

SECURITY · DATA BREACH · AUSTRALIAN BUSINESS

Origin Energy Breach: What Every Business Should Do

Australia's largest electricity and gas retailer is investigating a major data breach. The stolen data is unusually rich, and the second wave, the one that reaches your staff and customers by phone, has not arrived yet.

In late July 2026, Origin Energy confirmed that customer data had been accessed in a breach now being examined by Australian authorities. Origin said the information 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 account**. Origin has around 4.8 million customers and has not confirmed how many people were affected; the individual claiming responsibility told a newspaper he had accessed around two million records, and reporting has since put the confirmed figure closer to 900,000. Investigations involve the Australian Cyber Security Centre, the National Office of Cyber Security, the Australian Federal Police and the Office of the Australian Information Commissioner.

The short version

What we know	Detail
When	Flagged as a potential issue in early July 2026, treated as a credible incident from around 22 July, publicly confirmed and customers notified from 28 July.
Scale	Origin has approximately 4.8 million customers and has not itself confirmed how many were affected.
Data types	Name, address, date of birth, contact phone number, account information, last four digits of a credit card or last three digits of a bank account.
Nature of the attack	Data theft rather than destruction or disruption. No evidence reported of systems being encrypted or services interrupted.
Who is investigating	The Australian Cyber Security Centre, the National Office of Cyber Security, the Australian Federal Police and the Office of the Australian Information Commissioner.
Unusual feature	The claimant contacted media directly and later reportedly agreed not to leak the data after some arrangement with Origin, something Origin has not confirmed.

■ Also worth knowing

Approach	What it looks like	What it is after
The bank fraud call	"We've stopped a suspicious transaction on the card ending 4417. I need to verify some details."	One-time codes, online banking credentials, or a "transfer to a safe account".
The energy account text	An SMS about an overdue bill or a refund owed, with a link to a convincing payment page.	Card details entered voluntarily, or credentials reused elsewhere.
The supplier invoice change	An email or call to your accounts team saying a supplier's bank details have changed.	A single large payment redirected. The most costly attack on Australian small business, consistently.
The executive impersonation	A call or voice message that sounds like a director, urgently requesting a payment or a gift-card purchase.	Immediate transfer, exploiting hierarchy and urgency together.
The IT help desk call	"We're resetting MFA across the business, I'll need the code that just arrived."	Account takeover, then everything downstream of it.
The slow build	Several harmless-seeming contacts over weeks, establishing familiarity before any request.	The high-value target that a single cold call would never land.

Treat "the data will not be leaked" as irrelevant to your planning

Even where a claimant says data will not be published, nobody can verify that a copy does not exist, has not been shared, or will not surface in eighteen months. Data that has left an organisation should be assumed to be in circulation permanently. Plan for the fraud attempts, not for the reassurance.

■ Questions the full guide answers

- ☐ What happened in the Origin Energy data breach?
- ☐ Why is this breach considered more dangerous than earlier ones?
- ☐ How has AI changed the risk from stolen data?
- ☐ What should a small business do this week?
- ☐ What is the one rule that stops most phone-based fraud?
- ☐ What are our legal obligations if our own business is breached?
- ☐ Should we tell customers we will never ask for certain things?

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 881 662** or visit **unidenvoice.com/get-started**.