



“Police Credit Union owes you money”

There is an incredible number of cold calling scams doing the rounds at the moment and in some instances the name Police Credit Union is involved.

As part of one such scam, the caller advises you as the call recipient that Police Credit Union owes you a refund of fees.

The caller then asks for further personal details such as date of birth, credit / debit card number or even a tele-service code (although they don't use that actual term).

If you seem interested, they'll tell you a figure of the refund, that you need to pay a fee to receive it, and then advise you that the government will also be in touch in the next day or so, in an attempt to give the call an air of legitimacy.

So what are the fraudsters after?

The caller is looking to get enough personal information from you to either take over your identity (even if this is just using a credit card) and/or getting you to forward an amount of money in order to receive your “refund”. This is known as “advance fee fraud”.

Is PCU being targeted directly?

We don't think so - there are a number of other Police Credit Unions in Australia.

We have received calls from a number of people who are NOT members of PCU advising that they have received a call from “Police Credit Union head office” fitting the scam criteria.

We can assume that a significant number of such calls are being made to non-members as only a small percentage of people would bother to call us to let us know they have received such a call purporting to be from Police Credit Union.

Another way the caller has gotten their information is through a bogus “telephone survey” some time before they make the “fee refund” call. We have been told this survey is one about service, mortgages, banking and finance, call centres or similar things that can be related to finance in which the call recipient unwittingly reveals they bank with Police Credit Union.

What to do now

Have a read through the table on the following page so that you know the ins and outs of this scam. Stay alert to potential scams and let your family and friends know to do the same.

Most importantly, if you receive a call that fits any of the above criteria - hang up immediately!

Then please call Police Credit Union on 1300 131 844 immediately to advise us of the details of the call.

In some instances the callers are persistent and annoying – if that's the case then one suggestion is to obtain a whistle and give the caller a decent blast over the phone!

Stay up to date with scam information.

Keep an eye out for Fraud Watch articles which are published on our website www.policecu.com.au

In addition to this, you can find a lot of useful information on the world of scams on ACCC's SCAMwatch website www.scamwatch.gov.au

If you need any further clarification or have any other questions about scams, please contact our Risk and Compliance department on 1300 131 844.



What should I look out for?

What is listed here are several comments that staff, members and non-members have told us and an explanation for where the scammers have got the information.

COMMENT	EXPLANATION
The member is asked for by name.	They will ask for "Mr Jones" or "Mrs Jones" depending on if a male or female answers. The caller does not know your name - the name and number is taken straight out of the White Pages.
They are advised the caller is from Police Credit Union.	They don't know that you specifically bank with Police Credit Union. There is a credit union representing the police and emergency services in every state of Australia. There have been a lot of non-members receiving these calls, so the caller is just hoping for a hit.
They are advised the caller is from head office.	When questioned, the caller often mentions being in Sydney – this is clearly wrong because our head office is in Adelaide, SA!
The member is asked to confirm their identity.	The caller is trying to get enough information to steal your identity.
The member is asked to confirm their card number as the caller reveals they have the first four (4) digits of the member's card – 4434.	PLEASE NOTE – the first four digits of many different credit unions cards are 4434. It is the first six (6) digits of a card that identify a particular credit union ie 4434 49 is one of our BINs (Bank Identification Numbers). Again the caller is hoping for a hit. The caller is trying to get your card number so they can use it fraudulently. Unless you have given out your actual card number there is no need to block your card.
The caller ID often shows 02 8005 8349 or another Australian phone number.	Research has shown this number is making a large number of fraudulent calls. It is thought the calls are being made via VOIP (Voice Over Internet Protocol) and are masked with this caller ID (or another domestic number) to give it some legitimacy.
The member is advised they are due a refund of fees that have been incorrectly charged, sometimes since the beginning of the membership.	There is no refund of fees due! The caller is hoping to ignite your interest. If you seem interested, you can be advised that the "government" will call tomorrow. Again this is to provide an air of legitimacy to the call.
The member is called by the "government" using the terms Department of Fair Trading, or Consumer Affairs or in one instance "Department of Bank Refunds".	This is where the final trap is being laid. You will be advised that you need to pay a fee to claim your refund. Often if you have been advised of a likely refund in the first call, the figure mentioned in this second call is substantially higher. A recent example is a member was advised they were due a refund of \$3,000 and the fee to be paid was \$300. In the second call, this had increased to a refund of \$9,000 and a fee of \$900!
The caller is advised that once the fee is paid the refund will be deposited straight in to their account.	To obtain the "refund", the fee is often asked to be paid via Western Union to an overseas account - strange considering the fee is meant to be paying an Australian Government department! Unfortunately though, some people have fallen for this. You are then asked to provide your membership details, or alternatively told that you can pay the fee via a credit card. If it's a credit card, they'll ask for the 3 digit CVV (Card Verification Value) number from the rear of the card thus allowing the fraudster full use your card.