Fraud and Scam Protection

Flip has long maintained account security verification processes as an additional layer of protection against unauthorised access and potential threats

To protect your private information from unauthorised high risk customer activity, identity authentication processes will be used to authenticate your identity prior to certain transactions proceeding. These transactions involve what Government regulations classify as high risk transactions. These include but are not limited to the following:

1. Changing or cancelling a service.
2. Adding additional services or products to an account.
3. Address changes, modifications, alterations, relocating or moving.
4. Amending or cancelling pending orders.
5. Simcard changes and replacements
6. Any other transaction that is deemed a high risk interaction.

Before we undertake any high risk transaction we will confirm at least two (2) forms of identification and send a verification code to you via SMS or email for you to confirm.

Additional Identity protection

In addition to the initial account verification above, when transferring your mobile number to Flip, we'll also further confirm it's really you:

- We'll send you another 4-digit code to your current Mobile number.

Please note: Make sure your mobile number remains active with the current provider until the transfer process complete:

- You will need to verify the code with us before we proceed

This step helps protect you from unauthorised transfers.

SCAM protection

Protecting yourself from scams comes down to a few consistent habits that make you much harder to trick.

Caution - First, treat any unexpected contact with caution. If you get a random call, message, or email claiming to be from a bank, delivery service, or government agency, don't trust it right away. Scammers often pretend to be real organizations like Australian Taxation Office or Commonwealth Bank. Instead of using links or phone numbers they give you, go directly to the official website or app yourself.

Verify - Always verify before trusting. Caller IDs, email addresses, and logos can be faked. If something seems even slightly off, look up the official contact details and reach out independently. Real companies won't mind you double-checking.

Slow Down -Take your time. Scammers rely on panic and urgency to get you to act quickly. Messages that say things like "act now," "your account will be closed," or "payment required immediately" are major warning signs. Slowing down gives you space to think clearly.

Private - Keep your personal information private. Never share passwords, one-time codes, banking details, or ID documents with someone who contacted you unexpectedly. Legitimate organisations do not ask for sensitive information like this out of the blue.

Do Not Transfer Money - Be careful with how you pay. Avoid sending money through bank transfers to unknown accounts, gift cards, or cryptocurrency — these methods are hard to trace and almost impossible to recover. Scammers frequently ask for urgent bank transfers. Safer options like credit cards offer better protection.

Protect your devices - Make sure your devices are secure. Keep your phone and computer updated, use strong and unique passwords, and turn on two-factor authentication. These steps reduce the risk even if someone tries to access your accounts.

Keep Alert - Stay aware of common scams like phishing emails, fake delivery notifications, investment offers promising high returns, and romance scams asking for money. Knowing what's out there makes it easier to spot something suspicious.

Tracking Scams - If you're ever unsure, you can check current scam alerts through Scamwatch, which tracks scams in Australia and helps with reporting. https://www.scamwatch.gov.au/

Telco-specific scams to watch out for

Scammers sometimes impersonate telecommunications providers, including Flip. Be alert to the following:

- Unexpected calls or SMS claiming to be from Flip asking for your account password or one-time verification code.
- Messages claiming your service will be cancelled or suspended unless you act immediately — this is a pressure tactic.
- Fake links or websites that look like the Flip website asking you to log in or enter personal details.
- SIM swap fraud — someone contacts your provider pretending to be you and requests a new SIM to take over your number, which can then be used to access your bank and other accounts.
- Unauthorised mobile number porting — a scammer initiates a transfer of your mobile number to another provider without your knowledge.

Flip will never ask for your password or one-time verification code over the phone, by SMS, or by email. If you receive a request like this, do not comply — contact us immediately on 1300 354 788.

Current scam alerts

Scam tactics change frequently. We encourage you to stay up to date with the latest alerts and active scams circulating in Australia by visiting Scamwatch regularly: www.scamwatch.gov.au. This page will be updated as new scam types emerge.

A simple rule to remember is that if something feels urgent, asks for money or sensitive information, or seems too good or too alarming to be true, pause and verify it independently before doing anything.

What to do

If you suspect identity fraud, your number has been transferred without your permission or you may have been scammed you should immediately report this to the Authorities

Identity fraud (your personal details stolen) including unauthorized transfer of your mobile number contact:

IDCARE

https://www.idcare.org/

1800 595 160

They should be your first point of contact **it is** free and they will help to secure your identity and reduce damage. They guide you step-by-step (credit checks, document replacement, etc.)

General scams (even if no money lost) contact:

Scamwatch

https://www.scamwatch.gov.au/

Report all types of scams (texts, calls, emails, online). Helps warn others and track scam activity

If money or bank details are involved contact:

Your bank (e.g. Commonwealth Bank or whichever you use) Contact them **immediately** to stop transactions. They may recover funds or block accounts

Serious cases or threats contact:

Your local Police Force. If there's large financial loss, threats, or ongoing fraud

What to do right away

1. Contact your **bank** (if money/details involved)
2. Contact **IDCARE** for identity protection
3. Report to **ReportCyber** (the Australian Cyber Security Centre's reporting platform at cyber.gov.au/report) for cybercrime including hacking and identity theft
4. Log it with **Scamwatch**

Simple guide

- Identity stolen → IDCARE + ReportCyber
- Scam report → Scamwatch
- Money affected → Bank immediately
- Serious situation → Police

In the event you suspect that your service or account has been subject to fraud you should also immediately report the activity to us on 1300 354 788.