JT's Non-Confidential Response to JCRA Call for Information – Calling Line Identity

24th September 2021

1. Introduction

JT (Jersey) Limited, (“JT”) is pleased to respond to this Call for Information (“CFI”) on Calling Line Identity (“CLI”) facilities. This is a non-confidential response and can be published in full.

CLI provides call recipients with the telephone number of the number calling and allows the call recipient to identify the person or organisation calling them, and to make informed decisions about how to handle incoming calls. JT welcomes the opportunity to respond to this CFI and recognises the importance of CLI in providing consumers with some protection against telephone-based fraud, allowing consumers to make informed decisions on whether to answer or reject a call.

2. JT's Response to Consultation Questions

Question 1: Do you have any comments on the Authority's plan to review, clarify and establish expectations for the use of CLI facilities in Jersey?

CLI information presented with a call can provide assurance to the recipient of the identity of the caller, allowing them to make informed decisions on how to handle incoming calls. However, the passage of CLI information can be vulnerable to misuse, for example the insertion of false information to intentionally mislead the recipient of the call as to the identity of the caller.

Invalid, malformed or illegitimate CLI can at best be confusing to users, or could prevent the user from establishing a return call. At worst, such CLI can be used for fraudulent purposes, either to establish return calls to high revenue numbers[1], or to pose as legitimate organisations with the intent of defrauding the user.

The technology available to inject a false CLI into a network is not expensive or complex, and can be a simple customer PBX (either incorrectly or maliciously configured). It is the obligation of the originating, transit and terminating network providers (where technically possible) to validate the CLI and ensure that a valid, dialable telephone number which uniquely identifies the caller, is provided.

Furthermore, users have privacy rights which allow them to block the transmission of their CLI if desired. Network operators are required to ensure that the CLI itself can be passed on accurately and that the privacy choices made by end users about their CLI data are respected by all network operators involved in the origination, transmission and termination of that call.

The UK and other jurisdictions are taking steps in establishing guidelines and obligations on network operators to mitigate misuse of CLI, and ensure users privacy is upheld. JT welcomes the JCRA's plan to review, clarify and establish expectations for the use of CLI facilities in Jersey. JT believes that the JCRA should first look at Ofcom's guidelines on CLI facilities[2] which can then be adapted to the local context.

Whilst much industry guidance focuses on the fraudulent risks posed by CLI related to calls, more recent attention has also been attributed to fraudulent use of SMS (so call 'smishing') where SMS are sent to users with invalid sender identity with the aims of defrauding the user.

[1] Referred to as Wangiri calls

[2] Guidance on the provision of Calling Line Identification facilities and other related services (ofcom.org.uk)

Groups such as the Mobile Ecosystem Forum (MEF) are working to establish databases of registered identities to facilitate operators in blocking unauthorised use. More information can be found on the web links:- https://mobileecosystemforum.com/sms-senderid-protection-registry/ and https://eandt.theiet.org/content/articles/2021/09/smishing-and-spoofing-targeted-for-eradication-by-sms-protection-registry/

Therefore, JT would also suggest that the scope of this review includes SMS. SMS based fraud has seen a significant increase in recent years, however it may be vastly more complex to police based on spoofed sender ID / Alpha numeric sender ID.

Since the COVID-19 pandemic, JT has seen a significant increase in the volume of fraudulent calls directed to both fixed and mobile subscribers. Whilst we have had reports of customers being targeted by Wangiri calls, we are predominantly seeing reports of the following scenarios coming into our network:

- The CLI presents as a UK fixed or mobile number, often with only one call coming into the network from each CLI (cycling through numbers);
- The CLI presents as a Jersey mobile number very similar to the B-number being called (a mobile);
- Calls from legitimate callers who are returning a call they received with a Jersey CLI that had in fact been spoofed.

We rarely receive reports of fraudulent calls coming from DNO numbers. Now that many UK operators have DNO blocking in place, it may be that fraudsters have moved away from this approach.

Question 2: Do you agree the Authority should consider amending operator licences to include conditions covering the provision of CLI facilities?

JT agree that the JCRA should look at amending operator licences to include conditions covering the provision of CLI facilities and should follow the requirements in place in the UK under the General Conditions of Entitlement[3]. In addition, the Communications Act 2003 gives Ofcom the powers to take enforcement action against misuse of Electronic Communications Networks or Services. We consider that is appropriate and that the JCRA should put in place the same requirements to protect consumers in Jersey as are in place in the UK.

Question 3: Do you have any comments on the importance or otherwise of protecting islanders from telephone-based fraud as far as practically possible?

JT considers it has a duty to protect islanders from telephone-based fraud as far as practically possible and continuously works to minimise the impact on islanders. JT encourages customers to report potential fraudulent calls and has a dedicated reporting area on its website[4]. JT then reviews each report and blocks the originating number and shares where appropriate. If a customer reports that their number has been spoofed and the return call attempts to their number becomes disruptive, we provide the option of blocking inbound calls for a period of time (usually only a few days).

JT is an active participant in the Jersey Fraud Prevention Forum (JFPF)[5], collaborating with the States of Jersey Police and other local operators. The JFPF provides consumers with information on how to identify fraud and what to do if a consumer suspects that they have fallen victim to a scam.

JT collaborates with other industry groups (such as the GSMA fraud forum and the Mobile Ecosystem Forum) on the techniques that operators around the world are employing to protect consumers. It is widely recognised within these groups that educating consumers on how to recognise fraudulent calls is one of the best ways to minimise the impact. This is because fraudsters are continuously shifting their approach when using CLI.

Some recent examples of fraudulent CLIs presented are:- standard UK geographic numbers, UK mobile numbers and Jersey mobile numbers. More often than not, on investigation, we are only seeing one call come into our network from each originating number which is a shift from prior to 2020 where we would see a flood

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/112692/Consolidated-General-Conditions.pdf
[4] Contact Us (jtglobal.com)
[5] www.fraudprevention.je

of calls into the network from one originating number.

Smishing has become a much more widely discussed topic in telecoms fraud over the past 18-24 months with operators across the globe sharing information and collaborating on detective and preventative measures in an effort to keep up with and get ahead of the fraudsters. In Jersey we are seeing much the same activity as in other countries, not only in terms of spam SMS (purporting to be from HMRC, a bank or the government) but there is also evidence that islanders have had their devices infected with Flubot or similar malware.

The Flubot scam is a text-message scam that infects Android phones. An SMS, pretending to be from a number of services, including voicemail or a courier, asks users to click an attached link and install an app which is actually a piece of malware. If a user installs the app, the malware takes over the device and sends more infected SMSs to the user's contacts or other mobile numbers. We would be happy to provide further information on this should this be required.

Question 4: Do you agree the Authority should pursue introducing a centralised CLI-fraud mitigation system

Ofcom, has introduced a centralised system for blocking telephone numbers potentially associated with fraudulent activity. Whilst blocking a list of do not originate (DNO) numbers can only be beneficial, based on the customer reports of fraudulent calls we receive, it would not have a significant impact in terms of reducing the volume of fraudulent calls. However, JT would be keen to get involved in the existing Ofcom DNO initiative and would be supportive of the JCRA exploring how Jersey operators could get involved in the scheme. It would be useful to understand more details regarding how the scheme works and the frequency of updates.

Channel Island operators are in a relatively unique position, due to them being part of the UK numbering scheme with dedicated number blocks and with close collaboration between them. It may be possible to establish a CI 'perimeter' whereby calls coming into the islands form a non-CI provider with a local CLI (indicating that this has been originated from outside of the Islands) could be assumed to be fraudulent and blocked in transit (this approach is broadly adopted in other jurisdictions such as Australia). Exceptions could be handled by the establishment of a central registry to ensure operators legitimately 'whitelist numbers' could be passed.

Furthermore, similar to procedures established in other jurisdictions (such as Australia), the sharing of reported fraudulent CLI numbers between operators to apply temporary blocks could be established.

Additional comments

In the absence of any Jersey specific CLI guidelines, JT has looked to the Ofcom guidelines[6] for direction and take our obligations of screening and establishing the validity of CLI seriously.

Presentation Numbers (Type 1 – 5)

JT currently follow Ofcom guidelines for Type 1 and Type 2 presentation numbers. The Ofcom description for Type 1 and Type 2 is included below:-

> *Type 1*
>
> *A Presentation Number is generated by the subscriber's network provider. The number is stored in the network and applied to an outgoing call at the originating node in the public network by the provider. Because the number is applied by network equipment there is no need for it to be verified each time a call is made – instead the level of authenticity will depend on the checks made by a network provider that a subscriber is entitled to use a particular Presentation Number.*
>
> *Type 2*
>
> *A Presentation Number which identifies a caller's extension number behind a DDI switchboard. Although the number or partial number is generated by the user's own equipment, the network provider is able to check that it falls within the range and length allocated to a particular subscriber. In this way the authenticity of the number may be ensured. It should be noted that some network providers classify Type 2 Presentation Numbers as network numbers (especially where the full number is constituted at the local exchange). This type of number is considered to carry sufficient authenticity to be classified as a network number and is carried as such by some networks.*

[6] Statement annex 2: Guidance on the provision of Calling Line Identification facilities and other related services (ofcom.org.uk)

JT currently do not provide Type 3 – 5 presentation numbers as a service but we believe that other operators in Jersey do. Type 3 is described in the Ofcom guidelines as:

> *Type 3*
> *A Presentation Number limited to the far-end break out scenario where a call's ingress to the public network may be geographically remote from where it was originated. The number is generated by the user's equipment and is not capable of being subjected to network verification procedures. Verification is based on a contract between the subscriber and the network provider in which the subscriber gives an undertaking that only authentic presentation numbers will be generated.*

To give context to Type 3, we describe a use case that JT has seen in Jersey. 'Network Provider A' (for example JT) has a number allocated to it by Ofcom which it provides to a 'Subscriber' for a service. The 'Subscriber' is also taking a service from 'Network Provider B' (for example Newtel) who contracts with another network provider 'Network Provider C' (for example Gamma). In this scenario the CLI is 01534 88XXXX (JT allocated number range). Type 3 presentation allows the subscriber to request that their outgoing CLI for calls via 'Network Provider B/C' uses the number for the service which they are taking from 'Network Provider A' (JT in this scenario). Therefore in the outlined scenario, calls would enter the UK PSTN from Gamma with a JT Jersey based CLI.

Ofcom CLI guidance states that Type 3 can be done under "*contract between the subscriber and the network provider in which the subscriber gives an undertaking that only authentic presentation numbers will be generated".* JT currently has no formal process in place to support Type 3 and would like the JCRA to look into specific guidance for this.

JT believe that clarity is required from the JCRA, in the following areas:

- To ensure the CLI is a "valid, dialable telephone number", the contract should be between the two network providers and the subscriber, such that if the subscriber ceases the service with network provider A, or has their service terminated, the network provider A must notify network provider B that the number is no longer a 'valid, dialable telephone number'.
- To facilitate lawful intercept requests, there should be a contract between the two network providers and the subscriber, such that if a lawful intercept request is raised to network provider A against the subscriber's number, network provider A can inform the authorities that network provider B is handling the subscriber's outbound calls.

- Where network provider B is used for the outgoing calls, it should clarified that all inbound calls to the number must continue to terminate on network provider A (i.e. the network provider to which the number block is allocated). This will then ensure that network provider B does not use internal local routing for the number range.
- where network provider B is used for outgoing calls, it should be established that calls to Emergency Services must be correctly terminated to the Jersey Call Handling service – a call to the Jersey Emergency Services which incorrectly enters the PSTN in the UK or other network may have no method of establishing communications to the Jersey Call Handling service.
- where network provider B is an unlicensed provider using an 'over the top' VoIP service, operating under Ofcom guidelines, but outside of the scope of the JCRA. Jersey's position as part of the UK numbering plan can cause confusion (especially to UK providers) who may not be aware of the different licencing regimes in the crown dependencies, and therefore apply UK conditions / guidelines to Jersey number ranges. Under such scenarios, guidelines from the JCRA may not be adhered to, access to the Emergency Services may not be available, and requests for lawful intercept may not be fulfilled.

Type 4 is described in the Ofcom guidelines as:

> *Type 4*
>
> *A Presentation Number available for the onward transmission of the originating number where a call breaks into a private network and breaks out again before termination, as in a DISA17 scenario. On the break out leg the number is generated by the user's equipment although it will have already been verified in consequence of having been delivered to the private network. To maintain the verification it is necessary to ensure that the number submitted by the private network is the number that was received.*
>
> *Network providers wishing to offer a Type 4 service will require a contractual commitment from customers that they will only submit CLIs that have been received from the public network.*

Whilst JT do not provide Type 4 today, we are broadly happy with the contractual obligations around these types of numbers. However, JT would propose that this could be tightened (where technically feasible) to restrict this to diverted calls with appropriate signalling headers, i.e. where the call originates directly from the PBX, this should be screened as normal.

Type 5 is described in the Ofcom guidelines as:

> *Type 5*
>
> *Presentation numbers that identify separate groups of callers behind a private network switch wishing to send different outgoing CLIs. A typical scenario is a call centre making calls on behalf of more than one client. Type 5 Presentation Numbers are generated by the user's equipment. Subscribers will need to enter into a similar contractual commitment with their network providers as for Type 1 Presentation Numbers – that they are entitled to use the numbers they have selected.*

JT believes the same clarity is required for Type 5 as for Type 3, however we recognise that due to the size of Jersey it is unlikely there will be many Jersey use cases that require Type 5 and we are not aware of any requests for this.