Vodafone Response to Ofcom Consultation: Reducing scam calls from abroad which spoof UK mobile numbers

Options for addressing consumer harm

1. Introduction

Vodafone welcomes the opportunity to provide input to Ofcom's Call-For-Input (CFI) regarding reducing scam calls from overseas which spoof UK mobile numbers.

We will be fully compliant with Ofcom requirements to block inbound international calls with +44 CLIs (with certain exceptions such as mobile numbers) and are confident that other international gateways will similarly be compliant. This inevitably means that some perpetrators of fraud will seek to circumvent these blocks by portraying themselves as roaming UK mobile customers, presenting a +44 7 CLI for display. At this stage, until the recently mandated blocking is implemented, we do not have evidence as to how great an issue this will be. However, it would be foolhardy to wait until there is evidence before examining mechanisms to prevent this (during which time consumer harm would be occurring), so we agree that options should be considered for refining the exemption of calls with +44 7 CLIs to narrowly allow valid roaming calls. Vodafone has taken an active role in NICC Standards, developing and refining the options that are set out in Ofcom's CFI.

2. Answers to Questions

Question 1:

a) Do you agree with our characterisation of the ways in which mobile calls enter the UK? Please give an explanation for your answer where appropriate.

b) What do you think is the relative importance and / or significance of each of the different routes used for calls to enter the UK? Please provide evidence for your answer.

c) If you provide mobile services to UK consumers, what international gateway provider(s) does your organisation use (including in-house services)? In addition, please explain the nature of the international gateway services you rely on.

For calls that are roaming where the visited network is 2G or 3G technology, we agree with Ofcom's characterisation of how calls from roaming customers enter the UK. However, we would highlight that there will always be a node carrying out international gateway functionality, even if this isn't discrete (e.g. in the scenario that Ofcom sets out in para 3.7 of the CFI of national networks that have bilateral interconnects, the UK node is carrying out international gateway functionality even if the node doesn't have that title).

Part c) of the question asks which international gateways our organisation uses. We believe this misunderstands the nature of how 2G/3G roaming works. When a Vodafone UK customer is roaming overseas and places a call to the UK, (absent home routeing) the choice of how to route the call is made by the visited network, in-line with the choices made for the generality of their customers' traffic. As such, we do not have any direct influence/choice over which international gateway provider is used for inbound calls. Indirectly however, we do have some influence, insofar that Vodafone UK will tend to prioritise roaming to other Vodafone Group networks, and those Vodafone Group networks will tend to use our in-house gateway capability (known as Vodafone Roaming Services). However, once a Vodafone UK customer roams onto a non-Vodafone Group network, how calls are routed to the UK are then out of our control. For outbound calls – not the subject of this CFI – Vodafone UK will always use Vodafone Roaming Services.

For 4G roaming (VoLTE roaming), the control of calls originated by customers roaming overseas remains with the home network (e.g. Vodafone UK), meaning calls back to the UK will ultimately be seen as a media stream that is directed via our network and then towards the terminating network – as such there is no (voice call) leg via an international call gateway. As all valid calls are controlled by the home mobile network and arrive into the UK as a data stream, in a scenario of universal VoLTE roaming, any calls with a +44 7 CLI traversing an international gateway will implicitly be fraudulent and can be blocked.

There is currently a dramatic increase in the level of VoLTE roaming, driven by mobile networks switching off 3G technology, and prioritising usage of 4G over usage of 2G. In August 2024, ✂% of Vodafone's outbound roamer traffic was VoLTE, in comparison to ✂%in August 2023. It should be noted that the selection of whether VoLTE roaming is invoked is not entirely within the control of the home network – we can and do ensure that VoLTE roaming is enabled (we currently have around ✂% of our primary relationships enabled), but whether it is invoked will be driven by the availability of 4G network in a given area of the overseas destination, whether the visited network has enabled VoLTE (including roaming) at specific masts, and terminal choice of network technology layer. This means that the growth set out above is in large part driven by more terminals being able to VoLTE roam, rather than whether there are VoLTE roaming agreements in place. Taking specific countries by way of example, in the same period of August 2023 to 2024, VoLTE roaming has increased from ✂%to ✂% of calls in Italy, ✂% to ✂% in Spain, ✂% to ✂% in Netherlands and ✂% to ✂% in the USA.

At the other extreme, there is clear case of diminishing returns – for example Vodafone UK saw only ✂ of roaming traffic from the Cook Islands over the last year, making the economics of negotiating VoLTE roaming challenging. However, for UK customers roaming in the Cook Islands, those calls would have been important, and it would be an unacceptable outcome for UK mobile operators to have to tell their customers that if they wish to visit smaller destinations, they must either use 3rd-party apps such as Whatsapp! to make calls, or purchase a local SIM card.

Any solution for exempting calls from 2G/3G roamers from blocking at international gateways will therefore be time-bound. This should heavily influence Ofcom's thinking both in terms of whether it is worth implementing *any* solution to better identify 2G/3G roaming calls (versus putting a hard deadline on when the expectation is universal VoLTE roaming), and if a solution is to be deployed, the choice of which is most efficient both in terms of time and cost to deploy.

Question 2: What variables and factors should we take into account when considering whether – and, if so, how - to address the harms caused by spoofed UK mobile numbers?

We believe that the factors that should be taken into account when considering whether, and if so how, to address the harms caused by spoofed UK mobile numbers are as follows:

- The degree of harm caused. Will the increase in calls using spoofed UK mobile numbers materialise when blocking of calls with other numbers is introduced? If so, to what extent? By the time that Ofcom is in a position to make a final decision following this CFI, more evidence should be available;
- The speed at which roaming arrangements are being migrated to VoLTE roaming – driven by the switch-off of 2G/3G networks overseas, hence rendering a more refined gateway blocking solution redundant. We have provided information on the evolution to VoLTE roaming in our answer to Question 1;
- The balance between preventing every potential fraudulent call getting through and inadvertently resulting in valid calls being blocked;
- Whether Ofcom has a hard requirement that any call with a potentially spoofed CLI be blocked, versus accepting that they might get through but with the CLI obfuscated so that the recipient cannot be fooled into thinking the caller is a UK mobile;
- The extent to which a blocking solution might be circumvented by perpetrators of fraud and consequences of their workaround;
- The time to implement a solution (and, conversely, the harm that might occur until it is in place); and
- The cost to implement a solution (spread across UK mobile networks, overseas mobile networks, international gateways and other nodes involved in call paths).

Question 3:

a) What is the scope and scale of consumer harm caused by spoofed UK mobile numbers?

b) What are the consumer impacts of spoofed UK mobile numbers more broadly?

Please provide evidence to support your responses.

Question 4:

a) How significant is the volume of spoofed mobile calls from abroad?

b) Is there any evidence that scammers are moving from spoofing fixed to mobile UK CLI?

We do not have anything additional material in this area. It may be possible to compare the volume of inbound international calls with +44 7 CLIs pre- and post- implementation of the expanded call blockings required in Ofcom's July statement[1], but we note that such data should be treated with caution because:

1. Some international gateway operators have implemented the blocking early, so bad actors may have already evolved to using mobile CLIs;
2. Overall volumes of roaming traffic are in a state of flux post-pandemic and in any case are highly variable on a month-by-month basis; and
3. The split of 2G/3G roaming (which will be seen by gateways) and VoLTE roaming is evolving.

So, for example, Ofcom might compare +44 7 traffic pre- and post- implementation of the July measures and see stable volumes hence conclude that there has been no material evolution to using mobile numbers to perpetrate scams. However, that could be masking that legitimate gateway volumes have diminished as VoLTE roaming increased, with the reduction having been offset by an increase in spoofed CLI traffic. Comparisons are therefore difficult.

Also, anecdotal evidence of frauds perpetrated using calls with a mobile CLI are not, of themselves, evidence of internationally-spoofed mobile CLIs. The call could also have been generated from a mobile phone (e.g. a "burner" PAYG handset), or be a mobile CLI spoofed in a UK network.

It is therefore difficult to secure concrete evidence, rather than supposition.

In principle Ofcom could secure billing information from every UK mobile network for their 2G/3G roamed customers and compare this to the overall volumes experienced at international gateways. However, this would only be possible if billing records were generated for non-billed calls (e.g. inclusive roaming minutes). It would also represent a huge data exercise.

[1] Statement: Tackling scam calls – expecting providers to block more calls with spoofed numbers

Question 6:

a) What is your preferred option for addressing scam calls made from abroad using spoofed UK mobile numbers, and why (including the pros and cons of the different solutions)?

b) Do you think it is possible to identify a solution that could be implemented relatively quickly now, and which would enable implementation of a more robust and effective solution in the future? If yes, what solution fits these criteria? Please give an explanation for your response.

c) What would be the advantages and disadvantages of obtaining more information about, and oversight of, the international gateway providers which bring calls into UK networks, in the context of tackling use of telecommunications networks to facilitate fraud and scams?

Please give an explanation for your response.

All of the options set out by Ofcom are workable in some environments, but each present advantages and disadvantages for the specifics of the UK. We set out our observations below:

Group 1 – proactive checks by the international gateway provider

We would highlight that all of the options in Group 1 present risks of mobile customer privacy being compromised, and of perpetrators of fraud circumventing the blocking to the detriment of legitimate roaming mobile customers.

Inherently, under the Group 1 solutions using a CLI related to a roaming UK mobile customer on a call from overseas would succeed, whereas using a CLI related to a UK mobile customer that was not roaming would either fail, or have its CLI suppressed:

1. This means that by spoofing CLIs, a fraudster can gain information as to whether a particular customer is roaming – this would compromise the mobile customer's privacy.
2. A fraudster wishing to use a spoofed mobile CLI could repeatedly generate calls with random mobile CLIs until one is accepted. They would then be at liberty to generate calls using that spoofed CLI, safe in the knowledge that it would avoid the blocking software. As the number would relate to a legitimate roaming customer, any return calls would then go to that innocent customer, at a time when they are away from home and least able to liaise with their provider to seek assistance. We note that such a brute force attack would not require outlandish volumes of call attempts to obtain a suitable dupe roaming customer CLI – perhaps 1 in 15-20 attempts would work during summer months[2].

Both these issues could be mitigated to some extent by taking a random action on CLI checks being failed (to make it more difficult for perpetrators of fraud to determine that the attempt had failed), but ultimately we believe that fraudsters would be able to determine that a CLI is a valid roamer then exploit this.

[22] ONS data suggests that around 86 million UK citizens travel internationally per year. The peak of these is likely to be during summer months. As a comparison, ✂ of Vodafone's customers roam overseas at least once per year.

An alternative approach might be to carry out two checks – firstly to the home UK mobile network to determine if the customer is roaming, then secondly to the visited network to determine that the valid customer is actually making a call. However, the second check would be technically problematic (it's not just checking a database, rather it's checking whether there is a call establishment in progress) and would require liaison with overseas mobile networks. Although the latter aspect may ultimately be overcome via, for example, the joint venture that has recently been announced by Ericsson and various mobile operators (including Vodafone)[3], that would not fall within the timelines to which Ofcom is operating.

Option 1a – Gateway roaming query (direct)

We believe that this would be a costly exercise as it would require a web of relationships between international gateway providers and mobile networks. We note that there does not appear to be a comprehensive list of gateway providers, and also that in this context "mobile networks" will need to comprise the traditional mobile networks, thick Mobile Virtual Network Operators[4] (MVNOs), and providers of mobile services using non-traditional networks.

To have any hope of success, there would need to be a standardised query/response interface supported by all stakeholders, that would take material time to develop. Within the NICC Standards activity, consideration has been given to using either an API (as is supported e.g. for banking customers to determine the host network for a number), or re-utilising queries such as C7 MAP. Although APIs developed have been suitable for query usage, we do not believe that such APIs support latency requirements appropriate for an in call-setup transaction. Conversely, we have concerns about usage of C7 MAP messaging, particularly for a web of relationships where one of the players may be a bad actor (or acting on their behalf).

As Ofcom rightly highlights in the CFI, the effect of number portability is of particular concern, given that the UK doesn't have a common numbering database. This means that the international gateway would not know which mobile network to query, leaving options of (a) querying the number rangeholder on the basis that they'll either forward on the query to the recipient network or respond with the identity of the recipient network, or (b) parallel querying very mobile network with the aim that one network responds with the authoritative information as to whether the number relates to a roaming customer.

Approach (a) is problematic as it would lead to significant response delays (which would manifest as post dial delay on roamers' calls back to the UK), and would require significant development in our network as the functions which would service such an API are not integrated with number porting information.

Approach (b) would generate large amounts of queries - at least 10-20 queries destined for irrelevant networks for each one destined for the valid home network for the number in question. We can also foresee issues in that it is not uncommon to have data which is redundant in networks (e.g. configuration relating to numbers that have ported away), with generally lies unused but could become harmful in this model. E.g. if a

[3] "Global telecom leaders join forces to redefine the industry with network APIs"

[4] i.e. those with their own core network equipment.

number has been ported from network X to network Y and redundant data has been left in network X, this might usually never be seen, but if an international gateway carries out an is-roaming check, both X and Y might respond that the customer is live, X saying that they're at home and Y saying that they're roaming. Who is the international gateway to believe?

There may also be issues with cleansing/purging of databases in home networks when roamers return to the UK. This may mean that an inadvertent "is roaming" affirmation could be provided when the customer had in fact recently returned to the UK (meaning the number was actually being spoofed).

Regardless of resolving these issues, this option would require development of both international gateways and mobile networks. This would be relatively costly for international gateways, significantly costly for mobile networks (particularly when the porting aspect is considered), and take considerable time.

For the above reasons, although we acknowledge that the option could work where there is a porting database, we do not believe it appropriate for the UK market.

Option 1b – Gateway roaming query (proxy)

Option 1b seeks to mitigate some of the issues of Option 1a requiring a web of relationships between gateways and mobile networks by using one or more proxies/hubs to act as intermediaries. The concept is that international gateways would be shielded from the complexities of interfacing to multiple mobile networks. By taking this approach, the need to standardise a query interface could be reduced, as the proxy could present an interface to the gateway that suits it, and an interface to the mobile network that suits it. Further, potential proxy providers have asserted that they have amassed porting information – we are less than clear how – so could query the correct home mobile network.

We are extremely sceptical of the benefits of this approach. We foresee two sub-options: one where there is an appointed proxy, and one where the proxy function becomes subject to a competitive marketplace. For the appointed option it must be recognised that the UK telecoms industry does not have a great history of coming together to appoint a central agency, agreeing cost-apportionment, and agreeing then implementing the specification of that function – or at least not of doing so on time. For the competitive approach, we would be very wary of there being somewhat of a wild-west with our having to connect (both as a gateway and mobile network) to multiple proxies providing partial connectivity.

In any case, the majority of concerns raised in response to Option1a also apply to Option 1b.

We note that when this option was discussed at length at NICC Standards, pretty much the only stakeholders supporting the model were potential providers of the proxy function.

For the above reasons, we do not believe it appropriate for the UK market.

Option 1c – Gateway roaming query (database)

Option 1c seeks to remove involvement of the home mobile network in real-time call set-up, and instead have international gateways query a database of numbers that are roaming (which would be populated by mobile networks as our customers begin to roam/return to the UK). This would require considerable development both by international gateways, and mobile networks.

As with Option 1a, there would need to be standardisation of interfaces, both from international gateways to the database, and from mobile networks to the database. A process to appoint a database provider would need to be agreed, and a funding model for the database. We note that from a security perspective, a breach on the database could render it impossible for any UK overseas roamer to call to the UK, or at the least would remove the ability to block calls until the incident is resolved. As such, the database would inevitably be a target and would therefore need to be extremely ruggedly engineered.

As with the other "is roaming" check options, there would need to be a mechanism for the database to address number portability – it would need to know which mobile network can authoritatively state that a given number is roaming, but absent an associated porting database this would be complex.

The databases within mobile networks do not readily lend themselves to triggering a message to an external database when it is recognised that a customer is roaming. Although the development to accomplish this could be feasible, the mechanism to similarly notify the database when a customer is no longer roaming would be significantly more complicated. Each of these developments would take time and money.

For the above reasons, we do not believe that this is a viable solution.

Group 2 – "Broad categorisation of incoming calls from abroad by the gateway provider without specific number checks"

(Note that we have used terminology from the CFI – we believe that this mischaracterises the solutions unless modified to read "…without specific number checks by the gateway" as checks are made elsewhere in the call path before a CLI can be displayed).

We note that whereas the options under Group 1 seek to check whether a given mobile number is roaming (hence it's reasonable to expect inbound international calls using the number as a CLI), the options under Group 2 additionally seek to verify that an individual call has actually been generated by the roaming customer involved. The outcome is therefore more sophisticated, and unlike the options in Group 1, those in Group 2 are not vulnerable to fraudsters detecting that a given number is roaming and then spoofing that number to generate fraudulent calls.

Before getting into the detail of the individual options, it is worthwhile noting that all of the solutions rely on Customer Applications for Mobile Enhanced Logic Home Network Routeing (CAMEL HNR). CAMEL HNR is a legacy capability which was developed to facilitate, amongst other things, the support of UK-specific short code access (e.g. voicemail access) and real-time billing of roaming customers. Vodafone has audited its roaming arrangements, and of ✂[5] visited networks, ✂ are capable of supporting CAMEL HNR (with a further ✂ currently being enabled). However, for Vodafone, CAMEL HNR is typically only invoked where required,

[5] Note that this represents the total number of roaming relationships; practically fewer of these will carry material traffic levels.

which is for an extremely small subset of use cases, that being ✂. This is important to note when considering timelines for deployment of the options within Group 2 – we believe that universal deployment and invocation would take a period analogous to that in which 2G/3G roaming will be usurped by VolTE roaming.

All of the options within Group 2 involve the enablement of CAMEL HNR to some degree. This will require significant testing and development in UK mobile networks. Simple enablement of CAMEL HNR is unlikely to be problematic as has been shown where it has been enabled ✂. However, in order to deploy on a more widespread basis, including ✂, we would need to comprehensively check interaction of CAMEL HNR triggers with other IN services. These verifications and developments would need to occur at both a network and IT (e.g. billing) level. ✂

Option 2a – CAMEL HNR (removed CLI)

In this model, calls entering the UK with a +44 7 mobile CLI would have this removed.

- Legitimate calls that are CAMEL HNR would route to the home mobile network, where the CAMEL logic would regularise the signalling, re-inserting the caller's CLI and associated privacy markings.
- Legitimate calls from any visited networks that did not support or invoke CAMEL HNR would route directly to the terminating network, but no CLI would be displayed.
- Fraudulent calls with spoofed mobile CLI would route directly to the terminating network, but no CLI would be displayed. As such, the fraudster's aim of passing themselves off as a UK mobile number would be thwarted.

The mechanism for "removing" the CLI has not been agreed by NICC, but for the purposes of this analysis, we assume that the original CLI is retained in the Network Number CLI (PAID header in SIP signalling), but the Presentation Number CLI (From: header in SIP signalling) is replaced e.g. by a string of spaces, or an agreed alphanumeric digit string (e.g. "International")[6] – this would need to be standardised. When compared to Option 2b, there would also be no impact upon Anonymous Call Reject (ACR) services.

Compared to Option 2d, this option would not require international gateways to have intimate knowledge of the specific temporary numbers[i] that are used to route calls towards home networks in CAMEL HNR, as calls to any UK destination number would be let through. The model is, however, onerous in requiring the gateway to interfere with the contents of CLI fields.

It could be argued that this option is less optimal than one which blocks fraudulent calls, because the calls still get through to the intended victims, albeit with no CLI displayed. We note that Ofcom consequently rejected a similar proposal by 3UK when looking at blocking calls with other UK CLIs[7]. We believe that the

[6] International technical standards do not allow the From: header to be absent – it must be present so the decision is what to populate in the header if the CLI is removed.

[7] Statement: Tackling scam calls – expecting providers to block more calls with spoofed numbers paras 3.12-3.18

problem statement for facilitating roaming is different to the wider call-centre situation that Ofcom was considering at the time, however – the aim of this exercise is to stop fraudsters passing themselves off as roaming mobile customers rather than more widely blocking fraudulent calls. Even if we find a solution that blocks any call with a fraudulent +44 7 mobile CLI, it is still open to fraudsters to send calls with no CLI displayed by simply withholding a foreign CLI.. Further, the intervention that Ofcom proposed in the statement impacted call-centres, who had the opportunity to take measures to avoid legitimate calls being blocked via deploying long-lines into UK networks, whereas in contrast legitimate roaming customers impacted by calls being blocked would have no opportunity to circumvent the blocks. As such we consider that the circumstances are different to those for wider blocking of calls with +44 CLIs, and we do believe that this Option 2a (and Option 2b) meet Ofcom's policy goals.

Whilst having superficial attractions, the issue with Option 2a is that it breaks existing nuisance call provisions. All UK networks are required and configured to reject any call where CLI fields do not contain a valid E.164 number. The technical standards and Ofcom regulations[8] would need to be updated, with consequent changes to every node in every UK network (assuming that it is possible for each equipment vendor to carry out this development). The need for this development would cancel out any early-deployment benefit achieved by not having to universally invoke CAMEL HNR.

For the above reasons, we do not support this solution.

Option 2b – CAMEL HNR (withheld CLI)

In this model, calls entering the UK with a +44 7 mobile CLI would have this marked as withheld/restricted from display.

- Legitimate calls that are CAMEL HNR would route to the home mobile network, where the CAMEL logic would regularise the signalling, re-inserting the caller's CLI privacy markings hence allowing the CLI to be displayed.
- Legitimate calls from any visited networks that did not support/invoke CAMEL HNR would route directly to the terminating network, but no CLI would be displayed.
- Fraudulent calls with spoofed mobile CLI would route directly to the terminating network, but no CLI would be displayed. As such, the fraudster's aim of passing themselves off as a UK mobile number would be thwarted.

The outcome of this approach is that any calls with spoofed CLIs will not have them displayed, rather than the calls being blocked; as we set out in our observations to Option 2a, we believe that this is sufficient to meet Ofcom's policy goals. Similar to Option 2a, .the huge benefit of this approach is that there would be no need to ensure that CAMEL HNR is enabled by every visited network. This would allow early deployment, making it a commercial decision for mobile networks whether to expedite enablement of CAMEL HNR so

[8] We note that this probably at the level of amending the General Condition rather than just the associated CLI Guidance.

that their customers' CLIs are displayed, or to speed up the deployment of VoLTE roaming that would similarly result in CLI display, or to tolerate the service detriment of roaming customers not having CLI displayed. It becomes a commercial decision for mobile networks as to the extent that they enable CAMEL HNR, indeed in the extreme there would be no regulatory requirement to enable it at all (we draw Ofcom's attention to our comments on diminishing returns in response to Question 1).

As with Option 2a, this option would not require international gateways to have intimate knowledge of the specific temporary numbers[ii] that are used to route calls towards home networks in CAMEL HNR, as calls to any UK destination would be let through. Some gateway development would be needed to mark CLIs as withheld, but we consider it to be moderate (and has already been achieved in other countries[9]).

No development would be needed to any other UK networks, as all signalling would be as currently standardised.

There is a philosophical issue with this option in that CLIs are marked as withheld by the network, when the usual practice is that a withheld CLI is always at the behest of the caller. There is a school of thought that CLI privacy markings are sacrosanct and should not be interfered with by networks. However, our view is that were this option to be adopted, the manipulation carried out by international gateway would be with regulatory backing and with good intention, that it is changing things in the safe direction[10], and for the CAMEL HNR case this change is regularised back to the caller's intent further down the call path. The UK would not be unique in adopting this approach, as it has already been implemented in Germany. We are therefore comfortable with taking this action.

We do note that there is an edge case that could be problematic: a legitimate caller from a non-CAMEL-HNR-enabled network, calling a customer who had invoked ACR, would receive an announcement saying to redial releasing their CLI…but since it wasn't the caller who withheld the number, there would be no means for them to do this. Whilst unfortunate, we consider this to be a very edge-case, and the consumer detriment is considerably lower than in e.g. Option 2d, where a similar caller on the non-CAMEL HNR-enabled network would lose capability to call UK numbers outright.

Although Vodafone's preference is to leave the current exemption for blocking of calls with +44 7 mobile CLIs as-is until there is evidence that fraudsters are exploiting the loophole, of the options presented for refining the blocking, we support this Option 2b, as it presents the best balance between cost/speed of deployment and optimal consumer outcome.

Option 2c – CAMEL HNR (withheld CLI+, i.e. with additional header)

Option 2c builds upon option 2b by additionally adding a signalling header to indicate that the call has been received from overseas and, potentially, which gateway received the call. We see two advantages of this:

[9] For example see German NNI specification, section 15.2.1.

[10] i.e. it would prevent a CLI that the caller hadn't expressed privacy about being displayed, rather than the more damaging scenario of causing a CLI that had been restricted by the user to be displayed

1. When regularising the CLI, the home network has added confidence that it wasn't the caller that asserted that they wished their CLI to be withheld; instead this was done by the international gateway (although we note that the fact that the mobile network received the call using the CAMEL temporary routeing number would *defacto* provide this confidence), and
2. In principle terminating networks could modify ACR behaviour such that calls with the international header would trigger a different announcement which didn't inform the customer to dial again releasing their CLI.

However, the additional header would need to be standardised then implemented by all UK networks, which would incur cost and delay[11]. On balance, we do not believe that the cost over Option 2b can be justified.

Option 2d – CAMEL HNR (allow list)

Option 2d would narrowly allow calls subject to CAMEL HNR, blocking any calls with +44 7 CLIs that attempt to route without CAMEL HNR. This would be accomplished by the international gateway creating pin holes for the temporary routeing numbers (IMRN) used by visited networks to route calls back to UK home mobile networks; calls to any other numbers would be blocked.

This approach has the advantage that any calls with spoofed mobile CLIs would be blocked and not delivered to UK customers at all (as opposed to Options 2a..c would deliver the call but with the spoofed mobile CLI not displayed). However, conversely if any overseas roaming networks do not or cannot implement CAMEL HNR, then it would not be possible for roamers on these networks to call home to the UK.

It would therefore be essential that mobile network operators have sufficient time to enable CAMEL HNR universally. This means that the implementation period would be very prolonged (years, rivalling the time for VoLTE roaming to become universal), and it is inevitable that even then, some foreign networks will not be enabled hence the scope of overseas roaming be reduced. Once again, we draw Ofcom's attention to the issue of diminishing returns highlighted in our response to Question 1. On the whole we would expect coverage of most (but not all) countries, but a reduction in the number of potential roaming partners in each country, meaning UK roaming customers would experience reduced coverage.

The activity within UK mobile networks will be the same as for other options in this group, albeit the volume of traffic subject to CAMEL HNR may be marginally higher. The changes at international gateway largely amount to altering configuration to allow through traffic to IMRNs but blocking traffic to other numbers. The IMRN ranges are similar (but not the same) as other ranges that have already been subject to pin holing arrangements to protect inbound roamers under existing blocking. Note that the list of IMRN ranges is not static, so international gateways would need to manage these arrangements on an ongoing basis.

Due to the need to universally enable CAMEL HNR before any further blocking can occur, we do not support this option – by the time the preparatory activity has been undertaken, we would be largely dealing with a

[11] We note that such headers have been developed internationally – see German NNI specification, section 15.2.3.

legacy issue as traffic will have evolved to VoLTE roaming. We understand that some other communication providers may support this option, but we do query whether they are aware of the sheer volume of roaming arrangements involved, and difficulty with negotiating changes in networks globally.

Summary

	1a Query MNO	1b Proxy	1c Query database	2a CAMEL remove CLI	2b CAMEL CLI withheld	2c CAMEL CLI withheld+	2d CAMEL blocking
Achieves goal	✓[12]	✓	✓	✓✓	✓✓	✓✓	✓✓✓[13]
Scope to be circumvented	XXX	XXX	XXX	✓✓✓	✓✓✓	✓✓✓	✓✓✓
Avoids erroneously blocking non-spoofed calls	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	XXX[14]
Time/cost to develop (gateway)	XXX	XX	XXX	XX[15]	✓✓	XXX[16]	✓✓✓
Time/cost to develop (MNOs)	XXX	XX	XXX	XX	✓✓✓[17]	XXX	XXX[18]
Time/cost to develop (others)	✓✓✓[19]	✓✓✓	✓✓✓	XX	✓✓✓	XXX	✓✓✓

Vodafone's preference is that any decision is deferred until there is evidence of the degree of consumer harm of fraudsters migrating to using spoofed mobile CLIs as a result of other blocking measures. If there is sufficient evidence, then of the options presented, Option 2b has clear advantages in terms of speed of delivery, and allowing mobile network operators to make commercial decisions on a roaming partner basis as to whether accelerate VoLTE roaming implementation, accept a degree of loss of CLI display, or implement CAMEL HNR. We believe a likely outcome would be to accelerate VoLTE where possible,

[12] Lower score than Group 2 because it only checks if the user is roaming – doesn't check if it is the valid is placing the call
[13] Higher score than other Group 2s because non valid roaming calls are blocked outright
[14] Recognising that it will not be possible to CAMEL-enable all visited networks
[15] Standardisation needed
[16] New header needed
[17] High score because if MNO isn't ready, solution could be launched (it just means their roaming customers would not have CLI)
[18] Need to arrange CAMEL HNR with every roaming partner globally
[19] No activity needed

implement CAMEL HNR for any high-volume roaming destinations without VoLTE support, and accept loss of CLI for low volume roaming destinations – a commercial rather than regulatory decision. Indeed, the regulatory intervention would be quite limited for this option – Ofcom would simply need to specify that from an agreed date, international gateways must assert privacy on any UK mobile CLIs received from overseas.

In contrast, the other options presented are either unsuitable for the UK (and arguably don't achieve Ofcom's goal), or force mobile operators down the path of implementing legacy technology (or face the loss of roaming partnerships).

Question 7: Are there any international experiences of tackling this issue that you think are particularly relevant for the UK? Please provide evidence and an explanation for your answer.

A roaming-check solution that has been adopted in Ireland (including by Vodafone's Irish operations), but we must stress that Ireland has a porting database so is able to triage queries to the relevant mobile network. As the solution has only recently been implemented, it is too early to observe whether fraudsters will seek to exploit the aspect that the solution only checks that the number is roaming, rather than whether the call is validly being made from that number.

We note that Ofcom did not reference the solution adopted in Germany, which most closely aligns with Options 2b/2c.

Question 8: Are the factors outlined in the section 'framework for evaluating options' the right things to think about when making a decision on options to address spoofed UK mobile numbers, and are there any additional factors which we should consider? Please explain your response

We agree with the factors set out in para 4.47. The table we provide in response to Question 6 sets out our thoughts on these.

Vodafone UK
September 2024