

SECURITY · DATA BREACH · SCAM CALLS

Origin Energy Breach: The Second Wave Is a Phone Call

Australia's largest energy retailer is investigating a major data breach, and the details taken are unusually rich. The part that reaches your business arrives later, by phone, from someone who already knows the last four digits.

Origin Energy confirmed in late July 2026 that customer data had been accessed in a breach now under examination by Australian authorities. Origin said the data may include name, address, date of birth, contact phone number and account information, plus the last four digits of a credit card or last three of a bank account. Origin has around 4.8 million customers and has not confirmed the number affected; the person claiming responsibility told a newspaper he held about two million records, and later reporting put the figure closer to 900,000. The Australian Cyber Security Centre, National Office of Cyber Security, AFP and OAIC are involved. Why it matters to you: those partial payment digits are the exact detail a legitimate organisation uses to prove it is legitimate, so they turn the standard verification ritual into the attack.

The short version

Point	What is known
Data involved	Origin said it may include name, address, date of birth, contact phone number and account information, plus the last four digits of a credit card or the last three digits of a bank.
Timeline	Raised internally as a potential issue in early July 2026, assessed as credible around 22 July, publicly confirmed with customer notifications from 28 July.
How many people	Origin has not confirmed a figure. The claimant said around two million records; subsequent reporting has put the confirmed number closer to 900,000 current and former customers.
Type of incident	Data theft. No reports of encryption, destruction or service disruption, the lights stayed on and the bills kept arriving.
Investigating	Australian Cyber Security Centre, National Office of Cyber Security, Australian Federal Police, and the Office of the Australian Information Commissioner.
Unusual element	The claimant went to the media directly and was later reported to have agreed not to leak the data following some arrangement with Origin, which Origin has not confirmed.

■ Also worth knowing

Reason	What it means concretely
Your people are in the data	Millions of Australian households buy energy from Origin. Statistically several of your staff are in that dataset with their home address, date of birth and mobile number, the raw.
Breaches merge	Criminals combine datasets. Origin plus Optus plus Medibank plus a decade of smaller leaks produces a profile far richer than any one incident, and none of it expires.
Your brand is borrowable	Whatever you sell, someone can ring your customers pretending to be you. You carry the reputational damage from a fraud you did not commit and could not see.
Home details still unlock work accounts	Date of birth and address remain accepted as identity verification at far too many help desks. Possibly including yours.

“It won’t be leaked” should change nothing about your planning

Nobody can verify that a copy does not exist, has not already been passed on, or will not surface in two years. Data that has left an organisation should be treated as permanently in circulation. Plan for the fraud attempts, not for the reassurance.

■ Questions the full guide answers

- ☐ What did the Origin Energy breach expose?
- ☐ Why do the last four digits of a card matter so much?
- ☐ Has AI made data breaches more dangerous?
- ☐ What is the single most effective thing we can do?
- ☐ What are our obligations if our own business suffers a breach?
- ☐ How can a phone system help rather than being the weak point?
- ☐ Should we warn our customers, and what should we say?

This is the summary. The guide has the detail.

Every point above is worked through in full on our site, with the Australian context, the numbers and the exceptions. If you would rather talk it through, call 1300 663 222 or visit vocphone.com/about/contact-us.