AMTA

Australian Mobile Telecommunications Association

COMMUNICATIONS ALLIANCE LTD

www.commsalliance.com.au

ACMA – Combating scams. A discussion paper on technological solutions

submission by:

Australian Mobile Telecommunications Association

and

Communications Alliance

17 May 2019

Introduction

The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance (Associations) welcome the opportunity to provide this submission in response to the ACMA discussion paper on technological solutions to combating scams (the Discussion Paper).

Industry takes scam communications and fraud very seriously and is keen to work with government and regulators to combat these issues. Industry believes that any measures put in place should be via an industry-led approach with the cooperation of government and regulators where necessary.

The Associations have already engaged with industry members to discuss potential solutions which could be put in place to combat scams and fraud. A working group has commenced discussions to investigate ways for industry to better cooperate to identify and disrupt scam calls. In addition, whilst out of scope for this Discussion Paper, it is worth noting that industry is currently engaged in two projects to combat the incidence and consequences of ID theft and mobile number fraud: one projects aims at the implementation of a pre-port verification solution while a second project (in cooperation with Jersey Telecom and the banking sector) has developed and implemented a post-port banking solution. The latter is designed to assist with minimising the detriment arising from ID theft in combination with porting fraud.

Associations

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

Combating Scams

As highlighted in the Discussion Paper, the communications environment is highly dynamic. For the majority of consumers, telecommunications services have become an integral part of their daily lives. For many of these consumers this constantly evolving environment can be an exciting world to navigate. For others, this environment may be overwhelming and complicated, paving the way for scammers to exploit unknowing and vulnerable consumers.

Scams in general cost Australians a significant amount of money. The ACCC reported that total losses from scams in 2018 were $489 million, a $149 million increase on the previous year[1]. With many scams being conducted through the use of telecommunications networks, the telecommunications industry is determined to be part of the solution. Industry believes that while there is scope for technical responses, it is unlikely these technical responses will provide a ‘silver bullet’. Instead, a combination of activities will be required. This will include strong consumer education campaigns and improved cooperation and information sharing amongst industry to track the source of scam calls., Where scammers can be identified, we note the efforts being made by law enforcement agencies[2] to target scammers and recognise the inherent difficulties faced by agencies in this work. We further note that the technological solutions that industry can assist with will necessarily be part of a concerted approach, involving law enforcement agencies and regulators to effectively make an impact on scams with strong enforcement action.

Raising consumer awareness

Raising consumer awareness about scams and how best to avoid them is clearly a priority and many service providers, therefore, offer information about scams on their websites to assist their customers. Some service providers also offer additional online and call centre support areas for those customers affected by scam communications. We strongly believe that building consumer awareness is an area where government and regulators can assist by engaging in regular awareness campaigns to educate consumers on where up to date scam information can be found, what to do or not do, and how to report instances they may come across.

We do note, however, that not all consumers are easily able to access the various online awareness tools available. Some consumers, who may also be the most vulnerable to being targeted by scams, are also those who do not make use of apps or social media or may have difficulty discerning which online information they should trust.

We therefore believe that there is great potential for industry, consumer groups, regulators and government to work together to improve consumer awareness campaigns and develop a consistent and targeted approach to reach all consumers.

Technical and operations responses to prevent scams

When it comes to addressing scam communications at a network operator level, there is no single, simple solution to the problem. In the past, Australia has collaborated with New Zealand on the development of a guideline to address fraudulent communications and international revenue share fraud. We have since seen the NZ Telecommunications Forum (TCF) release the Code for Scam Calling Prevention, with a heavy focus on industry cooperation, rather than additional regulatory measures.

[1] ACCC, Targeting Scams, April 2019

[2] https://www.brisbanetimes.com.au/national/queensland/taiwanese-phone-scammers-sent-packing-from-brisbane-airport-20190514-p51n6o.html

Industry is working to identify ways as to how network operators can improve the way they monitor, identify and react to scam calls. As an initial step, we have begun development of a draft guidance note targeted at consumers about how to protect themselves from scams. At the same time, an industry guidance document is being developed, similar to the NZ Code, on how network operators can cooperate, share and attempt to minimise the incidence of scam calls being transmitted over their networks. The difficulty with this approach is that as soon as a network operator blocks an A-number identified as being used in scam calls, the scammer moves to a new number. Blocking numbers will only temporarily disrupt the scammer. Other approaches are also required.

Network operators also recognise the value of improving the accuracy of Calling Line Identification (CLI) information, providing customers with effective screening mechanisms and monitoring network traffic for suspicious calls. Some members have measures in place to identify potential scam calls based on common characteristics such as a high volume of calls from a single CLI or A-number, high volumes of short duration calls, or missing or incorrect CLI's. There are difficulties associated with distinguishing scam calls from legitimate outbound calls, but with proposed improvements to CLI quality and cooperation in the sharing of information on scam calls this task may be made easier.

Many of these scam communications are generated internationally and may pass through multiple carriers, so it is also important to attempt to block these as closely as possible to the international gateways.

In relation to SMS and email spam, most large providers use commercially available spam filtering products on their networks. Many of these allow end users and network providers to flag messages as spam/phishing, thereby building up their knowledge base on potentially problematic messages and enhancing their filtering capabilities.

In the development of the industry guidance document, international initiatives in addition to those in New Zealand have also been discussed. Some of these, such as the STIR/SHAKEN solution used in the US, may prove difficult to implement in Australia due to Australia's combination of IP based and legacy networks. Further investigation and scoping would be required to fully understand how such solutions would work, what impacts they may have on current systems and whether they are suitable as an industry-wide solution. As with many types of scams and fraud, fraudsters are quite agile and are able to quickly take advantage of areas of vulnerability, especially where not all providers have the same level of protections.

The level of sophistication and agility now seen with scammers and fraudsters is one of the key issues faced by industry. Their key motivation is to make a profit as quickly as possible, so they are very adept at keeping track of what technological solutions industry is putting in place and how to exploit these if possible. While measures such as blocking certain A-numbers will temporarily disrupt scammers, industry highlights the need for strong enforcement activity where scammers are identified. This is an area where regulatory intervention may be beneficial. As mentioned above, potential scam calls need to be investigated to ensure they are actually scam communications, and network operators ought to cooperate more closely and share information, particularly with respect to the tracing of scam calls and blocking of A-numbers. However, in order to be effective, once industry identifies scam calls and traces their origins, regulators are required to take prompt and appropriate enforcement action to create a strong disincentive for fraudsters to (re)engage in such activity by moving to new numbers from which to commit the fraud.

Regulators and consumer protection agencies can also engage in this process through the circulation of up to date information on new or re-trending scams and consumer complaint information.

Multiple reporting platforms makes it difficult for consumers to report scams and we believe that a regulator driven capture point would assist in the effective sharing of the captured information with network operators.

An additional measure, which requires further investigation to assess its feasibility, is the creation of a centralised tool for customers to report suspect numbers, with an aim for the reported numbers to be validated (to ensure it is not a legitimate number) and blocked.

Conclusion

The Associations look forward to further engaging with the ACMA and other stakeholders on this important issue and to assist with the increased protection of Australian consumers.

The Associations also note the current MTAS declaration review being undertaken by the ACCC. Some members lend their support to a reform of MTAS and feel that such reform may assist reducing SMS-related scams. We note, however, that the need for reform and its potential impact on SMS scams is not shared by all members.