# ACCAN welcomes new mobile-porting regulation

The Australian Communications Consumer Action Network (ACCAN) welcomes the Minister for Communications, Cyber Safety and the Arts' announced changes to the regulation of mobile-porting in Australia's telco sector.

Fraudulent mobile number porting happens when a scammer uses consumers' personal details to port their mobile number from one provider to another.

As Australia's voice for phone and internet consumers, ACCAN has heard countless stories of the harm that fraudulent mobile number porting can cause.

"Our mobile phones are essential to so much of our daily lives now. If your mobile phone number is fraudulently ported, you're vulnerable to financial loss from scammers, negative credit ratings, and of course the emotional stress that accompanies these issues," explained ACCAN CEO, Teresa Corbin.

"This is an issue that we have been highlighting to the telco industry for quite some time now; it's positive to see that action is finally being taken to safeguard consumers."

"The Minister's announcement today of new industry-wide identification measures, such as two-factor authentication, is a key step towards ensuring that Australians are protected against would-be scammers."

ACCAN looks forward to the future findings of the Australian Communications and Media Authority's Scam Technology Project.

"We congratulate the Morrison Government for recognising the negative impact that telecommunications scams have on Australians. We look forward to continuing to engage with Minister Fletcher, the ACMA, and the telco industry to ensure that consumer-based outcomes remain at the heart of the conversation."

-   **ENDS -**

## How to tell your number has been ported

- A sign that your number has been ported is that your phone will show 'SOS only' where the reception bars usually appear.

## What to do if you have been scammed

- Contact your mobile provider. They will be able to tell you whether your number has been ported. If it has been ported by a scammer, ask them to port it back.
- Contact your bank to see whether scammers have accessed your bank account. Let your bank know of any fraudulent transactions straight away.
- Change your passwords on your online accounts for social media, banking, emails and other important accounts.
- Scammers may try to steal personal information from your close contacts using your accounts. It is a good idea to let your family and close friends know to watch out for strange emails and messages sent from your account if you have been scammed.
- Report the scam to Scamwatch and the Australian Cybercrime Online Reporting Network (ACORN).
- For help with identity fraud, you can contact IDCare.