Pivotel Satellite Pty Limited Response to

INDUSTRY CODE DR C661:2022 REDUCING SCAM CALLS and SCAM SMs

Pivotel Satellite Pty Limited ("**Pivotel**") appreciates the opportunity to respond specifically to the options presented in clauses 4.2.1(e) and 5.2.1(e) of the Code.

Pivotel strongly believes the drafting presented as *Option 2* in both cases reflects long standing industry practice in the use of numbers, recognises consumer choice in how they consume telecommunications services, supports service innovation across the telecommunications industry, and enables carriers and carriage service providers ("**C/CSPs**") to build reliable and resilient network connectivity.

It is Pivotel's view that *Option 1* will cause considerable disruption to legitimate call and SM traffic and use cases currently existing in the market, while having almost no impact in reducing Scam traffic. We understand there are some concerns regarding interception, blocking and traceback when consumers are given a choice of C/CSP to use to originate calls and SM with the numbers for which they hold the rights of use ("**ROU**"). However, we do not believe there are material hurdles preventing these obligations being met, admittedly in some cases with extra effort from industry participants.

There are many reasons why a ROU holder may seek to use a number for services other than those provided by the C/CSP who issued the number to them. A common example seen today is ROU holders, particularly small to medium businesses ("**SMBs**") using the number associated with their mobile carriage service to message or call their customers, clients, suppliers etc. using an application-to-person ("**A2P**") platform or service, more generally a 'communication application', provided by a C/CSP other than the C/CSP who issued the number to them. This allows ROU holders to receive responses to messages or calls they've originated through a communication application, directly to their mobile phone, greatly simplifying these increasingly important interactions.

Option 1 would deny ROU holders the ability to use numbers for this purpose and greatly restrict their choice of the hundreds of C/CSPs providing communication applications to address niche end user needs and business cases. This severely restricts consumer choice, and acts to dampen industry innovation.

Many CSPs today rely on call termination services ("**CTS**") as a means of sending outbound traffic from their network. These CSPs have designed their network around the CTS products they typically acquire from multiple other C/CSPs. In so doing, they benefit from the resilience of having multiple call paths for calls to enter and exit their network, and they are not reliant on a single C/CSP to provide them with connectivity to the PSTN. A CSP may have numbers allocated from multiple C/CSPs. CTS products are designed to be used between C/CSPs to transit traffic to the PSTN. The Originating CSP is responsible for ensuring the A-Party CLI is valid.

Option 1 would require Carriers to block calls from their own number ranges entering their network, causing a portion of calls from transit C/CSPs providing CTS to fail. They will have no mechanism to send those calls to the Terminating Carrier when the Terminating Carrier is the holder of the A-Party CLI.

This breaks a very significant call model currently supported in the market, and will result in many legitimate calls being blocked. This is likely to lead to high customer complaints and dissatisfaction, and a material disruption to any-to-any connectivity.

Pivotel does not believe the restrictions imposed by *Option 1* are necessary for C/CSPs to meet their obligations when required to intercept, block and/or traceback. None of these functions are dependent on restricting the use of a number to a service provided by the C/CSP who issued that number.

Adopting *Option 2* will not change the obligation for the C/CSP who issued the number to the ROU holder, to keep the IPND database up to date with an accurate record of the person to whom the number has been issued.

Outbound calls and SMs originated by a ROU holder on a C/CSPs network can always be traced back from the terminating network to the originating C/CSP from which the call or SM was originated. For target numbers originating calls and SMs, this mechanism allows law enforcement agencies ("**LEA**") with the support of industry to traceback and identify the C/CSP from which calls and SMs are being originated.

Inbound calls and SMs terminated to a target number will always be routed back to the C/CSP who issued the number to the ROU holder.

Once the originating C/CSP has been identified, when necessary, LEAs can request interception warrants for both the originating C/CSP and the C/CSP who issued the number to the target ROU holder.

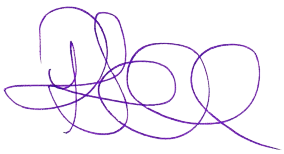
Data retention obligations apply to all C/CSPs and adopting *Option 2* does not affect the obligation of a C/CSP to retain data.

In Pivotel's strong view, adopting *Option 1* for clauses 4.2.1(e) and 5.2.1(e) will have a minimal impact in reducing scam traffic, whilst having a very significant, disruptive impact on legitimate traffic and use cases which have long been in operation throughout the industry.

The use of *Option 1* will result in Australian business' communication processes being severely disrupted and their choice of communication applications and services drastically reduced. This raises significant competition issues that should be considered by the ACCC, as the restriction in use of numbers in this manner is most likely to not be in the long-term interests of end users.

The use of *Option 2* avoids breaking established communication practices, without weakening the Scam mitigation protocols present in the respective clauses and elsewhere throughout the Code. We strongly support Option 2 being adopted for clauses 4.2.1(e) and 5.2.1(e) in the Code.

Yours sincerely



Robert Sakker
Executive Director