions by using a PIN.
- Adhere to authorisation limits, don't split a single transaction between two or more sales.
- Don't dispense cash off a credit card transaction (including refund transactions on any payment card).
- Don't use your merchant facility to transfer funds between your own accounts.
- Refunds should only be processed to the original card used for the transaction.
- Records of all transactions need to be retained in a secure place for 18 months after which they should be securely destroyed.
- Be alert to, and report all credit card fraud.
- Protect account, transaction and transactional information.
- Never store the CVV/CVC codes (3 digit security codes on the reverse of the card).
- If cards are left behind at your premises, keep the card in a safe place for two business days. Only hand the card over after establishing the claimant's identity. If not claimed within two business days, contact the issuing bank or securely destroy the card.
- Follow the correct authorisation procedures for manual transactions.
- Make sure you are PCI compliant for every payment channel you use.
- Be aware of your obligations as stated in the MCCFA.

Find out more

Download the Merchant Credit Card Facility Agreement (MCCFA): **westpac.co.nz/mccfa**

Visit the PCI DSS website: **pcisecuritystandards.org**

Call the Westpac Merchant Assist team: **0800 888 066**, option 4