Response of Microsoft Corporation to Ofcom's consultation document

"Guidelines for CLI Facilities"

14 November 2017

1. Microsoft and its customers have the potential of being harmed by those engaged in CLI fraud, and thus Microsoft has a strong interest in eliminating those practices. At the same time, Microsoft's Skype product and Skype customers have the potential of being harmed by poorly designed, albeit well-intentioned, efforts to minimize harmful call spoofing. Thus, Microsoft would like to constructively assist in the industry effort to establish rules and practices to combat CLI-related fraud in ways that do not harm legitimate calls, including those made using non-traditional voice technologies such as Skype.

2. Telephone network-based mechanisms alone are unlikely to stop the categories of fraud that utilize CLI spoofing. It used to be that these tech support scams and similar forms of fraud relied upon an initial "cold" telephone call to the victim. However, the fraudsters are now increasingly making their initial contact with victims through a computer screen pop-up identifying a fabricated computer vulnerability and providing a telephone number for the customer to call to resolve this artificial danger. Accordingly, the effort to stop tech support scams and other incidents of CLI fraud warrants a multi-pronged approach which, in addition to network-based approaches such as those raised by the consultation, should include consumer education,[1] technological tools, and active pursuit by law enforcement.[2]

3. It bears emphasis that some forms of CLI spoofing (for lack of a better term) are legitimate and do not cause harm to consumers. Earlier this year, the U.S. Federal Communications Commission, which has similar concerns about consumer protection and CLI fraud, recognized that:

> there are legitimate uses for spoofing, such as a domestic violence shelter seeking to protect victims who make calls, doctors wanting to display their main office number, or call centers calling on behalf of a business displaying that business' main customer service number or a toll-free number for return calls instead of the number for the originating line used by the call center. [3]

---

[1] For example, Microsoft provides these tips for consumers to follow if they receive a notification or call from someone claiming to be from a reputable software company: (1) Be wary of any unsolicited phone call or pop-up message on your device; (2) Microsoft will never proactively reach out to you to provide unsolicited PC or technical support; (3) Any communication Microsoft has with a consumer must be initiated by the consumer; (4) Do not call the number in a pop-up window on your device. Microsoft's error and warning messages never include a phone number; (5) Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer; and (6) If skeptical, take the person's information down and immediately report it to your local authorities.

[2] Microsoft actively supports efforts to prosecute tech support fraud. For example, earlier this year, four fraudsters were arrested after two years of forensic and investigative work by the City of London Police and Microsoft. For more information, please visit: <https://news.microsoft.com/en-gb/2017/06/28/four-arrested-police-work-microsoft-crack-fraudsters/#sm.00017peh8lpttcs2wqj1h88kryeal>.

[3] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 17-24 at ¶ 5 (U.S. FCC, rel. Mar. 23, 2017).

When revising its CLI guidelines and rules, Ofcom should remain cautious of these valid reasons for CLI spoofing and should seek to avoid preventing or unnecessarily burdening them.

QUESTION 1: *What are your views of the use of CLI authentication to improve the accuracy of CLI information presented to an end user, in particular the viability and timeframe for implementation? Are there any issues associated with implementation?*

4. Carriers in some other jurisdictions have supported the blunt mechanism of blocking calls suspected of nefarious CLI spoofing and Ofcom suggests that approach for certain calls.[4] The blunt force approach of blocking illegitimate calls inevitably involves a risk of blocking legitimate calls, thereby reducing the reliability of the public switched telephone network.[5] Accordingly, in lieu of call blocking, Microsoft strongly prefers emphasizing an approach that supplies consumers with information possessed by the network that can attest – or not – to the authenticity of the CLI. Such an approach allows calls to terminate properly, identifies risks for consumers, and allows them to make informed decisions on how to treat incoming calls.

5. CLI authentication must be designed properly to avoid building technological discrimination into the network. Preliminary consumer testing indicates that once consumers begin to understand CLI authentication mechanisms, a call lacking the appropriate degree of authentication or attestation is likely to go unanswered. If the authentication program is designed in a manner that authenticates only certain forms of calls or only calls using certain technologies, then those voice services excluded from the authentication program are likely to suffer in the marketplace. Consumers won't use voice services that result in their calls going unanswered. Given the consequences of CLI authentication mechanisms, their design must account for a variety of calling types and technologies to avoid discriminatory outcomes in the marketplace.

6. The Secure Telephone Identity Revisited (STIR) standard currently under development is promising. The SHAKEN framework is being developed under the ATIS standards body for implementing STIR in the United States. There remains significant work to be done before SHAKEN can be implemented as a reliable authentication method. Without specifying details here, Microsoft has expressed concerns with some elements of the current iteration of the draft standard. Microsoft remains actively involved in ATIS's SHAKEN development

[4] See Consultation document paragraphs 4.18 and 4.19 (requiring CPs to prevent calls from being connected to the called party where the CP considers the CLI provided with the call contains invalid or non-dialable CLI data).

[5] In extreme circumstances, one could conceive of call blocking that could have severe consequences for the safety of life and property. Imagine a child in danger calling a parent for help from an unfamiliar phone only to have their call blocked because it is mistaken as an illegal robocall. The stakes are high when voice providers block calls versus implementing alternative approaches, such as warning their customers that they perceive irregularities, thus putting the customer on notice.

process and is encouraged that others working through ATIS are working with Microsoft to address its concerns.

7. The consultation document indicates that implementation of SHAKEN in the United States is expected to begin at the end of this year, with possible network scale deployment by the end of 2018.[6] In Microsoft's estimation, that expectation is a bit overly ambitious. Microsoft has observed a general albeit informal assumption among many ATIS-SHAKEN participants that network-based implementation is unlikely to occur before 2019.[7]

QUESTION 2: *Do you have any comments on the proposed changes to the CLI guidelines?*

8. Not all outbound calling technologies require the calling party to have a telephone number and the CLI proposal discriminates against (or, at a minimum, does not adequately account for) those technologies. The consultation document discusses a new proposed condition that CLI displays must be populated with a valid, dialable telephone number that uniquely identifies the caller (barring a caller requesting privacy status). Ofcom should make provisions for technologies and services that do not require a calling party to have a telephone number.

9. For example, paragraph 4.14 states that "[t]he revised [General Conditions] requires that the number that is provided is a dialable telephone number that uniquely identifies the caller. This means that the CLI presented to the recipient of the call should be a number which can be used to make a return or subsequent call, *i.e.* a number that is in service." This requirement does not appear to contemplate one-way outbound calling features that do not assign telephone numbers to calling parties.

10. Unless the customer affirmatively asks to populate their Skype CLI field with their separately purchased Skype Number or their mobile number (which is verified), the CLI fields for outbound Skype calls made to the Public Switched Telephone Network (PSTN) are populated with a number assigned to Skype, but which is not unique to the calling party and does not enable a return call to the calling party. In these circumstances, Skype instructs PATS providers to apply CLI restriction so that the number is not displayed to the called party. This approach is used because the feature allowing Skype calls to landlines and mobile phones is a one-way outbound calling feature and does not include the ability to receive inbound calls.

11. Requiring CLI displays to include a number that could be used to make a return call or that is unique to the calling party discriminates against one-way outbound calling technologies. Accordingly, Ofcom should revise the proposed Guidelines to make it clear that one-way calling offerings may populate the CLI field with a valid dialable telephone number from a

[6] Consultation document at n.9.

[7] Some carriers in the U.S., however, are currently introducing database- and analytics-based CLI displays to indicate when a call is suspected to be a nuisance call and these may work in conjunction with the SHAKEN framework.

number range that has been allocated to the one-way calling provider where it is not technically feasible for a one-way service to provide a telephone number that uniquely identifies the caller or is usable for making a return call to the original calling party. Section 4.9 of the proposed Guidelines already contemplates an originating CP "providing the CLI from a number range that has been allocated to them." By clarifying that providers can associate with VoIP calls a number validly assigned to the provider, the Guidelines can explicitly address compliance with GC6 for one-way offerings while still addressing the need for traceability of a call as a number will be associated with the call that identifies the originating provider, who can provide further information about the subscriber making the call.

12. Paragraph 4.17 states that "CPs may need to run further checks on the CLI where the call appears to come from a source that they should reasonably suspect to carry nuisance traffic. CPs could also demonstrate that only valid CLI data will pass between networks through a contractual agreement with its interconnect partners to guarantee that only valid, dialable CLI that uniquely identifies the caller is provided with any calls that are passed to their network." Affording this level of discretion to CPs, without further guidelines, fails to adequately consider the negative effects that could befall legitimate traffic from providers lacking interconnect or other contractual agreements with CPs or who are identified erroneously as the source of nuisance calls. Advocating this self-help approach could lead to discrimination by CPs against newer or different calling technologies such as those that do not require a telephone number to be associated with the calling party.

13. If CPs are allowed to act on a unilateral "reasonable suspicion" that a calling source is carrying nuisance traffic, they should adhere to and make available upon request objective, valid, and transparent criteria for making such a determination. They also should establish a means of recourse for third parties to challenge or seek modifications of nuisance determinations. Finally, Ofcom or some other designated neutral third-party should remain available to resolve matters that cannot be resolved to the satisfaction of the parties involved. Such measures will help to protect consumers and ensure that traditional and newer technologies can interact in a manner that supports continued reliability of the public switched telephone network.