THE HON PAUL FLETCHER MP

Minister for Communications, Cyber Safety and the Arts

MEDIA RELEASE

2 December 2020

Detecting, tracing and blocking scam calls

The Morrison Government is taking actions to detect, trace and block scam calls, today unveiling a new industry code that will help put a stop to the calls.

Scam calls are a serious problem, and can have damaging financial consequences for victims. Australians have lost nearly $36 million to scam calls in 2020.

Minister for Communications, Cyber Safety and the Arts, the Hon Paul Fletcher MP, welcomed the Reducing Scam Calls Code, which has been developed by the telco industry and has today been registered by the Australian Communications and Media Authority (ACMA).

The Code sets out the processes for telcos to identify, trace and block scam calls.

Over the course of 2020, the Scam Telecommunications Action Taskforce, comprising representatives from the telecommunications industry, government and the communications regulator, has been focused on tackling three scams – the Australian Taxation Office (ATO) scam, 'Wangiri' scam calls and international scam calls:

1. **ATO scam:** In this scam, Australians were receiving calls which appeared to come from a legitimate phone number used by the ATO – this is calling "overstamping" or "spoofing". In the 12 months to October 2019, the ATO received over 160,000 reports of scams involving spoofed numbers – an average of more than 10,000 per month. Telcos used software to identify calls using ATO numbers and block them.
2. **Wangiri scam calls:** 'Wangiri' is Japanese for "one ring and drop'" Victims receive a missed call, often from an international number. When they call back, the call is charged at a premium rate. The 'Reducing Scam Calls Code requires the telco industry to monitor, trace and block Wangiri call scams.
3. **International scam calls:** Evidence suggests that the majority of scam traffic originates from overseas. The Reducing Scam Calls Code requires the telco industry to monitor, trace and work with international carriers to block international call scams.

Telcos are already taking action to stop scammers, and have blocked more than 30 million scam calls over the past year.

"The Morrison Government is serious about tackling scam calls," Minister Fletcher said.

"The Reducing Scam Calls Code will work alongside the other measures we have announced to tackle scams, including the new industry standard I announced earlier this year to stamp out fraudulent mobile number porting."

For more information about what the Government is doing to prevent scams, go to https://www.acma.gov.au/scams-and-online-misinformation.

Media contact:

Imre Salusinszky | 0432 535 737 | Imre.Salusinszky@communications.gov.au

Background

Combatting Scams: Action plan

On 27 November 2019, Minister Fletcher signed-off on the ACMA's *Combating Scams Action Plan* to crack down on scams perpetrated over phone networks. Industry, government and ACMA have been working to deliver on the action plan.

The plan had three actions:

1. Establish a Scam taskforce to provide oversight of telecommunications scam minimisation strategies.
2. Three scam prevention measures: blocking calls using fraudulently 'overstamped' numbers; identifying and blocking 'Wangiri' calls; and deterring networks from carrying scam traffic.
3. Develop enforceable obligations requiring telcos to protect their customers from scams, including to: identify illegitimate use of calling line identification; block scam traffic; refer scammers to authorities; and provide advice to consumers.

Fraudulent Mobile Number Porting

On 16 October 2019, Minister Fletcher announced a measure to stop scammers hijacking peoples' mobile phone numbers in order to steal money from their accounts. ACMA was formally directed to make an industry standard mandating stronger identity verification processes before mobile numbers can be transferred between providers.

Scammers take advantage of number porting rules (which allow people to keep their number when changing providers) to steal a victim's mobile phone number and then get around verification processes (e.g. authorising bank transfers using verification codes sent by text message to the fraudulently ported number). The industry standard commenced on 30 April 2020.