Non-Confidential

Vodafone Response to Ofcom Consultation:

Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers

Introduction

Vodafone welcomes the opportunity to comment on Ofcom's thinking around detecting and blocking calls with spoofed Calling Line Identity (CLI) numbers.

We share Ofcom's goals. Vodafone was first UK network to deploy call blocking, and we retain a team dedicated to detecting and stopping nuisance and fraudulent calls. We have been a member of Ofcom's strategic working group on the reduction of nuisance calls for over five years. We have been instrumental in ensuring that NICC Standards investigated the requirements for STIR in order that an informed decision could be made as to whether it should be implemented.

Although we would like to, it is not feasible to implement measures that will totally stop such fraudulent activity. Inevitably, we are dealing with a game of whack-a-mole - a more realistic aspiration is to make the perpetrators of fraud's life more difficult, and to disrupt their schemes.

Vodafone doesn't subscribe to the mindset that "*all the bad guys are overseas*" and that as such, anything within the UK is likely legitimate. This is particularly the case as greater controls are introduced on inbound international calls, which will displace fraudulent traffic to using UK origination instead. We therefore need techniques that will complicate perpetrators' activities whether they are undertaken nationally or internationally. We need a suite of solutions, but practicably, given it is a game of whack-a-mole, we cannot support spending large sums of money on measures that are easily circumvented: a balance must be struck.

We do not believe that a case has been proven for the deployment of CLI authentication (STIR) in the UK. That is not to say that we oppose deployment, instead we consider that Ofcom needs to go a lot further in establishing the costs and benefits associated with STIR, and in counterfactual solutions which could achieve similar goals, before there can be any regulatory mandate to deploy it.

Answers to questions

> Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

We recognise the scenarios that Ofcom sets out, which are indeed frequent.

Although we support measures to reduce the degree of illegal spoofing of CLIs, no approach is ever going to be entirely water-tight (indeed, Ofcom must guard against portraying that future developments are achieving that goal, as to do so would be misleading and provide a false sense of security to consumers). The examples cited by Ofcom therefore illustrate the importance of educating the general public as to the weaknesses of CLI display services. It must be made clear that, much like display names in emails, the public can only ever

regard the CLI displayed as informational rather than authoritative (at least to the level that no-one should consider handing over money based on a call depicting a familiar CLI).

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

The inherent nature of a game of whack-a-mole is that once one mole is struck, another appears. So from this perspective, of course, there is always more that can be done – indeed success can be gauged by the ability to anticipate and address the fraudster's next move before they have chance to make it. It is important that network operators and Ofcom continue to meet to confidentially share intelligence on the latest approaches by the perpetrators of fraud and state-of-the-art in solutions for combatting spoofed numbers. However, as alluded to in our introductory text, an approach where each countermeasure costs large sums of money – inevitably borne by customers - but where the countermeasure is overcome within days, is doomed to failure.

We believe that it is instructive to divide the problem based upon the origin of the call:

- For calls originated internationally, we have already taken measures to block calls with UK Network Number CLIs which are likely fraudulent, and are currently blocking around ✂ such calls per month. This inevitably leads to such fraudulent calls instead being sent with either UK Presentation Number CLIs, or using UK mobile numbers (which are currently exempted to allow UK customers roaming internationally to call home).

  We believe the matter of whether to extend the blocking to include calls with UK Presentation Number CLIs is an issue that should be agreed between Ofcom and those legitimate UK enterprises that have off-shore call centres which currently send their traffic into the public network in the locality of their call-centre. We note, for example, that some of the Government outbound call-centres used during the COVID pandemic made use of such an approach – an offshore call-centre is not, in and of itself, an indication of fraudulent behaviour.

  If blocking was extended to UK Presentation Number CLIs, this means that the required architecture (absent displaying an overseas CLI, or onshoring the call-centre), would be to long-line the egress of calls from the call-centre to a UK national network. As a UK national network, it would therefore be somewhat self-serving of Vodafone to lobby for such a mandate (or, indeed, to implement such blocking without a regulatory requirement to do so). If, however, Ofcom were to extend its blocking rules, then we would of course comply on our international gateways, whilst providing long-line solutions for those enterprises that wished to have off-shore call-centres.

We appreciate the desire to extend international call blocking to include mobile CLIs. We are meeting with other mobile network operators and gateway providers to determine if there is a mechanism to do this (but would caution that the exercise is not trivial, either form a technical or cost perspective). It is important to note that VoLTE roaming, which will increasingly become the norm over the next few years, inherently passes all calls via the home network, so will close the necessity for the loophole – we are not seeking to dismiss consideration with an excuse of "*wait for VoLTE roaming*", but we must be wary of designing a solution which is both expensive and only delivers at the point it becomes redundant in any case.

- For calls that are originated nationally, the key need is that there is rapid traceback to the originating network so that the perpetrators can be brought to account where potentially fraudulent calls are identified. Two things are needed to achieve this, namely identifying the calls, and tracing the calls back.
    - For identification, we believe that there needs to be more intelligence sharing between terminating network operators so that when fraudulent patterns are observed, knowledge is not kept within a single operator's team. We acknowledge that our teams need to be on guard for generic fraud against our customers, rather than only focussing on fraud relating specifically to their telephone service or fraud against our organisation. Whilst mobile termination has a standardised reporting mechanism via 7726, there is no equivalent for fixed telephony. We wouldn't necessarily advocate a centralised reporting function (as the terminating network is best-placed to initiate the subsequent traceback), but it may be appropriate to have a standardised access code/reporting interface.
    - For tracing, there is no effective traceback process in the UK. Indeed, it is seriously unhelpful that given a particular number range, operators do not have a comprehensive list of contact details to liaise with the originating network. Our understanding is that Ofcom doesn't either[1], which simply isn't good enough for the numbering plan administrator. At the very least, both Ofcom and network operators should have access to a list of (manned) email contacts for each rangeholder, and in the case of hosted number ranges, contacts for the network that is hosting the range. We believe that if there was an effective traceback process – it doesn't require automation, just reliably-resourced inter-operator helpdesks that could provide an immediate response, then it would be possible to determine who originated a fraudulent call and hold them to account in minutes rather than the weeks that it currently takes.

[1] At least one that is suitable for the 21st century – we need working contact email details, not a number for a fax machine.

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

At the outset, we must reiterate that Vodafone does not believe that a case has yet been made for implementation of STIR technology in the UK. This is not to say that we necessarily oppose implementation, rather that until a full regulatory impact assessment has been completed, there is insufficient evidence. As we are sure Ofcom recognises, the current consultation does not engage in detail on this matter. A proper impact assessment must include the costs and benefits of implementing STIR when compared to the costs and benefits of alternative measures. The costs must be rigorously assessed via an in-depth feasibility study. For now, we are providing comments as to the feasibility and workability of the proposals in the consultation, as these might shape any subsequent impact assessment exercise: we stress, however, that this should not be taken to be tacit support for implementation.

Overall purpose of attestation

When it works, STIR technology would allow a call to be instantly and unambiguously traced back to the originating network, and if combined with a numbering database, could provide evidence of the originating network's rights to populate the CLI(s). This is undoubtedly a step forward from the existing situation, but it requires a significant certification infrastructure, the deployment of application servers at the originating and terminating networks, the carriage of potentially large amounts of signalling data in call headers, the implementation of rules to ensure that signalling is maintained on an end-to-end basis (which may conflict with the provisions of the Code of Practice under the Telecoms Security Act[2]), and agreed processes to cope with exceptions. It is therefore a costly exercise.

Much of the expense stems from the implicit design assumption in STIR that calls are carried through untrusted networks. It would have been a simpler development to add a parameter to signalling that identified the originating network, but STIR adds an extra layer of security via digitally signing various signalling parameters to prevent man-in-the-middle attacks and/or one originating network passing themselves off as another one. These are undoubtedly risk vectors in an internet-calling environment, but it is less clear whether the additional complexity can be justified in a purely national scenario with a relatively limited number of telephony networks involved. Nonetheless, if we are to align with international standards, then it seems that for CLI attestation, STIR is the only available solution.

It may be possible to justify the expense of CLI attestation if there were no practical alternatives, and implementation provides assurance in 100% of call cases. However, we are concerned that there are alternatives that could be considered (see response to Q4.1), and the presence of call cases where full STIR

[2] Paras 2.78-2.79 of the Code of Practice specifies that networks should fully parse and process signalling before passing it to core networks (i.e. the implication is that signalling should be reconstructed). However, inherently the logic underpinning STIR is that signalling is end-to-end and is not manipulated in any way by transit networks. It is unclear the degree to which these paradigms are in conflict.

attestation cannot be provided will leave gaps that inevitably will be exploited by the perpetrators of fraud (see response to Q5.2).

The CLI Authentication Administrator

We are reassured that Ofcom proposes the sensible approach of there being a single CLI Authentication Administrator for the UK (we note that the SHAKEN model adopts an additional layer of complexity by there being multiple certification authorities – this addition of potential competition may be justifiable in a market the size of the USA, but it is unlikely to be so in the UK). We are, however, dismayed that Ofcom identifies the need for this key role but passes implementation to industry. This is incompatible with Ofcom's role as the UK national numbering administrator, and if it wishes to see attestation of numbering data then we believe it must take an appropriate role in deployment of the solution to ensure it technically works.

For example,

- how could an operator-owned Authentication Administrator know who to distribute certificates to, when only Ofcom knows the correct details for each numbering range holder?
- in the case of a dispute about the identity of the originator, a complainant may claim the Authentication Administrator is acting anti-competitively. Vodafone does not want to be in the role of policing the identity of competitors, indeed, we believe this would be inappropriate for the market.

We anticipate an argument that the regulator should not be involved in the operation of UK networks. We agree. The CLI Authentication Administrator is not an operational role, it is an administrative one, responsible for ensuring that the legitimate number range holders, and only legitimate number range holders, have access to the certificates which are vital to the success of CLI attestation. The extra features set out in the consultation around intervening when rules around STIR are not followed are inherently regulatory functions.

If Ofcom seriously wants to implement STIR in the UK, then Ofcom must play its part and act as the Authentication Administrator, being the central agency for associating certification data with originating networks – at worst it might consider outsourcing this function to the Office for Telecoms Adjudication, however, we again note that this is not an industry function.

Common Numbering Database

We see the merits in the UK having a common numbering database. However, we are unclear if the benefits of such a database are justified by the implementation costs (technical, financial, and human resource) of achieving it. From a STIR perspective:

- Without a database, STIR can provide a pointer back to the originating network.

- With a database, STIR can provide a pointer back to the originating network and also allow analysis of whether usage of the CLI in question was permitted from the originating network[3].

As a database can, largely, be bolted onto a STIR solution, we consider that this can be a sequential exercise. If STIR was to be implemented without a database, an assessment could then be undertaken as to the extent that originating customers and/or networks were seeking to mislead by using numbers as CLIs when they had no rights to do so. If there was significant abuse, then that would form part of the impact assessment for implementing a numbering database to refine the STIR solution. If, however, there was little abuse, then there would be little justification (at least from a STIR perspective) to implement a database. Therefore, at this stage we would assert that Ofcom cannot have the evidence to justify the costs of incorporating a database – it would be premature to mandate one.

Notwithstanding this, we do note that there would be advantages of having a database for improving CLI integrity, beyond the narrow case of a database being used for terminating network STIR lookup. If a database solution incorporated "*also permitted from*" data that provided a list of originating networks that a given enterprise had chosen to use, then originating networks could validate the presentation CLIs that their customers were using on a call-by-call basis. Whilst this could influence whether a call should be signed via STIR, absent STIR implementation it could also determine whether a call was allowed to proceed at all. However, the population of this database would not be trivial and per our earlier comments, Ofcom would need to make a compelling case for the resources required compared to the effectiveness of the proposed solution.

Inbound international

We note the proposal that inbound international calls be marked with gateway attestation, which seems a pragmatic approach (in absent of interworking with other global STIR schemes). For UK mobile customers that are roaming overseas, the gateway attestation could potentially be elevated to a higher full attestation, should a solution for identifying them be found (see response to Question 4.1).

We are concerned, however, by some of the language utilised in Paras 5.46-5.48 regarding the responsibilities of gateway providers – in particular that they would be expected to validate calls using common numbering databases in other jurisdictions, and that they would be expected to validate calls from their own customers regardless of their location.

- The first of these requirements misunderstands the nature of gateway facility provision – on the whole gateways are relatively dumb transit hubs that do not incorporate facilities such as Intelligent Network lookups, let alone integration into originating networks and/or national numbering databases to carry out this check. Further, UK gateways do not typically receive calls directly from

[3] So long as the database contains details of both the authoritative network-of-record for the number, and also a list of networks where the customer might use that number for outbound calls.

originating countries, rather they are a link in the chain with global transit providers being upstream – so for example we might receive calls from a French carrier that relate to Asian CLIs, so it is unclear what check Ofcom is expecting we carry out when we have no relationship with the Asian origination.

- The second requirement goes further, and risks being anti-competitive. We query what Ofcom means by *"calls made by their own customers irrespective of location"?* For Vodafone, is the reference to "*own customers*" relating to Vodafone's UK contracted customers, any customers of subsidiaries of Vodafone plc, or any customer of a company bearing the Vodafone brand[4]? For VMO2, would this extend to any customers of Telefonica or Liberty Global? It is not feasible to hold companies with multiple international companies to take responsibility for CLIs populated many hops away, while providers that are predominately UK-based would have no such requirement, hence face a far lower regulatory burden, and undercut our operations. ✂

We note that both of these requirements are implicitly focussed on non-UK CLIs, as other initiatives are already addressing that usage of +44 CLIs from international origins. Yet we have seen no evidence of fraud being perpetrated using international numbers. As such, the requirements appear to be seeking to address a problem that doesn't at present exist.

There are better and alternative solutions to the underlying problem of CLI fraud, and we remain an active partner of Ofcom in respect of these.

[4] Noting that we have partner relationships where the Vodafone logo is used but which are not a consolidated part of Vodafone.

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why

The problem with STIR is not with the call cases that are covered by the technology, but those which are not readily addressed. The rather weak attestation that is introduced on international calls has been recognised by Ofcom, but another area is where calls are forwarded/diverted. There are measures built into STIR technology that can readily cope with network-based call forwarding, but the scenario of a customer diverting calls from their own equipment is not easy/possible to accommodate within the STIR standards (at least where a common numbering database check is involved), meaning that such calls will either go unattested or fail verification[5]. This is because in the scenario of the customer equipment diverting the call (Type 4 CLI), the presented CLI will be that of the original caller, so any lookup to the numbering database will assert that the CLI is associated with neither the "originator" (i.e. the customer who diverted the call) or their chosen network.

It may be asserted that this is an edge case, and the majority of calls will benefit from STIR attestation, but it is these edge cases which are both important and which represent cracks in the supposed defence created by STIR. For example it is common for doctors' surgeries to put lines on divert out-of-hours, and we are sure that Ofcom would be unhappy if such diversions failed. So a sensible response may be to exempt these calls from the STIR scheme – but then when a terminating network receives an unsigned call, is that a doctors' surgery on diversion, or is it because it's a call with a fraudulent CLI? The defence provided by STIR starts to crack.

Would STIR reduce the volume of nuisance calls? Yes. Would it reduce the volume of fraudulent calls? Maybe. We suspect that if STIR were to be implemented in the UK, the task of dealing with fraudulent calls would evolve to detecting ways in which perpetrators of fraud are seeking to attack consumers via the gaps left by STIR technology, indeed consumers may be lulled into a false sense of security if it was portrayed that CLI was now attested so somehow more secure..

Further, as we set out in response to Question 4.1, there are alternative solutions in the guise of improved traceback processes. In comparing STIR with these, the main advantage of STIR is that the answer to the question of which network originated a call is provided instantly, rather than potentially taking a few minutes. As such, there would need to be a huge value premium in securing that instant answer, to justify the extra costs of implementing STIR.

[5] This gap could in principle by closed by insisting that all call forwarding must use a network-based solution. However, it ill-behoves us as network operators to tell our customers that they MUST stop using their own facilities and instead use our charged-for services, as a consequence of technology that we have introduced. We believe that the SHAKEN implementation seeks to address this by allowing customers to attest their CLI, but this brings another level of complexity as it would require administration of their certificates, and a numbering database extending to cover the identity of the customer too.

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

Inevitably there are gaps in STIR as we set out in response to Question 5.2, which are difficult to close:

- Diverted calls are not well catered for. There are extensions to STIR which can cope with these, but they are not suitable where the diversion is being handled by customer equipment (absent sending certain signalling parameters to the equipment which we are not permitted to do). We do not know of any way of resolving this issue, short of mandating that all call diversion is network-based.
- International calls are not well catered for, absent interworking of national STIR implementations. We are surprised, however, that Ofcom's consideration appears to have missed the potential of interworking with other jurisdictions, and instead is assuming that all calls arriving from international destinations will need to be signed with gateway attestation by international gateways. This is the case for any calls received with no STIR information (which is the situation today), but where a call is received with, for example, SHAKEN signing[6], we would expect the correct behaviour to be to pass that signing transparently for the terminating network to verify it, rather than deleting it and substituting less authoritative gateway attestation. Of course, to do this requires that terminating networks are aware of/have access to the certification regime in the originating country. We would expect the role of building this information to sit with Ofcom, as the CLI Authentication Administrator – the numbering plan administrator cannot take a passive role.

However, we consider that even with the suggested changes, these gaps seriously undermine the potential worth of STIR implementation.

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

Although we agree with much of the substance of the material in Section 6 of the consultation, we cannot endorse the approach set out. As the UK's numbering plan administrator, we believe that were STIR to be implemented, Ofcom cannot take a passive role and instead must step forward to be the STIR Administrator. It may be sensible for some of the monitoring functions to be outsourced to for example the OTA, but we consider it unacceptable that regulation is outsourced to network operators with the expectation that we monitor and police the behaviour of our competitors.

[6] i.e. USA implementation of STIR

We must highlight that although there will be isolated instances where UK network providers become part of the problem via lax systems and procedures, overwhelmingly the major UK networks have proven themselves to be willing to work collaboratively to reduce the problems of fraudulent calls. Whilst there does need to be the backstop of regulatory action, we have some concerns that the tone of Section 6 of the consultation is to direct blame towards UK communications providers for the behaviour of fraudsters, when in reality we've put considerable resource into seeking to address the issue.

Ofcom is correct to distinguish between inadvertent and deliberate failures on the part of originating networks. The detail of when a network should accept some responsibility very much depends on whether STIR (if implemented at all) was implemented with or without a database:

- Without a database, whilst an originating network can take all reasonable measures to ensure there is contractual binding for enterprise customers to use the correct CLI (per the CLI Guidelines), ultimately they do not have the capability or information to check the Presentation Number CLI information is correct on calls on a granular call-by-call basis[7]. It is for this reason that the SHAKEN implementation introduced "partial attestation", which if implemented in the UK would have the meaning "*as originating network I accepted this call into the public network, I have the correct contractual safeguards with the customer but cannot check individual calls*". Unless, there is a numbering database, Footnote 342 of the consultation is wrong to suggest that this is not required in the UK - absent partial attestation, there is no way to distinguish between a CLI that has been provided by the originating network themselves/checked against an authoritative database, and a CLI that has been provided by the customer under the contractual bindings set out in the CLI Guidelines.

  On the assumption that partial attestation is supported, then the scope for inadvertent failures on the part of the originating network is limited. The situation is clear : either they provided the CLI / checked it against a whitelist so full attestation is asserted, or it was obtained from the customer so partial attestation is asserted. The situation set out in para 6.10 where an originating network "*fail[s] to pick up when a customer is misusing a number and as a result fully attest a call incorrectly*" cannot arise, because if it is a customer-supplied CLI then partial attestation should be used[8] – as such if an originating network marks a CLI as full attestation and an issue is then found with it, then they are wholly responsible, it cannot be considered an inadvertent error. Conversely, if an originating network marks a CLI as partial attestation and an issue is found with it, then the onus is on the originating network to enforce their contractual provisions - any regulatory action against them should only ensue if they are failing to do this.

[7] This is because enterprise customers using Type 3 and Type 5 CLIs typically connect to more than one originating network and the individual numbers may not be assigned to the originating network (i.e. either native or ported).
[8] Unless it has been checked against a whitelist

- With a database, we accept that the partial attestation status is not required. However, in this situation, we would expect that part of the checks that an originating network would undertake before asserting full attestation on a given CLI would be to check the contents of the database to confirm that the customer is allowed to use the number concerned. As such, the scope for inadvertent full attestation suggested in para 6.10 is limited.

Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?

We agree that a proper functioning STIR implementation would facilitate immediate traceback. However, to achieve this would involve substantial expense and the need to overcome significant technical challenges. For example STIR involves digitally encrypting various signalling parameters and checking that this encrypted version matches that received at the terminating network, which means that it is critically important that none of the parameters are amended *en-route* – but these will be traversing multiple border gateways and call servers, so changes may be needed to existing practises to ensure there are no modification of the parameters. Resolving the technical challenges will take time and skilled resource, so there is every prospect that a "jam tomorrow" solution distracts the extremely finite industry skilled resource away from providing shorter term solutions.

It is Ofcom's task to develop a regulatory impact assessment which proves whether the costs and timelines of implementing STIR are worthwhile. However, we must stress that the counterfactuals should include getting a proper traceback process in place, and so any benefits of STIR must be measured relative to that rather than the *status quo*. It should also recognise that to a large extent we have an either/or situation with STIR because the same communication provider resources would be needed to develop STIR and develop a better traceback process.

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

Ofcom is correct to highlight the interdependencies with other initiatives such as the retirement of legacy networks. We note that reference is made to end-2025 for when the majority of fixed networks will have been migrated to IP, which is undoubtedly using BT's plans as a proxy. There are other network equipment retirement plans though, for example ✂. Ofcom should also take account of the demand of other initiatives for limited skilled resources, notably that significant manpower will be required to support the provisions of the Telecoms Security Act. As such, we believe that any implementation of STIR is likely to be at least three years away, and longer if a numbering database is mandated.

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

No. We believe that the initiative should be an Ofcom-led one, rather than the task being passed to industry. We believe that the tasks set out are broadly correct, however.

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry

We do not believe that a common numbering database can [yet] be justified solely to support the implementation of STIR. The regulatory failure in this context has not been established – for a numbering database to be required, there would need to be evidence of originating networks fraudulently asserting the rights to use a number and STIR signing it, or evidence that customers were breaking the provisions of Presentation Number CLI agreements with originating networks to facilitate STIR signing, at a level where the consequences justified the cost of a numbering database. But STIR has not been deployed so inherently Ofcom cannot have the evidence to show that originating networks will fraudulently sign calls with numbers over which they have no rights.

We are therefore of the view that there has to be a sequential approach – **if** Ofcom can make the case for deploying STIR and when that's done there is evidence of misuse that would be resolved by a database, then **if** the costs of deploying the database are justified by the benefit of removing that misuse, a database should be considered. We are not there yet.

As and when the need for a database is established, then we believe that industry could lead on the specification, although an Ofcom regulatory mandate would be required to secure implementation. Further, we accept that if there were a mandate, industry should lead on the implementation (unlike the STIR Administrator function).

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment

We agree with the benefits framework suggested by Ofcom, but would be interested to hear proposals of how some of those stated can be quantified. For example, what figure would be put on reduced anxiety on having heard about friends or family having been scammed (i.e. we do not assert this this isn't a valid concern, rather we question how Ofcom will incorporate it into an impact assessment with any economic rigour).

On the costs, we believe that certain aspects have been missed:

1. Wherever costs are commonly faced by communications providers, standard economic theory would suggest that these will be passed through to consumers of the services. We believe that the analysis should take account of any consumer detriment that would arise as a result of such price rises (acknowledging that this may be considered a second order effect). Where costs are not uniformly incurred, the analysis should consider whether this will have any impact on competition – for example if the costs are "lumpy" and do not raise linearly with call volumes, this will advantage large network providers at the expense of small ones, as they are able to spread the costs across larger customer volumes.
2. The industry is facing a skills and resource crunch, at a time when there are absolute priorities in terms of compliance with the Telecoms Security Act provisions, Shared Rural Network coverage obligations and One Touch Switching, and other near-mandatory requirements such as PSTN switch-off, 3G switch-off and 5G rollout. Quite apart from the financial requirements of another major development, the industry has finite skilled resources which are already stretched, and any further regulatory development will be at the expense of discretionary commercially-attractive developments (at a time when two of the principal mobile operators are already struggling to secure returns exceeding their cost of capital). Ofcom acknowledged this issue in the conclusion to the mobile market review, where it stated that future consumer work would have a greater emphasis on compliance with existing rules rather than introducing new ones[9]. The impact assessment should therefore address the ripple effect on other investments that will either not be delivered, or be deferred, should delivery of STIR be mandated.

Vodafone UK
June 2023

[9] https://www.ofcom.org.uk/__data/assets/pdf_file/0036/248769/conclusions-mobile-spectrum-demand-and-markets.pdf paras 5.23-5.30