

**Important Information  
on Security regarding  
Electronic Account Access  
and  
Regular Payment  
Arrangements**



For You, Your Family, Your Future.



**The Police Department Employees' Credit Union Ltd**  
ABN 95 087 650 799. AFSL/Australian Credit Licence No. 240018  
Level 27, 1 Market Street, Sydney NSW 2000.  
Customs Credit Union is a division of The Police Department  
Employees' Credit Union Ltd. All terms and conditions that apply to  
Police Credit Union also apply to Customs Credit Union.

## **ELECTRONIC ACCOUNT ACCESS**

These guidelines are provided to assist you in maintaining security for accounts where transactions may be carried out through electronic access. Information is also provided regarding your liability for transactions on your accounts through electronic access.

## **SUMMARY OF SECURITY GUIDELINES**

### **Internet and Mobile Banking**

The Credit Union employs the third-party verification (SSL certificate) to ensure uncompromised identity. Effectively, every time a user is connected to the Credit Union's Internet Banking facility, the SSL "handshake" occurs where a browser requires authentication from the Credit Union's server. If the information does not match or the certificate has expired, the browser displays an error message.

Using SSL technology also ensures that all information exchanged during your Internet Banking session is encrypted, scrambling the transmission and guaranteeing message privacy and integrity.

For Internet Banking, we have also implemented a second factor authentication function known as a *Captcha* test (Completely Automated Public Turing Test To Tell Computers and Humans Apart). Captcha is functionality that protects websites against unwarranted attacks from Trojans by generating text that humans can read easily but current computer programs cannot.

You are also able to order a one time password security token which provides an extra layer of security for your details to help counteract fraudulent internet attacks. We strongly recommend all Members take advantage of security tokens, available to order free of charge through Internet Banking or call 131 728.

### **Redial Telephone Banking**

We employ a telephone banking system (Redial) which only allows you to access your accounts after you have provided your access code electronically over the telephone.

### **Cards**

For EFTPOS and ATM transactions, (where you press savings or cheque account) we employ an electronic card access system which only allows access to your accounts after you have provided your personal identification number (PIN).

For transactions where you press "credit" there may be no need for pin or signature for small amount transactions or payWave transactions.

## **WHAT YOU NEED TO DO TO MAINTAIN SECURITY**

### **PIN and Password Security**

- Never record your PIN or password on your card or on anything that you usually keep with or near your card. We recommend you memorise your PIN and Password. Also never use your PIN as a password.
- Destroy any notification we send you containing PIN or passwords.
- When selecting a PIN or password, do not choose numbers and letters that can be easily identified or associated with you (such as initials, phone numbers, date of birth etc).
- Try not to use the same PIN and password for every service.
- Never disclose your PIN or password to anyone. No employee from the Credit Union, the police or a merchant should ask for your PIN or password.

### **Internet Banking, Mobile Banking and Website Security**

- Always log in directly by typing our site address [www.pcu.com.au](http://www.pcu.com.au) ([www.customscu.com.au](http://www.customscu.com.au) for Custom Members) from your browser.
- When using internet banking, check for a locked padlock symbol. This indicates that it is secure to use.
- Never accept links or redirections from other websites or emails for the purpose of logging into internet banking. Never click on an email that asks for your personal banking information, and beware of phishing emails.
- Change your password regularly. Never write your password down, store it on your computer and/or mobile device.
- Install anti-virus, anti-spyware and firewall software on your computer. If you use our Mobile Banking Service we recommend you also install anti-virus software on your phone to reduce the risk of phone hacking. To get the most benefit from this software, make sure you always keep it updated.
- When performing financial transactions online, never leave your computer or mobile phone unattended while the session is still active.
- If you use Mobile Banking you should ensure you place a password/PIN on your phone in case you lose your phone, to secure against unauthorised access to your accounts.

- Be careful about using internet banking from other PC's (such as those at some Internet Cafés) which may not have up-to-date virus protection installed.
- Always log off when you are finished using internet or mobile banking to avoid others accessing your account details.
- Safeguard your account details if you save or print them. Keep this information in a secure place or destroy it once you have finished with it.
- You should clear your browser cache files at the end of a session.
- Beware of windows that "pop-up" during an Internet Banking session and be very suspicious if it directs you to another site which then requests your account details or password.

## **Cards**

- Report lost or stolen cards immediately to us on 131 728, or if after hours call toll free on 1800 224 004.
- Sign your card on the signature panel as soon as you receive it.
- Protect your cards as if they were cash, always keep them in a secure place.
- Ensure that you get your card back after every purchase.
- Always check sales vouchers for the correct purchase amount before you sign them, and keep copies of your vouchers and ATM receipts.
- Always check your billing statement and verify the amounts of your purchases. Report any unauthorised transactions to the Credit Union immediately on 131 728.
- Destroy all old, cancelled or expired cards.
- When destroying your old card, be sure to cut vertically through the magnetic strip before disposing of it.
- Don't lend your card to anyone. You are responsible for all card transactions.

**Make sure you keep up-to-date on security issues by regularly visiting our website [www.pcu.com.au](http://www.pcu.com.au) ([www.customscu.com.au](http://www.customscu.com.au) for Custom Members) and clicking on the “Fraud Tips” link.**

## **SUMMARY OF LIABILITY GUIDELINES**

### **Liability for Use by an Authorised Person**

Where you have provided the means to access your accounts electronically to another person by:-

- authorising that person to have a Visa Card and/or Redicard linked to your accounts, or
- against our advice giving your access code details to that person, you are liable for transactions on your accounts carried out by that person.

### **Liability for Loss through Unauthorised Use**

Where there has been unauthorised use of your Visa Card, Redicard or access code, you are not liable for your loss if it is clear you have not contributed to your loss (and the transactions involved were carried out without your knowledge and consent).

However, if we establish you contributed to the unauthorised use, then you are liable for the lesser of:-

- the actual losses or
- the amount you are able to withdraw from your account or
- the total amount you would have been allowed to withdraw on the days that the unauthorised use occurred or
- the balance in the account accessed, including if applicable, the amount available through an Overdraft or Credit Card facility. If you delay in notifying us, then in addition to the previously mentioned losses, you are liable for the losses incurred (because of that delay on the same terms as previously detailed).

You are not liable where:-

- the losses are caused by the fraudulent or negligent conduct of our employees
- the losses relate to any component of internet banking that is forged, faulty, expired or cancelled
- the losses arise before we provide you with an access code the losses are caused by the same transaction being incorrectly debited more than once to the same account
- the unauthorised use takes place after you tell us that your access code has been misused, lost or stolen or has become known to an unauthorised person.

In all other circumstances not covered above, you are liable for the lesser of:-

- \$150.00 or
- the balance in the account accessed including, if applicable, the amount available through an Overdraft or Credit Card facility or
- the actual loss at the time we are notified of the loss, theft and/or misuse.

### **EFT Code of Conduct**

These guidelines will always be read in conjunction with the EFT Code of Conduct (available by contacting 131 728). In the event of any discrepancy between these guidelines and the EFT Code of Conduct, your liability for loss (if any) will be determined under the EFT Code of Conduct.

---

## **REGULAR PAYMENT ARRANGEMENTS**

### **What is a 'Regular' Payment?**

Regular payments can be either a recurring payment or an instalment payment. A Regular Payment represents an agreement between you (the cardholder) and a merchant in which you preauthorise the merchant to bill your card account at predetermined intervals (e.g. monthly or quarterly) or at intervals as agreed by you. The amount may differ or be the same for each transaction.

For example: You may ask your local gymnasium to charge your monthly gym membership fee to your credit card each month; or,

You may have purchased a new television from your local appliance store and are being billed by the merchant in subsequent multiple periods.

## **What are the benefits of Regular Payments?**

There are many benefits for cardholders who set up regular payments including:

1. Ensures timely payments to the merchant
2. Saves you time as the payment is processed automatically
3. Saves you money as you do not have to pay for cheques, money transfers or postage, nor will you be liable for late fees.

## **Customer Responsibilities & Obligations**

Regular payment arrangements are an agreement between you (the cardholder) and the merchant. You should keep a record of all regular payment arrangements you have established with your merchant and store in a safe place. A template for recording your regular payment arrangements is available from APCA's website [www.apca.com.au](http://www.apca.com.au)

You are responsible for notifying the merchant when your account details change, including a change in card number and/or change of card expiry date. Until you notify the merchant, your bank is required to process transactions from the merchant. Visit the Account Switching Service on our website [www.pcu.com.au](http://www.pcu.com.au) ([www.customscu.com.au](http://www.customscu.com.au) for Customs Credit Union Members) to generate a Change in account details letter to your merchant. We recommend you keep a copy of any Change in account details letter sent to your merchant and your earlier regular payment agreements. This correspondence will be required if your merchant does not comply to your request in a timely manner and you decide to dispute any incorrectly charged regular payments.

## **Customer Rights to Dispute**

Any issues with your regular payments, including the failure of the merchant to act on a change in account details advice, should be taken up directly with your merchant first. Should further assistance be required to resolve an issue between yourself and a merchant, contact the Credit Union on 131 728 for more information.

Visit APCA's website [www.apca.com.au](http://www.apca.com.au) to read FAQs on regular payments.

## Contact Us

### Police Credit Union

#### PCU Assistance Centre

Phone: 131 PCU (131 728) E/N: 88899

#### PCU Direct

Phone: 131 PCU (131 728) E/N: 88884

#### Sydney

Phone: (02) 8268 2500 E/N: 44850

#### Parramatta

Phone: (02) 9841 8200 E/N: 44700

#### Penrith

Phone: (02) 4720 5000 E/N: 44750

#### Newcastle

Phone: (02) 4908 6200 E/N: 44870

#### Canberra

Phone: (02) 6206 7000 E/N: 44860

#### Goulburn

Phone: (02) 4827 1000 E/N: 44730

#### Gosford

Phone: (02) 4320 0200 E/N: 44880

#### Wollongong

Phone: (02) 4221 9000 E/N: 44830

#### Campbelltown

Phone: (02) 4640 7000 E/N: 88839

#### Port Macquarie

Phone: (02) 6582 9900 E/N: 44840

**Email** [info@pcu.com.au](mailto:info@pcu.com.au)

**Website** [www.pcu.com.au](http://www.pcu.com.au)

---

### Customs Credit Union

**CCU Assistance Centre:** 131 728

**Canberra** Phone: (02) 6243 8900

**Mascot** Phone: (02) 8335 4200

**Melbourne** Phone: (03) 9642 1003

**Email** [info@customscu.com.au](mailto:info@customscu.com.au)

**Website** [www.customscu.com.au](http://www.customscu.com.au)

---

The product issuer for deposit and payment products is Police Credit Union Ltd, AFSL/Australian Credit Licence No. 240018. A Financial Services Guide (FSG) including terms and conditions is available at all Branches, on our website and upon request. Any advice given has not taken into account your personal needs and financial circumstances and you should consider whether it is appropriate for you. Please read and consider the FSG in deciding whether to use a particular product.