CALLING LINE IDENTIFICATION AUTHENTICATION: A POTENTIAL APPROACH TO DETECTING AND BLOCKING SPOOFED NUMBERS

INTRODUCTION

1. Sure (Guernsey) Limited, Sure (Jersey) Limited, and Sure (Isle of Man) Limited (together "Sure") are pleased to respond to Ofcom's consultation regarding its proposals for calling line (CLI) identification authentication in the UK. We are grateful to Ofcom for actively considering the impact that its proposals could have on Crown Dependency operators and welcome its decision to proactively engage with the operators[1].

2. We are responding to Ofcom's consultation to express our preference for how Sure, and specifically Sure's calls to and from the Channel Islands and Isle of Man, are treated under Ofcom's proposed CLI authentication regime. Our preference is for Sure to be a member of any future CLI Authentication Administrator, and to be involved in the development of CLI authentication for UK calls to the extent that its technically and economically feasible for Sure as a small operator (Option 1[2]). We support Ofcom's assessment that more could be done to prevent scam and nuisance calls and we agree that the Crown Dependencies should not act as a loophole for such calls to enter the UK network. However, we believe that any requirements imposed on Sure (or any other Crown Dependency operator) under membership of the Administration must be proportionate to Sure's size and scale; we should not be punished for being smaller and more resource constrained than our UK counterparts.

3. In the Annex below, we have provided a fuller explanation for why Sure's preference is to voluntarily join the CLI Authentication Administrator. Additionally, and as requested by Ofcom, we have provided brief responses to the questions set out in the consultation document where

[1] On Tuesday 20 June, Ofcom hosted a meeting with licenced operators from Guernsey, Jersey, and the Isle of Man to present more information on its consultation proposals and respond to any questions.

[2] Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers – paragraph 5.51(a) – page 48.

we believe our input could be useful. As always, we remain ready to engage with Ofcom on these issues and can provide further information as and where required.

ANNEX

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.

Yes, we broadly agree with Ofcom's analysis regarding the ways in which number spoofing is used, both legitimate and illegitimate, and the types of harm associated with its use. Like consumers in the UK, consumers in Guernsey, Jersey, and the Isle of Man ("CIIM") continue to be subject to scam and nuisance calls, albeit we believe on a less frequent basis than the research cited by Ofcom. We take our responsibility to protect our customers and island communities from CLI and telephone-based fraud very seriously. Where a Sure customer is the recipient of a scam or nuisance call, they are encouraged to report this to Sure via our call centre or by using an online form. Sure then investigates each and every report received and either blocks the originating number (usually for a finite period of time) and/or advises the customer of action they can take to prevent scam or nuisance calls from being received (such as blocking calls on their mobile handset). A review of our interactions with customers over the last 12 months suggests that [✂]:

- [✂];
- [✂];
- [✂];
- [✂]; and
- [✂].

In some of the cases reviewed between January and July 2023, we found that [✂]. We therefore agree that a solution that prevents such calls from reaching the customer, whatever the mechanism, is best placed to truly protect customers.

We believe that Ofcom's analysis should also consider the impact of scam and unwanted calls on small businesses. Whilst Ofcom's research primarily looks at calling behaviours and impact assessments for individual consumers that are victims of telephone-based fraud, our experience is that small business customers across CIIM continue to be targets for telephone-based fraud and misuse of CLI data as well. Furthermore, we believe that the risks for small businesses can, in some circumstances, be greater due to their inclination to answer incoming calls for which they do not recognise the CLI in order to do business.

As an example, [✂].

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.

Yes, we agree that more can and should be done to tackle number spoofing and prevent scam and nuisance calls from reaching the customer.

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

We believe that Ofcom’s proposed approach to CLI authentication, to the extent that it is a high-level framework, is both feasible and workable. We have shared and discussed Ofcom’s proposed approach with our mobile, fixed, and signalling firewall vendors and all have agreed that, [✂][3]. Similarly, our fixed network vendor stated that [✂]. However, due to the high-level nature of Ofcom’s proposals, our vendors have not yet been able to provide indicative costs and further discussion will be required to fully understand how CLI authentication will work in practice, [✂]. We look forward to engaging with Ofcom and industry in more detailed discussion on this issue.

As a Crown Dependency operator, we agree with Ofcom that permitting calls from the Channel Islands and Isle of Man without attestation could create a loophole that could be exploited by scammers and nuisance callers. We also do not wish to see calls from CIIM customers blocked due to inadequate authentication or information about CIIM callers. As a result, our preference is to be involved in the development and delivery of Ofcom’s proposed CLI authentication mechanism, and, where possible, be a voluntary member of the CLI Authentication Administrator (subject to technical and economic viability).

We do not believe that it will be necessary for the GCRA[4], JCRA[5] and CURA[6] to mandate membership to the CLI Authentication Administrator because Crown Dependency operators will already have the requisite incentive to engage with the Administrator and ensure that calls appropriately attested and authenticated. Crown Dependency operators are net outbound callers to the UK, with a large quantity of outbound calls made from the Channel Islands and Isle of Man to UK fixed and mobile numbers each day. [✂]. These allowances, which CIIM customers value, would potentially be blocked by UK terminating operators if they have not been appropriately attested and authenticated, resulting in significant customer dissatisfaction. Any Crown Dependency operator that finds a proportion of its calls blocked by UK terminating operators could find themselves at a competitive disadvantage, which would have obvious financial and reputational implications.

However, whilst we are keen to ensure that our calls are appropriately attested, it is important that any scheme involving the Crown Dependency operators is technically and economically feasible given the size and scale of those operators. As Ofcom will be aware, the Crown Dependency operators are significantly smaller than their UK counterparts, with fewer resources available to adopt new processes, or pay for and implement new systems[7]. It may not be technically or economically feasible for Crown Dependency operators to adopt and implement all of the features and functionality desired by Ofcom or the CLI Authentication Administrator, and it may take us longer to achieve a given level of compliance. In voluntarily engaging with this process, we expect that any future requirement to attest and authenticate calls would be proportionate and achievable, with derogations provided to smaller operators where possible and appropriate.

In addition to the above, we have several comments or requests for clarification.

Ofcom states that the role of the originating provider is “to attest each and every call originated on their network” and then pass this “across the public telephone network as a completed attestation passport”[8]. Ofcom also explains that the originating provider must satisfy itself that the calling customer can legitimately use the associated presentation number. However, the consultation does not fully explain what an originating operator should do in the event that a calling customer on its network attempts to make a call with an illegitimate presentation CLI. Should the originating network simply prevent the call from being initiated (i.e. block the call at the point of call setup – something we do using SystemX at the

[3] [✂]
[4] Guernsey Competition and Regulatory Authority - About Us | GCRA
[5] Jersey Competition and Regulatory Authority - About Us | JCRA
[6] Communications and Utilities Regulatory Authority - About Us (cura.im)
[7] For example, [✂].
[8] Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers – paragraph 5.21 – page 42.

moment) or should the call be permitted with an attestation passport that makes clear that the presentation number is being illegitimately used (which could then be blocked by the terminating operator)? We would be grateful if Ofcom would clarify its expectations for such a scenario.

Regarding gateway attestation, Ofcom states that 'gateway providers who introduce harmful calls from outside the UK would be reported to the CLI Authentication Administrator, and subsequently to Ofcom'[9]. The clear suggestion is that some kind of action would be taken against gateway providers who introduce potentially scam or nuisance calls from overseas[10]. However, as acknowledged by Ofcom, the gateway provider will not normally be able to attest the presentation CLI being used and may be unable to authenticate the network number. Under Ofcom's proposals, the gateway provider is simply providing gateway attestation – confirmation of who gateway provider is and, where possible, the provider from whom the gateway provider received the call – it is not making any warranty as to the legitimacy of the presentation number or validity of the network number (both outside of the gateway providers control). It is therefore unclear why instances of a gateway provider introducing potentially harmful calls into the UK would need to be reported to Ofcom (and potential enforcement action initiated). In our view, a more appropriate expectation, which could be written into guidance for participating operators, would be for instances of harmful calls to be reported to the relevant gateway provider, and for that provider to use their commercial relationships with their interconnect partners to prevent instances of scam or nuisance calls from being sent to the UK.

Finally, we believe that calls to the emergency services should be fully exempt from the CLI authentication process. That is, calls to the emergency services should not require any authentication information to be applied and should simply be passed to the emergency services call handler as per today. Whilst we welcome Ofcom's clarification that operators should not block or impair calls to the emergency services that don't have the requisite authentication information, we remain concerned that the authentication service or certification authority, however constructed in practice, may act as a single point of failure during call setup and thus prevent a call to the emergency services from initiating.

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.

No comments at this time.

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

No comments at this time.

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?

We support Ofcom's proposed approach to monitoring and enforcement and agree that non-UK providers that do not comply with the Administrator's rules should be suspended or excluded from membership.

[9] Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers – paragraph 5.46 – page 47.

[10] All other references to the CLI Authentication Administrator reporting matters to Ofcom relate to possible enforcement action.

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?

Whilst we broadly agree that CLI authentication could make the task of call tracing (that is, working back from the terminating operator to identify the true originator of the call) and identification of those performing scam or nuisance calls easier in some circumstances, it will not address all of the difficulties associated with call tracing.

As explained in response to Question 3.1, CIIM customers have been and continue to be subject to scam or nuisance calls from UK mobile numbers. Where these UK mobile numbers are allocated to end-users and used for an unregistered pre-paid account, it will be difficult, if not impossible, to identify the party that is using that pre-paid SIM to make scam or nuisance calls. Whilst the originating operator will be able to identify the account responsible for these calls and terminate it, enforcement agencies will still find it difficult to identify the identity of the party responsible, and those perpetuating the scam or nuisance calls could simply move their activities to different pre-paid numbers.

Originating and terminating operators will continue to have data retention policies for call records, which are informed by our data protection obligations and storage capacity. As a result, enforcement will still need to make requests for call records in a timely manner in order to be successful, and this issue will not be resolved by CLI authentication being applied to calls. Furthermore, overseas providers that fall outside of the jurisdiction of the UK's enforcement agencies may still ignore or take time to respond to tracing requests.

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

Yes, we support Ofcom's proposal not to introduce CLI authentication until after the end of 2025 and agree that it would be overly complex and costly to introduce some form of CLI authentication on legacy networks. [✂].

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

Yes, we generally agree with the proposed implementation tasks set out in Ofcom's consultation document. However, we have some concerns about the apparent casualness with which Ofcom refers to "the establishment of the CLI Authentication Administrator"[11] by telecoms providers. As Ofcom will be aware from the formation of The One Touch Switching Company ("TOTS Co"), establishing a body to develop and administer a process for industry is a significant undertaking that requires a lot of time and industry engagement (including from Ofcom). Time must be allowed for industry to negotiate and agree the body's objects and Articles of Association, agree funding streams (which may include loans from participating members), establish corporate bank accounts, appoint a board, and hire staff to fulfil the functions of the Administrator. Only once these administrative tasks have been achieved can the Administrator (with the support of industry) proceed to develop and deliver the technical functionality

[11] Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers – paragraph 7.5(b) – page 58.

needed to facilitate for CLI authentication. In our view, industry must not be set up to fail because insufficient time was provided to establish an Administrator.

We believe that the formation of the Administrator alone will take at least 12 months. A further window would then be needed to actually develop and deliver the requisite functionality between the Administrator and members, which could be significantly in excess of 12 months depending on the level of complexity and cost associated with delivery. As a result, agreement on the mechanism for how the Administrator will be established (either via an industry collaboration or outsourced third party) and by whom should be reached in the early stages of this process so that the aforementioned administrative tasks can be completed while IP networks are being deployed.

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?

Whilst we support the concept of a common numbering database, there is currently insufficient information to be able to make an informed decision about how feasible it will be to design and implement.

However, we do have two high-level concerns. Firstly, as recognised by Ofcom, developing a common numbering database that provides accurate information about the status of specific telephone numbers is a significant undertaking. It is unlikely that UK or Crown Dependency operators will have sufficient resource to be able to deliver a CLI authentication process and common numbering database in tandem. We therefore suggest that Ofcom stagger development and deployment of these two systems, prioritising the development of the CLI authentication process before seeing how it can be complemented by the use of a common numbering database.

Secondly, we are concerned about the frequency with which this common numbering database would need to be updated by operators, and in particular Crown Dependency operators. In the Isle of Man, Sure and MT have a fully automated and near instant mobile switching process, which is dramatically faster than most markets, 24-hour delays can take place due to some manual steps being required. A similarly quick process is in place in Guernsey and Jersey for pay-as-you-go, where we enable customers to port their number in-store in under five minutes. Given this very quick switching process, there will be a need for Crown Dependency operators, and in particular Sure and MT in the Isle of Man, to update the common numbering database in almost real-time to reflect the fact that a subscriber could have ported from one operator to another. Failing to do so could result in a new Sure customer (that has ported from MT) being unable to make calls to UK numbers because the common numbering database has not yet updated to reflect the fact that the customer has switched/ported. This is a problem unique to the Channel Islands and Isle of Man as switching in the UK ordinarily takes between one and two working days.

Finally, we have concerns about how regularly such a database would need to be interrogated and, as a result, the extent to which querying such a database would introduce extra latency into the call setup. However, we recognise that this can be dealt with once more detailed discussions about the common numbering database have started.

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.

No comments at this time.