Security Guide

for electronic transactions

Firefighters Mutual Bank

Firefighters Mutual Bank is a division of Teachers Mutual Bank Limited

Teachers Mutual Bank Limited ABN 30 087 650 459 AFSL/Australian Credit Licence 238981

Who We Are

Firefighters Mutual Bank is a division of Teachers Mutual Bank Limited ABN 30 087 650 459 AFSL/ Australian Credit Licence 238981.

In this document, "the Bank", "we", "us" and "our" means Teachers Mutual Bank Limited; and "you" means a person with one or more of our products or services.

We are committed to safeguarding your personal details, money and financial transactions. We protect you with industry leading security systems, transaction monitoring and fraud prevention tools so you can enjoy a secure electronic banking experience.

Electronic banking transactions occur when you deposit, withdraw or transfer money from your account using the following methods:

- Cards
  - rediCard
  - Visa Debit card
  - Credit card
- Phone banking
- Online banking
  - Internet banking
  - Mobile banking
  - Pay anyone

You can protect your electronic transactions and account information by using the security tips in this guide.

Contents

Card security

Protecting your card

- Sign the signature panel of your card as soon as you receive it.
- Make a record of your card number and telephone number for reporting lost or stolen cards and keep it in a safe place.
- Report lost or stolen cards immediately to avoid fraudulent transactions.
- Keep copies of sales and ATM receipts.
- Ensure that you get your card back after every purchase or ATM transaction.
- Never give your card to anyone, even family or friends. You may want to request an additional card for their use.
- When your card expires, destroy it by cutting it in half through the signature and magnetic strip.

Protecting your PIN

- Don't tell anyone your PIN. No one from a financial institution, the police, or a merchant will ask for your PIN. You are the only person who should know it.
- Never record your PIN (disguised or not) on a card, device, computer, mobile phone or tablet device.
- Don't write your PIN on your one time password device, account statement or anything you keep with your card.
- Don't select a PIN that is the same as any of your existing PINs. Select a unique PIN to reduce the chance of someone discovering all of your PINs and access codes.
- When changing your PIN or access code, avoid obvious options such as your name, telephone number or date of birth.
- Change your PIN regularly.
- Use a PINSECURE card, a safe and secure way of storing your PIN. This is provided when we send you a new PIN.

Treat your card as if it is cash.
Do not leave it unattended.

Using your card at an ATM or EFTPOS terminal

- Be ready to make your transaction when you approach the ATM or EFTPOS terminal.
- If the ATM or EFTPOS terminal appears abnormal in any way, do not use it.
- If an ATM displays messages or signs indicating that the screen directions have been changed or to use another ATM, do not use it. Banks and other ATM owners will not put up messages directing you to specific ATMs, nor would they direct you to use an ATM which has been altered.
- Memorise your PIN before you approach the ATM or EFTPOS terminal.
- Make sure you cover your PIN and stay alert when at an ATM or EFTPOS terminal.
- Be aware of people around you at the ATM. If you feel uncomfortable, use another ATM.
- Take your receipt with you as a transaction record.
- If your card gets stuck inside an ATM, be suspicious of anyone offering their help. Criminals can obtain your PIN by several means, then retrieve your jammed card from the ATM and use it to withdraw funds.

After completing your transaction,
secure your card and cash immediately
before exiting the ATM or EFTPOS terminal area.

Card security and online purchases

- Look for the padlock displayed on your browser which helps to determine if the website you are using protects your information.
- Only use known and reputable online merchants or stores. Anyone can set up a website, so if you are unsure of the company or their online security then ask for more information before you use their service.
- Make copies of online receipts to make it easier to check your statement.
- Always check your statement, especially after a trip. Check all transactions, even the small ones, because criminals test stolen accounts by buying inexpensive items rather than large ones.

Verified by Visa **protects your online purchases.**

Online banking: Security tips

Internet and phone banking

- Always type our website address, which is listed on the back of this brochure, into the address bar of your web browser to access internet banking.
- Do not share your access code with anyone including family members or our staff and change your access code regularly.
- Never provide your personal banking information over the internet or phone.
- Never record your access code on your computer or mobile phone.
- Regularly check your transaction history or statement for any unusual or suspicious transactions.
- Increase/reduce your daily transaction limit on your account to meet your daily transaction needs.
- Avoid using public computers at internet cafés or libraries to access internet banking.
- Don't leave your computer unattended while logged into internet banking.

Mobile banking

- Never store your banking passwords in your smartphone.
- If you don't need to connect to the internet you should switch off Wi-Fi™ and Bluetooth™ in order to ensure your smartphone security is not compromised.
- Only use Wi-Fi™ hot spots that are reputable and password protected.
- You should install smartphone security software and consider programs that can wipe data in the cases of theft or losing your smartphone.
- You should make use of built in security features such as auto-locking and password protection.
- Do not 'jailbreak' your smartphone as this makes it vulnerable to malware.
- Limit the amount of personal information on your smartphone.
- Make sure you delete all personal details if you sell or discard your smartphone.

One time password security
protects all new and unfamiliar transactions.

Other important information

Protection with security software

- Ensure you have security software installed on your computer including anti-virus, anti-spyware, anti-spam and firewall products.
- Ensure regular automatic updates are enabled and virus scans are completed. This will help to keep your computer protected against external attacks by viruses, worms or hackers.
- Be aware of email, online and telephone scams. We do not send emails requesting you to confirm or disclose your online banking login information.
- Delete spam email and don't open email attachments from unknown sources.
- Choose a reputable online service provider to supply your internet access.
- Disable the option on your web browser to automatically remember user names and access codes.

Reduce identity theft

- Secure your letterbox to help prevent mail being stolen.
- Ensure documents containing personal details are destroyed or shredded.
- Notify us immediately of changes to your address or contact details.
- Set up a password on your account to use when you speak to us.

Unauthorised electronic transactions

The ePayments Code provides information on situations where you could be liable for unauthorised electronic transactions involving your card, access code or PIN. Refer to www.asic.gov.au for more information.

Request to receive your statements online.

Notifying us

Make sure you contact us as soon as you become suspicious or aware that:

- your card has been misused, lost or stolen
- your PIN, access code or any password you use to access your account becomes known to someone else
- your security token has been misused, lost or stolen
- your mobile phone is lost or stolen if your mobile number is registered for SMS security
- there is an error or an unauthorised transaction on your account.

Keep up to date

For more information go to our website.

Other useful websites

www.staysmartonline.gov.au

www.scamwatch.gov.au

www.protectfinancialid.org.au

www.afp.gov.au

www.moneysmart.gov.au

www.crimecommission.gov.au

www.mycreditfile.com.au

www.microsoft.com/security

Be aware of email, online and telephone scams.
We do not send emails requesting you to confirm or disclose your online banking login information.

Key terms

Term	Meaning
Access code	Your online or phone banking password
ATM	Automatic Teller Machine
Chip	An electronic microchip embedded in a Visa Debit card or Credit card offers better security than the magnetic strip, because the chip is more difficult to counterfeit
EFT	Electronic Funds Transfer
ePayments Code	ePayments Code issued by the Australian Securities and Investments Commission (ASIC)
EFTPOS	Electronic Funds Transfer at Point of Sale
Electronic transaction	Any transaction using your account, card, PIN, access code, password, mobile phone or security token
Merchant	Any retailer or online store that accepts EFTPOS or credit card payments
One time password	A six-digit security code sent to your phone via SMS or a security token
Online banking	Internet, mobile and pay anyone
PIN	Personal Identification Number used for ATM and EFTPOS transactions
Security token	A security token generates a one time password which is required when making certain transactions in online banking
Skimming	Involves using a device, either attached to an ATM or at a merchant without your knowledge, to copy the information stored on your card's magnetic strip to create a counterfeit card
SMS security	SMS security generates a one time password on your mobile phone which is required when making certain transactions in online banking
Spam	A disruptive, commercial message posted on a computer network or sent as an email
Unauthorised transaction	A transaction that has been made by someone else on your account without your consent or approval
Verified by Visa	Verified by Visa is a free service that provides extra protection when you shop online at Verified by Visa merchants using your Visa Debit card or Credit card

This page was left intentionally blank

Need more information, we're here to help

1800 800 225
8am to 7pm, weekdays and 9am to 3pm, Saturday

contactus@fmbank.com.au

fmbank.com.au

Card hotline
To report the loss, theft or unauthorised use of your card:

- Within Australia call 1800 800 225.
- Outside Australia – for Visa cards:
  - Please contact us before you travel overseas for the current Visa hotline arrangements; or
  - Or call +61 2 9735 9225

Printed on 100% recycled paper

Firefighters Mutual Bank is a division of Teachers Mutual Bank Limited
Teachers Mutual Bank Limited ABN 30 087 650 459 AFSL/Australian Credit Licence 238981
Effective 1st November 2016 | 00146S-MEM-FMB-1116