SAFETY - FIRST AID CHECKLIST

1. Sign your Cards immediately when you receive them
2. Check your transactions regularly and report anything unusual immediately to the 24/7 Card Services team
3. If you print statements from the internet, keep them safe and shred them when you've finished using them
4. Never give your personal details to someone who phones you claiming to be from a reputable company
5. Don't give out your details in response to unsolicited email
6. Be wary of anyone who asks for common security details, like your mother's maiden name, date of birth, or information about your work
7. Never give your PIN to anyone, not even if they claim to be from Federal Bank
8. Don't let yourself get distracted when using ATMs – somebody may be trying to get to know your PIN

ATM FRAUD

1. Never write down a PIN or keep it together with the Card. Be very alert when using ATMs, and ensure:
    - ☐ The machine has not been tampered with
    - ☐ Nobody can watch you entering your PIN
    - ☐ Card and cash are concealed and safe before you leave the machine
    - ☐ You retain any printed records for safe disposal at a later time
2. If your Card is retained, contact Card Services immediately for assistance

COUNTERFEIT FRAUD

Always keep your Card in sight when making a purchase or it may get skimmed. "Skimming" occurs when the genuine data on a card's magnetic strip is electronically copied onto another card, allowing fraudsters to steal the funds on your card. This can happen at gas stations, restaurants, bars and at ATMs. Skimmed card information is often sold on to organized crime groups.

USING YOUR CARD ON THE INTERNET

Make sure that you're using a secure browser. A secure browser such as Microsoft Internet Explorer or Mozilla Firefox will indicate whether the website you are visiting is secure or not. These browsers scramble your personal data before sending it, so no one else can read it. Ensure that your computer has upto-date virus protection and a firewall will help protect you from attacks.

KEY POINTS WHEN BUYING GOODS/ SERVICES ON THE INTERNET

a. Know who you are dealing with. Use a reputable company and type its internet address into the browser yourself
b. Don't give out your details in response to unsolicited email
c. If the website gives you the option of using a secure checkout; opt for yes
d. Just as you save till receipts, in case you need to return or exchange something, you need to keep a record of all transactions too. Print and save a copy of your completed order form and your order confirmation

PHISHING

"Phishing" is an attempt by fraudsters to "fish" for your card or account details. Phishing attempts usually appear as an email apparently from your bank or card issuer. Within the email, you are then encouraged to click on a link to a fraudulent log-in page, designed to capture your details. We may contact you by email, but we will NEVER ask you to click on a link that directs you to enter or confirm your security details. If you are in any doubt about the authenticity of an email appearing to be from us, telephone Card Services immediately.

PHARMING

"Pharming" employs the same type of tricks as Phishing to lure you to a site address, but uses hidden software to redirect you from real websites to the fraudulent ones. This is particularly clever, as it hijacks trusted brands of well known banks, online retailers and card issuing companies and convinces you to respond under cover of trust to enter your personal details.
Just remember, if you are asked to type your PIN into a website along with your Card details, it is probably a fraudulent website, and you should close the browser and contact Card Services immediately.

LOST AND STOLEN CARDS

If you lose your Cash Passport or it is stolen, reporting this to Card Services immediately will help protect the funds on the Card. Our dedicated team is on hand 24 hours a day, seven days a week, to help you get back to enjoying your travels.