SECURITY · AFTER THE BREACH

The RingCentral Breach and Your Phones

Contact data for about 1.6 million records, taken in July 2026. The breach is contained. The scam calls that use the data are what comes next.

In July 2026 the extortion group ShinyHunters talked its way into RingCentral and took names, email addresses, phone numbers and street addresses. RingCentral disclosed it on 28 July, said the phone platform was not affected, and refused to pay. Have I Been Pwned verified **1.6 million unique email addresses** on 13 August after the group published a 280GB archive.

What we know

- Social engineering, July 2026.
- Four data types: name, email, phone, address.
- Platform not affected, per RingCentral.
- No ransom paid.

What we do not

- The exact entry method.
- Which system held the data.
- The forensic findings.
- How many records are Australian.

Why contact data is enough

Most scam calls claiming to be your telco fail because the caller is guessing. **This list removes the guess,** supplies correct details that make the caller sound genuine, and comes with a real news story to explain the call. Many help desks still verify identity with exactly these details, so it also helps criminals pose as you.

How this group works

In 2025 it phoned staff as IT support and talked them into approving a fake Salesforce data tool. **Qantas lost data on about 5.7 million customers that way.** From late 2025 it relayed single sign-on logins through fake pages while staying on the line. More than a hundred organisations were targeted by January 2026. The best tool it has is a confident voice with accurate details.

Optus Loop customers

Nothing published says Optus Loop customers were affected. But **a business mid-migration expects emails about new logins from two companies at once,** which is exactly where a fake blends in. Act only on instructions you can trace to a number or portal you used before the migration began.

Four scripts to expect, and the response

Script	The response
Security re-verification. "Read back the code I just sent."	Never read a code to someone who called you. Ring the number on your invoice.
Help desk re-enrolment. "Sign in on this page while I stay on the line."	IT never reads you a login page. Hang up and call IT on the known number.
Billing change. "We have moved banks after the incident."	Confirm bank changes by phone on a number you already had.
Number transfer. "Please confirm your transfer code."	Port lock on business mobiles. An unrequested code is an attack in progress.

A one week plan, about four hours in total

1. **Monday.** Write the callback rule and share it with everyone.
2. **Tuesday.** Five minute briefing on the four scripts. Nobody is in trouble for hanging up.
3. **Wednesday.** Phone system audit: admin accounts, forwarding rules, international barring, alerts.
4. **Thursday.** Passkeys or hardware keys on admin accounts. Block staff approving new apps alone.
5. **Friday.** Carrier port lock on mobiles. Check emails on haveibeenpwned.com. Note what you checked.

Their breach can become your breach

Under the Notifiable Data Breaches scheme, a covered business whose personal information is involved must notify affected people and the OAIC, and must assess a suspected breach within **30 days**. A supplier's notice does not automatically cover you. Confirm who is notifying, and hold less personal information in the first place.