JT's Non-Confidential Response to Ofcom Calling Line Identification (CLI) authentication Consultation

30 June 2023

1. Introduction

JT (Jersey) Limited and JT (Guernsey) Limited ("**JT**")welcomes the opportunity to respond to the Ofcom's Consultation: CLI authentication a potential approach to detecting and blocking spoofed numbers (the **"Consultation**"). We have several comments on the Consultation which we address below in answer to the questions posed. This is a non-confidential response and can be published in full.

2. JT's 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.

JT would agree with OFCOMs views on the ways of spoofing and the extent of the harm associated with this.

However, JT would question whether the harms invoked through spoofing are inherent with the user trusting apparent 'enterprise' numbers which are predominantly in the 'fixed' numbering space, and whether the same risk is as inherent from mobile CLI.

Whilst JT concede that voice based scam calls continue to pose a threat to users, JT do not agree with the apparent downplay of alternative scam mechanisms, particularly SMS (3.68), as the threat of SMS based scams is clearly outlined in the UK Governments Fraud Strategy: Stopping Scams and Protecting the Public 2023, and is something that JT have seen on an increasing basis. With the relevant ease to spoof an SMS number or alphanumeric ID, and the ability to include phishing links in the SMS content, JT could see that this mechanism could overtake call based scams, especially given the restrictions already imposed with the existing May 2023 CLI changes.

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.

JT would agree that further measures to tackle number spoofing could be considered.

However, JT are also aware that measures recently introduced by OFCOM, and closely aligned with the

Finnish and German (and other jurisdiction) approaches of blocking inbound calls to the UK with UK +44 CLI have only recently been implemented, and the positive effects of this are yet to be understood.

JT also consider that the current loophole of Mobile numbers being excluded from this screening could be reduced through a look-up to validate whether the caller is roaming (though JT would highlight that such look-ups themselves could be perceived by some networks to be abuse). This option may prove simpler to implement than STIR/SHAKEN, and may not be reliant on the move to SIP for all providers.

As such, whilst STIR/SHAKEN may provide some improvements, this still leaves potential gaps (roaming mobile), and is predicated on the concept that the spoofed numbers are largely being generated from within the UK.

JT also agree with some of the earlier respondents (4.77-4.79) that more can be done to ensure existing measures are adhered to, and that clarity / guidance / central registration of services such as Type 1, 3, 4 and 5 which could remain open to abuse even if STIR/SHAKEN were to be implemented.

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

JT believe that the introduction of STIR with a central Authentication Administrator is a workable solution, though would likely require significant development of existing telecom infrastructure to support this. Whilst many networks have transitioned to SIP, many SIP equipment providers have not (or do not) support the STIR standards.

With regards section 5.51

a) JT believe that opening access to the UK CLI Authentication Administrator would not only satisfy the requirements of the Crown Dependencies, but would also facilitate some of the other problematic use cases where calls are potentially originating from outside of the UK, including non-UK based call centres.

   Consideration should be given to the proposed mechanisms outlined in section 6 and how these could be extended to ensure potential transgressions are raised to the local regulatory authorities.

   Furthermore, due consideration may be required on the nature of connectivity to the CLI Authentication Administrator to ensure that the remote nature of the Crown Dependencies is considered (especially where this is being used between local operators), or even consideration of local deployment capabilities.

b) Whilst technically viable, JT believe Option B could be problematic, putting the onus on a limited

number of UK providers to provide a bespoke service for the Crown Dependencies and potentially creating a monopoly, or imposing increased termination costs to cover the attestation services.

c) JT question the technical viability of this option given the challenges identified by UK operators to the original OFCOM 2022 guidance.

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.

5.27-5.31 outline that the obligation is on the originating provider to validate the CLI (as is the case today). JT question, given existing measures already taken to limit the origination of Fixed CLI calls to the UK, whether the introduction of STIR will make a significant improvement, or whether the originating providers will continue to allow incorrectly validated calls to be originated.

5.30 & 5.46 indicates that the validity of calls would be 'policed' by the customers of the terminating provider, and that customer complaints could trigger the terminating provider to raise complaints to the originator/gateway. Whilst JT appreciate that STIR would improve validation of the originating network, JT would be concerned that the customer complaints would be based on their assumption that the 'caller seemed like a scam', rather than having any validated complaint. Furthermore, it is unlikely that the customer would be making a complaint that the CLI was invalid or misused (especially in the case of an international number).

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

Section 5.40 – Whilst it is generally accepted that 2G and 3G circuit switched roaming calls 'break out' in the roamed network and are routed back to the UK, as outlined, mechanisms to check (either dynamic query or via database) whether a user is roaming should be viable. Alternatively, there could be options (e.g. using CAMEL) to home-route roamed calls back to the home network where the CLI could be validated before passing on. Furthermore, whilst home-routing is common on 4G / VoLTE calls, this is not the universal option, and some networks may adopt Local Break Out as VoLTE roaming becomes more prevalent.

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?

Section 6.2 highlights a potential challenge with some calls potentially not being attested. It is JT's view that there needs to be a very clear (binary) position, else it would become impractical for terminating providers to appropriately implement blocking.

JT question to some extent the role of the Administrator in infringements, and would see this more as an escalation path in the event that the Terminating provider is unable to get the Originating provider to make suitable changes after notification. JT do agree that the Administrator would play a role in consolidating repeat incidents of non-compliance, and where necessary may have the ability to impose measures for repeat offences to ensure the provider is compliant with their membership terms, or escalate with evidence as required to OFCOM or an alternative regulatory or enforcement body.

With regards 6.18, JT believe that 'voluntary members' would apply to corporate entities outside of the UK who may have been allocated or sub-allocated numbers to support their business activities (such as call centres etc) and wish to have the CLI attested so that a UK CLI can be appropriately used for their business. JT do not believe that it is valid to consider the Crown Dependencies as 'non-UK providers', nor falling under the category of 'voluntary members'. We do not agree that the Administrator would have the authority to 'suspend or expel' Crown Dependency providers as whilst taking the grave nature of serious contravention in mind, could be materially damaging to our subscribers and the Crown Dependencies themselves. Instead, JT would propose that the Administrator should establish a similar reporting regime with the Crown Dependency regulatory bodies such that these bodies can take equivalent actions to OFCOM within the Crown Dependencies.

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?

JT believe that CLI authentication would make tracing easier and more timely, and as such should improve notification to the Originating provider in a timely manner to take appropriate action. However, the detection of scammers and nuisance callers would still be largely reliant on end-customers correctly identifying and reporting calls, which itself could be open to false negative reports.

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

With regards the assumptions in 7.3, JT would broadly agree that attempting to implement gateways or other such systems to interwork legacy networks that are due to be retired in the short term would not be beneficial. However, JT would highlight that IP based networks (or more specifically SIP based networks) have been established for a long time whilst the STIR/SHAKEN standards were only finalised in 2018/19. As such, there will be many existing UK SIP based networks that may not be able to support the STIR/SHAKEN standards, or where significant network upgrades would be required to support such standards.

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

JT broadly agree with the outlined steps, but would like further consideration for inclusion of the Crown Dependency regulators and operators to ensure appropriate access and inclusion.

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?

As outlined, the Common Numbering Database is another significant piece of work. In JT's view, this should be considered separately to the implementation of STIR/SHAKEN, and could be used to further enrich / validate the CLI information at a later point.

With regards part 'a' of the question, JT would observe concerns that the scope of the Common Numbering Database has been significantly expanded by many contributory stakeholders to the point that there is a risk that it may not achieve a cohesive agreement to a specification, or (in relation to part 'b' of the question) the specification would not be feasible to deliver using standard technologies and protocols.

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.

With regard 8.10, Due to consumer scepticism of scam calls (even where the CLI and the caller are genuine) scammers and fraudsters are already actively transitioning to alternative solutions such as OTT and SMS. JT believe that if mitigations are put in place on the CLI of phone calls, the scammers and fraudsters will be well positioned to exploit these alternative services (where in some cases it may be even easier to impersonate a business, or entice a user to perform an act in an automated manner without requiring voice callers). Many of the exploits would continue to rely on the 'caller identity' being presented through the OTT application (which may be a phone number), or SMS. It should also be noted that whilst the industry may be able to differentiate between the CLI used on a Fixed / Mobile call, vs an SMS or an OTT app, many end-users are unable to differentiate this technical distinction (especially in the case of making / receiving calls through an OTT app which may be associated with an E.164 caller identity). JT question the legitimacy of excluding the caller identity of these services from the overall consideration, though do acknowledge that the measures outlined (notably STIR/SHAKEN) are largely used for voice calls. JT also acknowledge OFCOMs intent to pick up these risks through alternative projects.