Important information

on how Squadron Energy will communicate with you

SQUADRON ENERGY

Protecting your personal information and safeguarding you from fraud is a priority for Squadron Energy. To help ensure payments to you remain safe and secure, we may contact you from time to time to confirm and verify changes to your personal details that you have requested.

Why do we verify your details?

- To ensure that the information we hold on file for you is correct and up to date. This helps us to identify and stop unauthorised changes that may occur.
- To ensure that we are acting in accordance with your requests.

When would we verify your details?

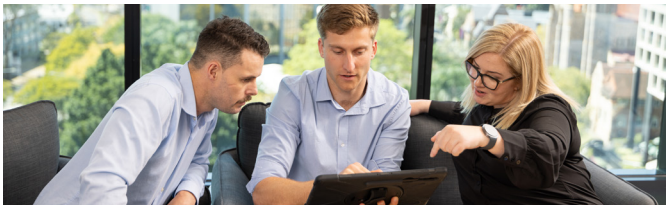
We may contact you to confirm:

- requests to update your personal details in our systems
- requests to update your bank details in our systems.
- if you are a new landowner

Squadron Energy communication

When we contact you to verify your details:

1. We will only verify changes to personal details by phone.
2. Phone calls will only come from an Australian phone number.
3. We will send a secure one-time passcode (OTP) via SMS to confirm we are communicating with you.
4. Any email correspondence sent to you, or you to us, should only come from an address ending in '@squadronenergy.com'.



If you are in doubt about being contacted by someone claiming to be from Squadron Energy, please contact us via your relationship partner from our Development or Operations team, or using contact information on our website www.squadronenergy.com/contact

Avoiding scams

We'd like to share the following tips with you to help you avoid falling victim to scams:

1. We will never try to contact you using:
   - a personal email account such as Hotmail or Gmail
   - WhatsApp, WeChat or other messaging applications
   - Facebook, LinkedIn, X or other social media platforms
   - an overseas telephone number.
2. We will never ask for passwords or credit card information.
3. We will never ask for your bank details via SMS.

Helpful resources

The following information can also help to further protect you to be more cyber aware:

- set strong and unique passwords across all of your online accounts
- use multi-factor authentication where possible
- keep on top of current scams through the National Anti-Scam Centre ScamWatch website.