

Cat Kelly  
Ofcom  
Riverside House  
2A Southwark Bridge Road  
London SE1 9HA

Dear Ms Kelly,

**Re: Mobile Spoofing**

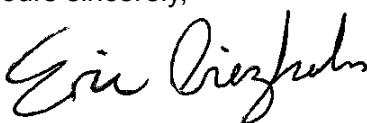
Thank you for your 29 July 2024 call for input regarding the spoofing of UK mobile numbers by international fraudsters.

The Mobile Ecosystem Forum (MEF) is a global trade association headquartered in London with members in 45 countries. We seek to provide an international perspective on matters that impact our members and the communications ecosystem as a whole. MEF members collaborate to develop and support best practices, codes of conduct, and anti-fraud schemes that benefit consumers, mobile network operators, and organisations that engage with the public through their phones.

Our comments are given in the following pages, using the format of your standard response form. The key observations are:

- Ofcom and UK communications providers have already significantly reduced the number of consumer complaints about scam calls by pursuing a strategy focused on the blocking of inbound international calls which spoof domestic landline numbers
- Blocking spoofed calls that come from overseas aligns with strategies covered by ECC Recommendation 23(03) of the European Conference of Postal and Telecommunications Administrations (CEPT) and hence encourages the rapid roll-out and harmonisation of consumer protection controls across the continent, to the benefit of both consumers and communications providers
- The experience of other countries that block inbound international calls which spoof domestic landline numbers is consistent with anecdotal accounts that UK providers are seeing an increase in the frequency with which UK mobile numbers are spoofed
- NICC has provided exemplary technical leadership in determining how to identify and block spoofed calls and the UK industry should continue to be guided by them
- Other countries are simultaneously exploring how to effect blocks on international calls that spoof domestic mobile numbers so the UK should also monitor their progress with the intention of sharing what each has learned
- Fraudsters adapt to circumvent new controls, so it is wise to prioritise the speed of implementation over the pursuit of perfection when designing technical measures to protect consumers from crimes that occur on a daily basis

Yours sincerely,



Eric Priezkalns  
Director of Anti-Fraud and Integrity, Mobile Ecosystem Forum

## Your response

Question	Your response
<p><b>Question 1:</b></p> <p><b>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></p> <p><b>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.</b></p> <p><b>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.</b></p>	<p>Confidential? – N</p> <p>a) Yes, your description of the ways that mobile calls enter the UK is both accurate and comprehensive.</p> <p>b) Per our members, each of the routes carries a significant amount of traffic. None of the routes is so minor that we can afford to ignore it. They all need to be addressed by anti-spoofing mitigations at the same time to avoid creating an incentive for fraudsters to evade new controls by simply changing which routes they use.</p> <p>c) Not applicable.</p>

<p><b>Question 2:</b></p> <p><b>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?</b></p>	<p>Confidential? – N</p> <p>Some of our members will be better able to evaluate the economic impact of crimes conducted by spoofing mobile numbers, so we will leave it to them to respond individually with estimates that will likely vary. However, it is the consensus amongst our members that the economic impact is serious and rising.</p> <p>It would be a mistake to assume that the retirement of 2G and 3G networks in other countries will contribute to a reduction in the number of harmful calls received by UK consumers. This is because there is no evidence that scam traffic is geographically distributed across international routes in similar proportions to that of ordinary, legitimate traffic. Whilst some near neighbours of the UK will undoubtedly retire legacy networks sooner, and they will represent a much larger share of legitimate inbound roaming traffic than that coming from other continents, fraudsters place their call centres in parts of the world which are most conducive to committing crime without interference. In 2023, the Office of the United Nations High Commissioner for Human Rights estimated that criminal gangs forced at least 220,000 people to work in scam call centres in Cambodia and Myanmar<sup>1</sup>. A May 2024 report from the United States Institute of Peace (USIP), a US government-funded nonpartisan research institute that focuses on conflict resolution and prevention, built upon the same research as used by the UN to estimate a further 85,000 people are being forced to work in scam call centres in Laos<sup>2</sup>. Per USIP's calculations, that would mean approximately 60% of scammers working worldwide are currently based in just these three Southeast Asian countries. However, international and national police operations to tackle scam call centres and human trafficking have been conducted against similar scam compounds in countries as diverse as Peru, Türkiye and Zambia, each of which evidenced ties to organized criminal gangs that originated in China. The locations of these scam compounds, and the use of forced labour to staff them, indicates that criminal gangs are adept at evading law enforcement by reconstituting the same scam business models in whichever regions allow them greatest freedom to act.</p> <p>The location of scam compounds bear little relationship to where potential victims will be called. Numerous reports indicate the key limitation for criminals is not the international routing of telephone calls and other forms of electronic communication, but the availability of scammers who are fluent in the same language as the intended victim. The aforementioned UN report identified at least 20 different nationalities amongst those forced to work in Southeast Asian scam compounds, whilst USIP said 60 different nationalities have been found working as scammers in that region. English language skills are amongst those sought. Indian embassies in Cambodia and Laos have been reporting a dramatic increase in the work they are doing to repatriate Indian nationals who state they had been lured into working in scam compounds by</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<sup>1</sup> <https://bangkok.ohchr.org/online-scam-and-trafficking-sea/>

<sup>2</sup> <https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security>

	<p>advertisements for well-paid jobs requiring proficiency in English and IT. The true nature of the work they were expected to perform only became apparent after they had arrived, at which time they are prevented from leaving. This work commonly involves meeting targets for the scamming of victims in Western countries, sometimes leading to physical abuse if targets are not met. Having been tricked into working in the scam industry, the unwilling scammer is prevented from leaving their scam compound unless their families are willing to pay a ransom for them.</p> <p>Large seizures of equipment by Thai police and customs suggest that criminal gangs have been rebasing scam compounds from areas affected by hostilities between rebel forces and the central government of Myanmar and its allies<sup>3</sup>. This equipment includes GSM gateways (also known as 'simboxes') and large numbers of SIM cards. In May 2024, Thailand's National Broadcasting and Telecommunications Commission, with the support of the Thai police, ordered the destruction of 84 mobile cell sites situated near Cambodia to deny coverage to scam compounds on the other side of the border<sup>4</sup>. This corroborates the conclusion that organized criminal gangs have been using mobile networks to originate much of their scam traffic. It is reasonable to assume that they will continue to base their operations in places where they will be able to work around network controls, in some cases by preferring the use of 2G and 3G connectivity.</p> <p>With these observations in mind, we think it appropriate to highlight that British consumers who are defrauded are not the only victims of this kind of organized crime. Many of the people who work as scammers are also victims, with a growing number of reports of not just human trafficking, but also of violence, torture and even the murder of individuals who refused to work or attempted to escape. Reducing the harm to British consumers will also cut the criminal proceeds being generated by these organized criminals and eliminate some of the incentive to lure, kidnap and enslave the people they force to work as scammers.</p>
<p><b>Question 3:</b></p> <p><b>a) What is the scope and scale of consumer harm caused by spoofed UK mobile numbers?</b></p> <p><b>b) What are the consumer impacts of spoofed UK</b></p>	<p>Confidential? – N</p> <p>We leave it to our members to provide their evaluations of the scale of consumer harm caused specifically by calls which spoof UK mobile numbers, some of which will be based on data that they may wish to keep confidential.</p>

<sup>3</sup> <https://www.facebook.com/royalthaipolice/posts/pfbid0bwS7YJVkioAY7xjrMhdzsrWPzbZgjVL7G5Qr4x5AuqJFdsQve4n6o3YpERKKTywl>

<sup>4</sup> <https://nbt.go.th/news/information/66026.aspx>

<p><b>mobile numbers more broadly?</b></p> <p><b>Please provide evidence to support your responses.</b></p>	
<p><b>Question 4:</b></p> <p><b>a) How significant is the volume of spoofed mobile calls from abroad?</b></p> <p><b>b) Is there any evidence that scammers are moving from spoofing fixed to mobile UK CLI?</b></p> <p><b>Please provide evidence to support your responses.</b></p>	<p>Confidential? – N</p> <p>The consensus of our members is that it is extremely difficult to estimate the current number of spoofed mobile calls coming into the UK from abroad. However, anecdotal reports from regions which have already started to implement blocks on spoofed mobile calls reinforces the impression that criminals rapidly transitioned to spoofing mobile calls following the implementation of comprehensive blocks on international traffic that spoofed landline numbers. In particular, business with an interest in Middle Eastern countries report that the need to block spoofed mobile numbers became almost immediately apparent following the successful implementation of blocks on spoofed landline numbers.</p>
<p><b>Question 5:</b></p> <p><b>How will developments in deployment of mobile technologies in the UK and abroad affect the problem of spoofed UK mobile calls from abroad? Please provide evidence to support your response.</b></p>	<p>Confidential? – N</p> <p>The evidence presented above speaks to the extent to which it is dangerous to assume the kinds of traffic generated by criminals will mirror trends in international traffic more generally. Criminal gangs have already shown themselves to be adept at locating and relocating their operations in response to even the unusually proactive cross-border law enforcement practices of the People's Republic of China. The history of global telecommunications gives us very good reason to believe that it takes decades for legacy technologies to be superseded <i>everywhere</i>. Whether 50%, 80% or 90% of regular traffic is handled by technologies that are inherently more secure is irrelevant to criminals who will continue to actively exploit the vulnerabilities inherent to legacy technologies so long as they can be found somewhere. British consumers will not be adequately protected for the foreseeable future unless comprehensive controls have been effected by businesses that are subject to British jurisdiction. The only fair way to protect British consumers is by imposing the same control objectives across all traffic coming into Britain from abroad, thus preventing any communications business from seeking an advantage by implementing a lower grade of controls, and thus profiting from</p>

	the additional traffic that criminals will preferentially route over their networks.
<p><b>Question 6:</b></p> <p><b>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></p> <p><b>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.</b></p> <p><b>c) What would be the advantages and disadvantages of obtaining more information about, and oversight of, the international gateway</b></p>	<p>Confidential? – N</p> <p>a) The approach outlined in the 'group 1' options represents the best prospect for reducing the number of calls spoofing UK mobile numbers sooner rather than later. In all matters involving consumer protection, it is vital to keep in mind the cost to the public of ongoing harm as well as the cost of any technologies and processes that curb that harm over time. Though it may not always be seen as an immediate priority by businesses operating in a highly competitive landscape, the ongoing harm caused by scam calls damages the public's perception of how much they can trust phone calls, and hence damages all businesses that generate an income from the supply of this service. Ofcom's own research indicates segments of the public are less trusting of calls from numbers they do not recognise and are less likely to accept them, accelerating the global decline in revenues generated by voice traffic.</p> <p>NICC is best placed to evaluate the costs and merits of the specific technical alternatives included within group 1. However, one variable that also needs to be factored into Ofcom's evaluation is the cost of mandates imposed by regulators from other nations on international gateway providers. If different national regulators impose mandates which are inconsistent with each other then the burdens on international gateway providers will multiply. However, if they are consistent then there will be considerable cost synergies. The cost versus benefit analysis of how to protect consumers from the <i>global scam</i> needs to be assessed with respect to the costs required to protect consumers in multiple jurisdictions, not just consumers in the UK. This means there will be greater cost efficiency if the same controls can be effected in multiple jurisdictions, and such cost efficiencies would outweigh any benefit sought by attempting to apply the lowest-cost method of protecting the public which is consistent with the law in each separate jurisdiction that communications providers may serve.</p> <p>No single party can state with certainty the extent to which other nations will seek to reduce scam calls by placing mandates on international gateway providers of the type described in group 1. However, the work done by CEPT and ComReg, as highlighted by Ofcom in this consultation, suggests a common direction of travel is now emerging. If the majority of European regulators can coalesce around a common group 1 approach then there will be considerable benefits in terms of managing costs and in gathering intelligence about the origin and routing of scam calls. The fact that such varied countries as Saudi Arabia and Poland have already adopted controls of the type included in group 1 suggests others will likely reach the same conclusion, with the result that many international gateway providers will need to comply with such requirements for at least some of the countries they deal with.</p>

**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.**

**d) What would be the advantages and disadvantages of industry-led solutions, and where might regulatory intervention be required? Please give an explanation for your response.**

The consultation document makes no mention of the work being conducted by the US Federal Communications Commission (FCC) to tackle international scam calls, but it is fair to state that this is also placing an increased burden on international gateway providers. In particular, it is difficult to envisage any scenario where international gateway providers are able to satisfy the evolving requirement to assist with international traceback without also devoting more resources to gathering and disseminating intelligence about the origins of voice calls that they convey. If this is to occur anyway, there would be considerable benefit to international gateway providers if they can access sources of information from mobile network operators about whether a call has spoofed the mobile number of an individual who is not currently roaming. Again, the cost of implementing a well-designed and common approach that is consistently implemented across multiple nations should be weighed against the benefit of improvements in an international gateway providers' ability to apply know-your-customer controls on who they do business with, and so progressively weed out bad actors in concert with the use of enhanced international traceback processes.

The transition to VoLTE will progressively reduce the freedom of action currently exploited by fraudsters. However, it would be erroneous to assume that criminals will originate scam traffic on different kinds of networks in the same proportion to the rest of society. On the contrary, the aforementioned willingness of criminal syndicates to base their operations in locations where they expect less interference from law enforcement highlights the extent to which they can also preferentially generate traffic that originates on pre-LTE networks. Some telcos may choose not to support outbound roamers on pre-LTE networks, but this is also a commercial decision and it has implications for providing connectivity to phone users who roam in developing economies. If we apply the common rule of thumb that criminals adapt to work around new anti-fraud controls, they will not need to adapt if they already originate traffic on pre-LTE networks which a local mobile network operator is not in a hurry to replace or shut down. There will instead be a perverse economic incentive for mobile network operators in other countries to continue to give unfettered access to pre-LTE networks to criminals, if there are no downstream controls that highlight the extent to which these networks are enabling international crime.

b) ComReg's approach of giving international gateway providers a choice of whether to interrogate the roaming status of a mobile phone with the home network directly, or via an intermediary, but subject to a threshold that exempts smaller operators, represents the quickest way to make progress with a control of this type. The exact details of how information is transmitted directly, or via an intermediary, need not be tightly prescribed if there is a general obligation for operators to provide this data and for gateway providers to obtain it. More value would be gained by pursuing consistency in the type of information that must be provided and obtained, as this would lend itself to the development of APIs that would be useful in any country for

	<p>scam reduction, and thus could be co-opted for further anti-fraud controls in future.</p> <p>c) It is rare for international gateway providers to be penalised for carrying criminal traffic, though the evolution of international traceback controls suggests this will change over time. The absence of punishment for businesses that consciously choose to apply lower standards in scrutinizing who they do business with, and the kinds of traffic they convey, is prejudicial to those international gateway providers that take a more robust approach to vetting customers and tackling fraud. Superior oversight of international gateway providers will likely prove to be of overall benefit to those providers that already do most to tackle crime.</p> <p>d) Industry should lead in the development of flexible and cost-effective methods such as the use of standardised APIs for the exchange of information required for controls of the type described in group 1. However, it is nigh on impossible for industry to impartially assess which businesses are doing too little to tackle fraud, and this means regulators must intervene to set both minimum expectations and to create an environment where it becomes routine to measure how well each business complies with those expectations.</p>
<p><b>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.</b></p>	<p>Confidential? – N</p> <p>ComReg based their determinations on exhaustive international research, and their experience as a prosperous English-speaking island nation is especially relevant when judging how effective an anti-fraud control would be if implemented in the UK.</p>
<p><b>Question 8:</b></p> <p><b>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</b></p>	<p>Confidential? – N</p> <p>All of the factors identified by Ofcom are relevant to this decision. In addition, we believe other factors should also be considered, or at least that unspoken assumptions should be avoided if it is impractical to evaluate the following factors.</p> <ul style="list-style-type: none"> <li>- The international nature of the crimes facilitated by mobile spoofing, and the international nature of the businesses that need to be involved in tackling crime, suggests that the most cost-effective way to tackle crime involves widespread international harmonisation of rules and regulations to detect and prevent scam calls. Harmonisation may be difficult to attain in practice, but costs on international providers should be understood in this context, as</li> </ul>



<p><b>UK mobile numbers, and are there any additional factors which we should consider? Please explain your response where appropriate.</b></p>	<p>should the effectiveness of controls that are put in place. Greater harmonisation will keep compliance costs down for telcos and increase the benefits of coordinated international action to identify and punish criminals and the businesses that enable them.</p> <p>- It is vital to avoid assumptions about the transition to LTE and how this will affect <i>scam</i> traffic. Criminals have demonstrated they have the resources to establish new scam compounds in new locations, including new countries, where there is an advantage to them because of the availability of the workers that they need, because there is less threat of intervention by law enforcement agencies, or because network connectivity is favourable to their goals. Any assessment of how the transition to LTE will affect international voice traffic should be made particular to the objectives and circumstances of criminals, or else it will present an unrealistically optimistic picture of how the roll-out of LTE networks in other countries might contribute to a reduction in crime within the UK.</p> <p>- It is often stated that tackling fraud is a game of 'whac a mole', where criminals rapidly adapt and use new methods to work around the limitations of any anti-fraud controls that have been adopted. Instead of being surprised by the ingenuity of criminals, let us instead assume that any work around that can be anticipated will soon be put into effect.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Please complete this form in full and return to [Mobilespoofingresponses@ofcom.org.uk](mailto:Mobilespoofingresponses@ofcom.org.uk)