Fraud

(30 June 2022)

We take fraud and the security of your account seriously at Cmobile. We are committed to helping prevent you becoming a victim of fraud, and to providing assistance if you do become a victim of fraud.

Fraud via your mobile phone service can occur in a number of ways. For example:

- Unauthorised mobile porting, where your service is ported to another provider in the control of the scammer. Once the scammer has control of your number, they may use it to attempt to access your financial accounts and other information.
- Unauthorised SIM swap, where your number is transferred to another SIM which is used in a device under the control of a scammer. In this case, the service does not transfer from your current provider. Scammers may attempt to change information on your mobile account in order to facilitate a SIM swap.
- Phishing scams. These involve scammers posing as legitimate entities in an attempt to gain access to your personal or private information.

How we keep your account secure

We take steps to prevent unauthorised mobile porting by requiring you to nominate a porting PIN when you sign up with Cmobile. That PIN is required in order to port your number to another provider and without it, the port cannot occur.

In order to protect your account from activity which would enable an unauthorised SIM swap or other fraud on your account, Cmobile has introduced two-factor authentication for high-risk transactions to authenticate the identity of the person making the request. A high-risk transaction is any transaction that could potentially facilitate fraud on your account. Examples include:

- Changing your address
- Requesting a SIM swap in cases where your phone has been lost or stolen
- Adding or removing an authorised representative
- Disclosure of your personal or account information
- Adding a new service to your account

This list is not exhaustive and Cmobile will consider all requests and require two factor authentication in those cases where we reasonably believe the request is high-risk or where we are otherwise required by law.

What to do if you suspect your Cmobile service or account has been subject to fraud

If you believe your Cmobile service or account has been subject to fraud, please contact Cmobile and your financial services provider(s) immediately. Our contact details are:

Email: support@cmobile.com.au

Phone: 1300 545 000 (Monday to Friday 9am to 6pm)

0414 201 181 (After hours)

It is important you contact your financial services provider because if you have lost control of your phone number, scammers may attempt to use the number to access funds held in bank accounts where security codes are sent to the mobile phone number associated with your account.

What to do if you believe your account is at risk of fraud

If you believe that your Cmobile service is at risk of fraud, please contact us to discuss. We can discuss further fraud mitigation protections that are appropriate for your circumstances. This may include features such as adding additional security questions to your account, nominating a senior manager within Cmobile to approve any changes to your account or any other measures that we reasonably believe will assist in maintaining the security of your account.

What you can do to reduce the risk of fraud

It is important that you always remain vigilant when using your mobile phone. If you have received an email or SMS from Cmobile that is out of the ordinary or that you did not expect, please contact us immediately and do not action or respond to the message. Do not click on links or open attachments contained within SMS or emails from senders you do not know or recognise, and remain vigilant even with links or attachments from senders you do recognise.

Do not share your Cmobile account information with anyone, particularly your account number, password or porting PIN.

Pay close attention to your bills and contact us immediately if you notice any unusual activity on your account.

What to do if you believe your identity has been stolen and used to create an account with Cmobile

Contact the police and report the identity theft and obtain the police report or event number. Once you have the police report or event number, contact us on the details above and provide the following:

1. The police report or event number.
2. A Statutory Declaration that is properly completed, signed and witnessed. If you need assistance finding a statutory declaration to complete, please contact us and one can be provided to you.
3. Any other supporting documentation that you have which evidences the fraudulent connection.