## Cover sheet for response to an Ofcom consultation

### BASIC DETAILS

Consultation title: CLI Authentication

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s): Magrathea Telecommunications Ltd

Address (if not received by email):

### CONFIDENTIALITY

What do you want Ofcom to keep confidential?

| | | | |
|---|---|---|---|
| Nothing | X | Name/contact details/job title | |
| Whole response | | Organisation | |
| Part of the response | | If there is no separate annex, which parts? | |

If you want part of your response, your name or your organisation to be confidential, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

### DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response. It can be published in full on Ofcom's website, unless otherwise specified on this cover sheet, and I authorise Ofcom to make use of the information in this response to meet its legal requirements. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here. ☐

Name T. Wright Signed (if hard copy)

Magrathea Telecommunications Limited,
5 Commerce Park, Brunel Road, Theale,
Berkshire RG7 4AB

0345 004 0040 info@magrathea-telecom.co.uk

20th June 2023

**Response to "CLI Authentication: a potential approach to detecting and blocking spoofed numbers"**

Magrathea welcomes the opportunity to respond to this consultation which forms part of Ofcom's work to tackle scam and nuisance calls. We are already an active participant in the NICC CLI Task Group and have engaged with Ofcom, ICO and Trading Standards regularly to discuss this area of work.

We note that this consultation is in fact a 'call for inputs' and makes no specific suggestions at this stage. Our response is prepared on that basis and our thoughts would require further examination at some future point when a consultation is issued. Our comments are made with the intention of enhancing debate and discussion and do not form our final opinions on this topic beyond any specific views expressed based on knowledge or evidence we have available at the time of writing.

We appreciate that Ofcom have taken this step to examine the proportionality of introducing such a considerable change to how telephone calls are processed in the UK and consider the exercise to be very valuable to the industry to discover the potential benefits, costs and challenges that any such changes could bring.

We also appreciate that Ofcom specifically recognise within the consultation that there is a difference between nuisance calls and scam calls. We have advocated that the two cannot necessarily be managed in the same way, nor indeed should they be. Particularly when, in our experience, many nuisance calls complaints are vexatious or have in fact been fully consented marketing calls.

And similarly, to see an understanding of 'spoofing' within the consultation is refreshing and welcome. This is a very common problem we contend with and is one with which various parties, not least the public, often have trouble understanding.

**Response to consultation questions**

Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

Ofcom's analysis appears to fit our understanding of the issues.

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

This is not a simple question to answer. We believe that proper implementation (and monitoring of that implementation) of existing rules and measures is likely to help reduce scam calls, the full impact that can be made has not yet been measured or assessed.

As an industry we have only very recently been obligated to block calls from outside the UK where they carry a UK network CLI. Not enough time has passed to be able to say if this has made an impact or not but clearly the analysis that brought about that change of regulation, combined with feedback from early adopters, appears to suggest this will be the case.

Similarly, the updated guidance around improved due diligence, blocking calls with CLIs on the DNO list and clarifying how to identify suspicious calls was only quite recently published with impact yet to be fully assessed.

We also believe that the introduction of surcharging calls to UK numbers, which was brought in quite suddenly in 2021, has had the effect of 'cleaning up' CLI generally. It is our understanding that surcharging is still not consistently and effectively applied across the industry so it may be difficult to determine the positive impact this has had but some analysis here could be interesting. Magrathea would still welcome industry best practice guidance on implementation to help deliver a more consistent result, again with a general positive impact on how CLI is used.

It is also worth noting that the proposed changes to the Data Protection and Digital Information Bill are not yet in force but are expected to assist in this area through greater awareness and guidance to report 'bad actors'.

The above points relate to calls using any kind of CLI, spoofed or genuine, however we do agree that more needs to be done to tackle number spoofing itself.

Historically it has been very rare for terminating providers to trace the source of calls on receipt of a complaint from their customer. This means it is seldom the call originator in these cases that is held accountable. Instead, the complaints are targeted at the range holder who, in the case of spoofing, will have no influence over calls or those making them.

There is currently nothing a range holder can do to protect themselves from the reputational damage or heavy support burden brought on by number spoofing therefore Magrathea are very supportive of Ofcom exploring solutions in more depth.

Currently the only reliable data available to networks or service providers in order to validate if a number is either their own internal allocation data, known only to them, or the Ofcom list of allocated numbers. Of course, checking the CLI is the correct length and format and appears on the Ofcom list are all basic checks that all networks should be doing. However, what we absolutely cannot do is verify if a number is active and allocated to an end user – and therefore likely to be used as a legitimate CLI.

In the case of a transit network like ours we cannot rely on our own allocation details as we do not originate the call, we must rely on the contractual obligation on the call originator to generate calls that comply with the regulations, but we have no realistic way of verifying that they are doing so. A common numbering database with details of which numbers are in available for use and which service provider has the rights to originate calls using that number as CLI would be of great benefit.

In the interests of transparency, it is worth noting that Magrathea take the Chair and Co-Vice Chair seats at the NICC Common Numbering Database Task Group and believe that the introducing of a CDB has a wide variety of benefits and use cases including CLI authentication, number portability and efficient call routing. It is our opinion that the use cases combined should give sufficient benefit to make the cost of implementation worthwhile. Please refer to our 2019 response on this topic.[1]

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?

Whilst the scheme has some merit which was also reported on by NICC, there are some fundamental differences to what was designed into STIR for its initial US market.

For example, the system is designed to sign the P-Asserted-ID header which in the US market is actually the display number and so fulfils its direct purpose. In the UK, we would actually be signing the network number. The presentation number, which is the actual number the customer sees, would not benefit from signing explicitly and so no direct protection is achieved.

Of course, the system allows the signing to specify that other caller ID fields were supplied as well and thus provide indirect authentication, but it is likely that a significant number of calls would end up being passed with only partial attestation and therefore a reduced level of benefit.

In addition, it is important to consider the amount of support available for this system in commonly available products in the market. This still is very low, especially in the smaller network end of the market which would make participation harder for those networks which tend to drive innovation.

Finally of course we need to consider both the cost and the mechanism for operation of this feature. Given that so far the UK industry has not yet managed to produce a workable central number database solution which would have significantly greater benefits, we should be mindful of where efforts are placed.

Regardless, when you take into consideration the early feedback from the USA, and the fact other countries don't yet have enough data to support one way or another, there is little evidence to show this will actually achieve the primary objective and support it being prioritised.

Consideration should be given to the value chain in the UK and ensure that implementing CLI authentication in the ways suggested does not provide an advantage to any particular type of provider. For example, if the major vertically integrated networks are by nature able to offer greater trust in authenticated CLIs (because they hold end user data) this could create a bias towards particular providers who have greater chance of having calls connected. In addition, there is a wide and varied selection of technical competencies and budget constraints across the sector which could, if the requirement is too onerous, see some providers having to exit the market.

Another critical consideration is that of what do users actually want. The current suggestions have us blocking calls by default before they reach the consumer, however it is our view that consumers may wish to make the choice for themselves.

For example, some businesses may prefer to suffer the occasional nuisance or scam call in return for removing the risk of blocking legitimate calls that have not been able to be fully attested for some reason. These matters require wide consultation.

And finally, we have concerns with the suggestion that industry should self-govern compliance. Apart from the additional burden, we would need to establish the level of evidence required to suggest non-compliance and if it is by fault or design, also needing sufficient protections against vexatious or spurious claims. Considerable reputational damage could be inflicted if this is not handled judiciously. It would certainly be our view that an independent and experienced governance structure be put in place if we proceed with this as a solution.

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.

Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?

In our experience scams and unwanted calls are often perpetrated on legitimately assigned and correctly used CLIs as often as they use spoofed numbers, as a result all those calls would likely continue to reach the called party as they do today.

It is our current view that adherence to existing rules and guidelines, combined with a more proactive approach to monitoring traffic and using data to inform best practice would have a sizeable impact on the primary objective. It is our opinion that the introduction of a common numbering database (CDB) would go a long way to improving what tools we can use in this regard and, combined with general improvements in data management should

bring about some improvements in how we, as an industry, manage bad actors and share information.

Magrathea is also championing a new initiative, raised in February this year with the ICO, whereby carrier networks could utilise Telephone Preference Service (TPS) data to retrospectively monitor service provider traffic, enabling rapid investigation of potential bad behaviour. Again, not something that will solve the problems by itself, but would be another tool in the box of things that would help give more control to industry to manage this problem.

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?

The approach seems reasonable and should result in easier call tracing, however there is the risk that the balance between restricting calls to prevent scam and nuisances and allowing genuine calls to pass could be difficult. Within the consultation Ofcom acknowledge that we need to "balance the need to connect legitimate calls with the need to close loopholes".

The idea proposed here is for blocking calls to be the default but there are likely to be cases of genuine issues, for example, if a network has a transient technical problems preventing attestation, in theory all calls should be blocked. However, the suggestion here is to allow a 'gateway attestation' in these cases which potentially will undermine the benefits of proper CLI authentication.

It is our view that the biggest challenge to trace the origin of scam calls and spoofed CLI is one of resource (and sometimes, willingness) rather than any significant technical constraint and therefore this proposal will only be better and easier if backed up by appropriate regulatory intervention.

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?

It would be entirely unrealistic to consider implementing CLI authentication as proposed here any sooner than the stage that the vast majority of calls are working via the SIP

protocol, otherwise too many exceptions will be in place allowing for loopholes and confusion.

Additionally, as an industry we are currently undergoing a considerable number of changes and demands on our resources (e.g., GPL Switching, TSR implementation etc) so it is crucial to allow time for these changes to bed-in and plenty of time to plan and implement the new requirements. The current One Touch Switching project should be a good indicator of how long it takes for industry to make changes and something of this size will need very careful planning and testing to be sure no legitimate calls are lost and end users impacted negatively as well as allowing industry sufficient time to budget and plan for the changes to their networks.

If a common numbering database were to be implemented – something we are supportive of, as mentioned above – there are several steps to be carried out. Perhaps the most time consuming and complex being data integrity. It is widely accepted that many networks have inaccurate records, particularly when it comes to ported numbers, so a period of data-clashing and correction to ensure the integrity of the data would be essential and a prerequisite for a useful database.

As for the specification, considerable effort has already been made by the NICC CDB Task Group so we are confident that with direction from Ofcom this can be turned into a useful starting point to establish a solution.

Realistically we would imagine 2028 as the earliest the full CLI authentication solution proposed could be expected to be in place when you consider that consultation is expected to commence in 2024 and is likely to require multiple iterations to capture the final set of requirements. However, once a plan is defined the procurement process for CDB and the vast data integrity project could get underway quite quickly.

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.

It is of course true that there is a cost to us all to manage nuisance and scam calls, not to mention the losses felt through the actual scams themselves. But we suspect the greater cost over time is the lack of trust in phone calls. Giving the public confidence to answer calls will, in our opinion, take a combination of technical improvements, awareness, education and penalties for bad actors.

If we set aside for the moment nuisance calls, which are by definition a nuisance rather than illegal. The greater problem as noted in the consultation is high profile scams that result in trauma and loss, and this is where existing regulations and access to better data could make a real impact.

**Summary and conclusion**

We note that in para 4.30 the mention of possibly consulting on restricting calls from overseas using a UK presentation CLI. As noted in previous consultation, this would impact many legitimate business models that have been in operation for years and whilst of course all options should be properly explored we would like it noted that this is a change that has wide ranging impact and must have full and proper consultation.

We are in favour of consulting on CLI authentication and, should the costs be proportionate to the problem it can solve, we would be supportive. However, our support is on the basis that a reasonable amount of time and a proper governance structure be in place to make this drastic change. The demand on service providers, networks and industry generally to implement and manage must not be underestimated.

We must learn from the experience of One Touch Switching implementation and accept that industry led initiatives are complex, costly and management intense.

Similarly, we are in favour of a common number database, regardless of the plans for a STIR/SHAKEN style implementation. We feel the benefits in a whole range of areas will pass the cost/benefit analysis when viewed altogether. Something we would be happy to discuss in more detail if Ofcom should require it.

And finally, we feel monitoring for compliance of existing and recently introduced rules will go a long way towards reducing nuisance and scam calls and it would be proportionate to properly assess this before we can fully assess the possible impact of any other solutions.

We remain available to discuss any of these points further if Ofcom should wish to do so.

Yours faithfully,

Tracey Wright
Magrathea Telecommunications Ltd

[1] https://niccstandards.org.uk/wp-content/uploads/2019/03/ND1522V1.1.1.pdf

[2] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/154407/magrathea.pdf