more than money

Security at NAB

Protecting you from the risk of fraud and scams

V1.10

Protect your business online

Secure ways to bank

Customers expect a secure, quick and convenient experience when they shop online. To help merchants face the growing threat of e-commerce fraud, NAB provides a secure channel that keeps your business and customers safe.

Free fraud prevention tools that protect your business.

reCAPTCHA

When a fraudster wants to use stolen card information for purchases, they look for vulnerable websites to 'test' with automated scripts or 'bots'. This is also known as a Bank Identification Number (BIN) attack.

reCAPTCHA, a free tool from Google, can tell humans and bots apart to help make your site less vulnerable to these kinds of BIN attacks.

NAB Transact risk management

Our free tool provides you with the opportunity to identify potentially fraudulent e-commerce transactions before they occur to help minimise chargebacks and write-offs.

- You set up your own risk scoring rules from within the NAB Transact management portal
- The system automatically detects high risk transactions based on your scoring rules and can be set to decline those transactions
- Transaction patterns are analysed in real-time to provide immediate protection
- You can view risk score results in the NAB Transact Management Portal to streamline your Risk Management rules
- You can choose to be notified by email if a transaction is flagged as high risk

For more information about EMV 3-D Secure or how to register, speak to your Transactional Specialist.

EMV 3-D Secure

Working with Visa Secure and Mastercard® Identity Check, our EMV 3-D Secure service provides a secure channel to process online card payments for your business.

Additional layers of verification authenticate the cardholder, to make the process secure, effective and seamless for stakeholders and customers.

And for added security, it also aims to reduce fraudulent transactions and chargebacks.

EMV 3-D Secure benefits

- Reduce fraudulent disruptions that affect your business and cardholder's experiences
- Improve cardholder engagement and loyalty
- Create good customer experience and repeat shoppers
- Drive revenue by reducing shopping cart abandonment
- Improve sales with better transaction completion rates and higher approvals rates

How EMV 3-D Secure works

1. Cardholders make an online purchase.
2. To confirm the purchase is being made by the actual cardholder, EMV 3-D Secure sends the issuer data about the transaction including, payment method and device information.
3. The issuer reviews the data, provides the authentication and processes the transaction.
4. The issuer can also choose to authenticate cardholders with a one-time passcode (OTP), knowledge-based questions, biometrics or other methods.

Terminal security

Safeguard your business from payment scams

One of the best ways to protect your business is to be hyper aware of payment fraud. Learning about common terminal scams and card fraud can help you reduce the risk of costly chargebacks.

Terminal takeover

Having physical possession and control of a merchant terminal is also known as 'terminal takeover'. In situations where the manual key function is enabled, scammers can re-key transaction amounts or pay for goods and services using a stolen card number.

The fraudster can benefit by:

1. Entering or 'hand-keying' the details of a stolen card into the terminal to make a significant purchase and leave with the goods
2. Entering or 'hand-keying' the details of a stolen card into the terminal for an amount significantly larger than the original amount and then demanding an immediate refund onto another card

Terminal theft

This is when criminals steal the physical terminal, by switching it with a fake identical terminal.

Criminals will then attempt to process refunds to their own card with the potential added risk of:

1. Processing compromised cards, exposing merchants to chargebacks and,
2. Refunding the unauthorised settlements from the compromised cards to their own card

Terminal security tips

- Educate front-line staff about fraud, payment scams and the risks associated with your terminal.
- Keep terminals behind the counter or on the person of your employees.
- Don't allow customers to edit or manually enter transactions and disable the manual key entry feature on your terminal, if you don't require it.
- Set a strong terminal password and activate the lock feature when the terminal is unattended.
- Keep a list of your terminals, including their make, model and serial number. Check these daily.
- Inspect your terminals for any changes or evidence of tampering.
- Ensure you change the default PIN on your terminal for refunds, and keep the PIN function enabled.

Card payment tips

- For contactless transactions, ask the cardholder to tap the card against the contactless card reader and, if prompted, enter the PIN.
- Always swipe or insert the card through your terminal yourself and only have the cardholder enter their PIN when prompted or take an imprint of the card and have the purchaser sign the sales voucher; and
- Where prompted to get a signature or where using manual vouchers, check the signature and compare the purchaser's signature with the signature on the card

Merchant chargebacks

Save yourself from costly chargebacks

A chargeback is when a cardholder disputes a card transaction. To reduce costly chargebacks, it's important to understand the process and each party's involvement.

Merchant chargeback rights

When a cardholder disputes a transaction, the merchant must provide evidence of the transaction. This includes the process of authentication and authorisation of the cardholder and transaction.

If the merchant can't provide legitimate evidence of the transaction and cardholder, then a chargeback is made against the merchant for the funds.

Common reasons for chargebacks are:

- The cardholder did not make the transaction (usually because of fraud)
- Cancelled recurring transaction
- Goods not as described, faulty or defective
- Failure to respond to voucher requests

How we handle chargebacks

When we're notified of a chargeback, NAB will request some information from you. If you want to defend the cardholder's dispute, it's your responsibility to respond with a valid answer.

This may include:

- A signed copy of the transaction voucher or receipt;
- A copy of the order or invoice;
- A copy of any correspondence received by you from the cardholder

Security tips

- It's important to keep all documentation about your transactions. This makes it easier to respond to any 'retrieval requests' if a transaction is disputed.
- Visa and MasterCard rules request that a PIN or signature be obtained during a transaction, except for contactless transactions. That means, Card Not Present transactions like online payments, are always liable for a chargeback.
- Never accept payments on behalf of third parties or for services you don't provide.
- Don't agree to forward payments or funds to other businesses or people.
- Watch out for customers who say they can't be contacted or unable to view the goods being purchased.
- Reduce your liability with EMV 3-D Secure for e-commerce transactions.

Electronic chargeback reporting

Registering for reports of chargebacks and information requests keep you informed and reduces processing times.

The report gives you:

- Requests for information or evidence of transaction
- Urgent or outstanding requests for information
- Acknowledgement of information received
- Chargeback pending notifications
- Chargeback debit advice

Speak to your Transactional Specialist about this free reporting service

For more information

Learn how to reduce chargebacks and protect your business from fraud:

nab.com.au/business/payments-and-merchants/merchant-support-centre/avoiding-chargebacks

Cybercrime

Protect yourself from cyber threats

More businesses are being targeted by sophisticated cybercrimes. NAB's large Security team is dedicated to protecting your business by helping you to spot suspicious activity online.

Business email compromise/invoice scams

Business email compromise is when criminals take over an organisation's email account with the aim of sending fake invoices, requesting updates to bank account details, or intercepting and altering payment details. Because the invoice looks legitimate, the recipient might not question the payment details, and send the payment to the account controlled by the criminal.

To prevent this, you'll need a process that requires the receiver to check the requester's email address carefully, before calling them to confirm the request using the contact's most current details.

Phishing

Phishing emails, SMS and phone calls are designed to trick you into providing personal information like:

- Usernames and passwords
- Credit card details or bank details
- Your name, date of birth, etc.

Criminals use these contact methods for the same reason legitimate businesses do, it's a cheap and easy way to get to a lot of people.

Phishing emails often pretend to be from legitimate companies such as banks, courier companies, or government departments and contain links to fake websites which trick people in to entering their bank details or personal information.

If you receive this type of communication, don't provide any information, and please forward to phish@nab.com.au. If you're unsure, you can always call NAB or your banker.

Signs of awareness

All businesses face the threat of cybercrime. Look out for the following signs of a suspicious message or call:

- A request to change payment details
- Asking for your personal or banking information
- Sender is unavailable to verbally confirm the request
- The sender's email address doesn't match the organisation the email is pretending to come from
- It's generically addressed (e.g., Dear Customer), and there's no sign off
- There's a sense of urgency (e.g., provide your information or we'll restrict access to your accounts)
- The tone differs from previous requests
- Incorrect spelling and improper grammar

Security tips

- Create safe payment processes. It's important to verbally verify payment requests or changes to payment details.
- Your employees are the first line of defence against cyber-attacks. Teach them to recognise and handle suspicious emails, text messages and phone calls. If your business gets a fake invoice, share it around so your employees know what to look out for in the future.
- Keep software up to date, including your anti-virus software.
- Protect your business data by regularly backing up, storing offsite and test your backups regularly.
- Be vigilant on passwords and access management for all staff.
- Put appropriate transaction controls in place, such as separate duties or dual authorisation.
- Use strong passwords and multi-factor authentication to protect your email account. Two-factor authentication adds security by using an extra authentication method, such as a code sent to your mobile phone via SMS.

Our security commitment

Banking securely

NAB is committed to keeping you safe and wants to work with you to reduce the risks to your business. We provide informative resources and tools, information on product features for enhanced security, and keep you updated on industry insights. By being aware of fraud and cybercrime threats, you can help reduce the risk of costly chargebacks, or harm to the business' reputation.

Security Hub

Our Security Hub (nab.com.au/securityforbusiness) provides up-to-date tools and the latest information and advice on security to minimise the risk of fraud and scams.

Within this Hub you will find:

- Security alerts (nab.com.au/securityalerts)
- NAB's security podcast (nab.com.au/securitypodcast)
- Monthly webinar series (nab.com.au/cyberandfraudsessions)
- A cyber security toolkit for businesses (nab.com.au/cybersecuritytoolkit)
- Cyber safety training (nab.com.au/cybersafetytraining)

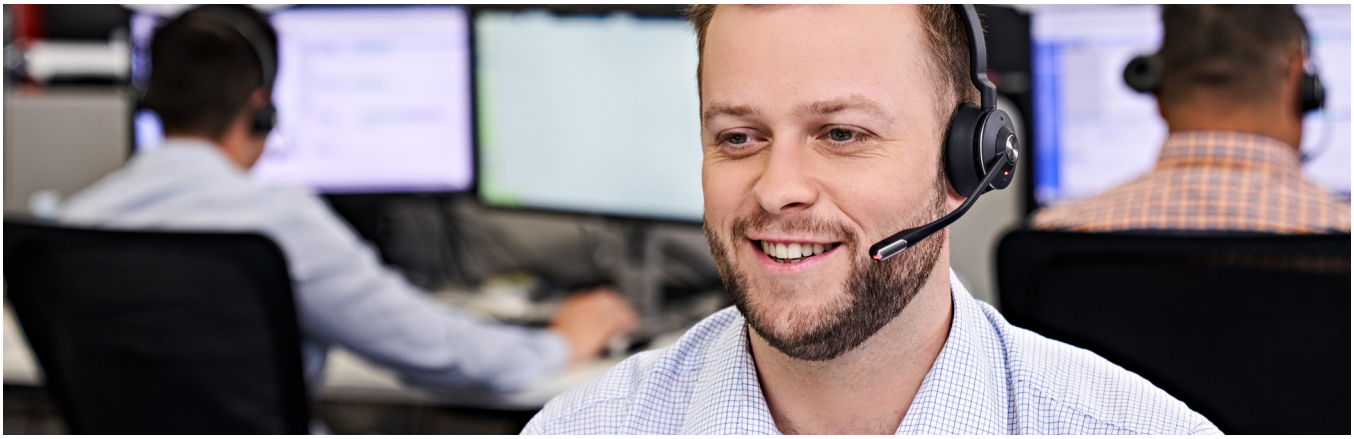
And a whole range of articles and videos, including:

- How to identify and avoid fraud and scams;
- How to protect your personal information;
- How to protect your business data; and
- How to manage security and running a business

For more information

- Australian Cyber Security Centre – ACSC (cyber.gov.au)
- Report a cyber incident (cyber.gov.au/report)
- Become an ACSC partner (cyber.gov.au/partner-hub/acsc-partnership-program)

NAB support teams



Our team	Assistance capabilities	Contact & availabilities
NAB Connect Support	• Technical support • Training • Password resets • Traces	• PH: 1300 888 413 • Monday to Friday 7:30AM–8:00PM (AEST) • Saturday 9:00AM–2:00PM (AEST)
NAB Transact Support	• Technical support • Integration • Password resets	• PH: 1300 852 950 • Email: support@transact.nab.com.au • Monday to Friday 8:00AM–8:00PM (AEST)
NAB Merchant Fraud	• For queries about preventing credit card fraud	• PH: 1300 622 372 (Option 3) • Email: merchant.fraud@nab.com.au • Monday to Friday 8:00AM–5:00PM (AEST) For Chargebacks: • 1300 781 935 • Email: merchantchargebacks@nab.com.au • Monday to Friday 8:30AM–5:00PM (AEST)
NAB Cards Fraud Team	• For queries about credit card transactions	• PH: 1300 622 372 (Option 1) or if calling from overseas +61 3 8903 9952 (Option 3) • Email: card.fraud.prevention@nab.com.au • Available 24/7
NAB Emergency Cards Team	• For queries about lost or stolen cards	• PH: 1800 033 103 or if calling from overseas +61 3 8641 9121 • Available 24/7

Received a suspicious message?

- Forward suspicious emails to phish@nab.com.au and then delete it
- Forward suspicious text messages to 0476 220 003 and then delete it
- You will not receive a personal response from the above contacts
- If you responded to a suspicious email or text message, please call NAB on 13 22 65 immediately or visit your local branch