General

BT response to Ofcom consultation on CLI authentication

23 June 2023

BT Group

1. Executive Summary

1.1. Despite action from industry, the prevalence of scam calling remains too high for consumers. Invalid and spoofed CLIs have increased materially and we agree action is required.

1.2. We think any action should be targeted, proportionate and effective. It should be based on the scale of risk and the ease of acting in a reasonable timeframe. The primary (though not exclusive) source of invalid and spoofed CLIs is overseas. This suggests to us two priority action areas:

- Implementing the effective alternative technical solutions of blocking presentation and mobile numbers originating from overseas. This should be backed up by establishing an effective industry Traceback body; and
- Robust enforcement of the existing and recently tightened General Conditions so that all invalid and spoofed CLIs - including those originating in the UK are blocked.

1.3. Our view is that these approaches will see a very significant proportion of invalid and spoofed CLI calls being blocked in the UK network – as much as 90% of total problem calls in the first instance – and at an estimated cost to industry of £20-40m.

1.4. Only once these approaches have been implemented should Ofcom consider a wider intervention such as any variation of Stir Shaken. At that point, we consider the consultation's preferred approach would deliver only marginal benefits at best. Those would not justify a likely industry implementation cost of c£100m.

2. Introduction

2.1. We are grateful for the opportunity to submit our views on Ofcom's consultation on Calling Line Identification (CLI) Authentication. The consultation states that, while industry has done much to combat the problem of scamming more needs to be done. We agree with this.

2.2. The past few years have seen a significant increase in the volume of invalid and spoofed CLI calls entering the UK network from overseas which we see as the primary source of the problem (as measured by volume of calls). There are several reasons for this, including the difficulty of applying effective controls at the UK network boundary and the low operational cost for scammers to send high volumes of calls into the UK.

2.3. Ofcom and industry need to focus on removing ever more invalid and spoofed CLI calls entering the UK network from overseas. At the same time, Ofcom needs to ensure robust enforcement of the existing General Conditions so that all UK-originated invalid and spoofed CLIs are blocked or traced.

2.4. A measure of future success would see a material reduction of invalid and spoofed CLI calls in the UK network combined with an effective mechanism to identify how any of these calls are still reaching the public.

2.5. We believe that there are credible options for making significant reductions in the level of invalid and spoofed calls in the UK network. They are:

- Establish a robust industry Traceback mechanism so that the source of invalid and spoofed CLI calls, both from the UK and overseas, can be identified and the relevant CP (Communication Providers) held responsible;
- Block calls coming from overseas which have spoofed UK mobile CLIs or UK presentation numbers; and
- Ensuring that existing and future obligations on CPs as set out in the General Conditions are robustly enforced.

2.6. **Several CPs are now initiating work with the NICC to assess the viability of both a Traceback mechanism and international mobile CLI blocking**.

2.7. Spoofed and invalid CLI calls from overseas would be blocked at international gateways. Those that evade blocking would be subject to identification through a new Traceback mechanism, providing strong incentives on carriers to comply with their regulatory obligations. This would almost certainly be achieved in a far more cost-effective way than the approach set out in the consultation.

2.8. The approach we set out should be backed up by strong enforcement of the existing General Conditions. This would secure, amongst other things, a marked reduction in the level of invalid and spoofed CLI calls which originate in the UK.

2.9. By contrast, the preferred approach set out in the consultation (similar, in many respects, to the US implementation of Stir Shaken but with some clear differences) will deliver only very limited incremental benefits compared to what we are proposing as an alternative approach. In particular, there would be no additional blocking of overseas spoofed CLI calls beyond the existing General Conditions. It could facilitate benefits for a Traceback mechanism but at a cost which is disproportionate.

2.10. We also believe that implementation of the consultation's preferred approach could take in the region of five years. This would be significantly longer with a second implementation phase with a common numbering database. The long timeframe is due to the complexity involved and resources already devoted to projects which would have interdependencies with the consultation's preferred approach. However, at this stage further assessment would be required to verify this timescale.

2.11. By relying on Traceback as opposed to blocking overseas spoofed CLI calls at the international gateway, the consultation's favoured approach would allow significant traffic into the UK network. This would mean that action would be taken after the scammers have contacted their victim. This would represent a poor outcome for consumers in the short term before the benefits of Traceback are fully realised.

2.12. A successful implementation of our proposed approaches, backed up by rigorous regulatory enforcement, could see as much as 90% of invalid and spoofed CLI calls removed from the UK network at the point of implementation. The cost of implementation would likely be in the region of £20-40m across industry. This contrasts with the consultation's preferred approach which we believe would see less than 40% of invalid and spoofed CLIs blocked at a cost in the region of £100m.

2.13. We set out our views in more detail in the following sections.

3. Establishing a Traceback body in the UK is crucial but does not require STIR

3.1. We agree with Ofcom that an independent third-party Traceback body needs to sit at the centre of any approach to combatting invalid and spoofed CLIs. An effective mechanism could signal to CPs that non-compliance with blocking obligations will not be tolerated. This is particularly important given the recent tightening of the rules in the General Conditions which we believe will deliver significant results if properly enforced.

3.2. Such a Traceback mechanism will only work, however, if accompanied by two core principles:

- Participation in the body would need to be mandated; and
- Where persistent flouting of the General Conditions is established, there needs to be effective sanctions in place on the responsible CP.

3.3. The first criteria above would require a direction to industry by Ofcom. The second criteria would require a signal from Ofcom that it will take appropriate robust enforcement action against operators who are in breach of their regulatory obligations.

3.4. The US experience with the Independent Traceback Group (ITG) can act as a template for such a body, although we would need to adapt that model in light of our own specific national circumstances. Participation is mandatory for CPs at the direction of the Federal Communications Commission (FCC). This has led to ITG securing tangible results, in stopping scam traffic in the US network. This includes warning CPs about illegal robocalls with, recently 22 out of 24 identified CPs instructed to stop the flow of known scam calls.[1] Elsewhere an international gateway was effectively "suspended"[2] when the FCC ordered CPs to cease sending traffic through them.

3.5. One element which we believe to be unnecessary for an effective Traceback system is STIR. Indeed, the ITG has not had to rely on STIR to achieve positive results as it had been in operation for some time before STIR SHAKEN's implementation. A digital signature may add some value in increasing the ease of establishing where scam traffic has originated from. But that limited benefit would likely come at a disproportionate cost to industry.

3.6. Working through NICC and Ofcom, CPs can collaborate to develop new reporting and Traceback arrangements. These should make use of automation to allow faster responses and increase the volume of requests handled.

3.7. Tracebacks could be broadcast to the entire UK network or specifically targeted towards the upstream CP. Traceback data includes information which could be considered commercially sensitive, such as interconnect arrangements and customer identities. An independent body administering the Traceback process would hold such information securely, releasing it for enforcement purposes under request.

3.8. We envisage that the bulk of the work of this group would be conducted by the CPs themselves, with Ofcom involvement restricted to the two areas cited above.

3.9. Exploratory discussions have taken place between BT, Vodafone, Talk Talk, Gamma and VM02 to assess options for establishing an industry Traceback body. Those discussion indicate that there is sufficient common ground amongst the major operators to initiate a work programme to work out the details of how an approach would work in the UK.

3.10. We have accordingly approached NICC to put in place a programme of work to design a Traceback mechanism that would work in the UK. This would need to extend to the wider community of voice service providers across fixed and mobile networks.

[1] FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters | Federal Trade Commission

[2] FCC Accelerates Action Against Illegal Robocall Gateway Facilitator | Federal Communications Commission

4. We propose blocking more international invalid and spoofed CLI calls

4.1. The consultation sets out an approach which helps in the identification of the source of an overseas invalid or spoofed CLI call after it has entered the network and reached the call recipient. The problem with prioritising this approach is that, in the case of overseas-originated calls, the call may have already reached its target and the fraud may have occurred.

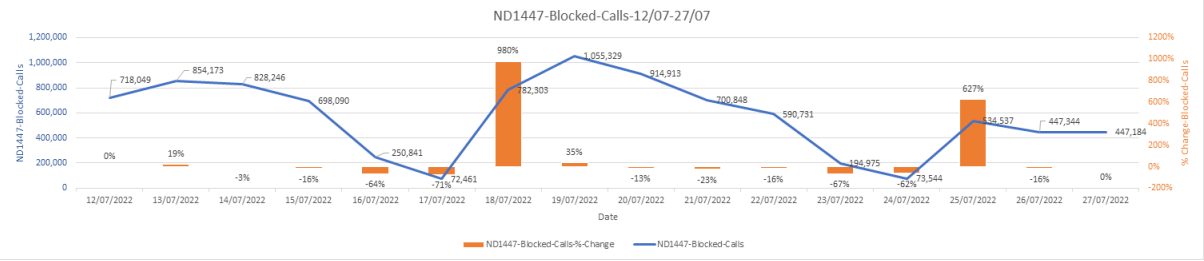
4.2. We agree that being able to trace the source after the call is crucial so that the CP can be identified and potentially sanctioned. However, more focus needs to be applied to stopping the calls from reaching their intended victim in the first place. This will minimise the number of scam victims in the short to medium term and until the benefits of Traceback are fully realised.

4.3. The consensus among industry experts is that the majority of scams originate overseas[3] although this is difficult to absolutely verify as we cannot measure the number of scam calls that successfully evade measures to block them. The consultation does refer to the overseas element of spoofed CLIs but does not set out the extent to which these are a driver of the overall problem. We note previous Ofcom statements on overseas fraud such as in 2022 when it noted[4] that numbering spoofing is a favourite tactic for Fraudsters based abroad[5]. The National Crime Agency (NCA) similarly estimates that "70% of frauds have an international component".[6]

4.4. Attested calls associated with the US implementation of STIR SHAKEN are not increasing significantly over time. This may be due to the limited use of IP-voice in the US, rather than the technology itself, but the evidence behind this remains unclear. The technology is, crucially, ineffective at screening international calls. Ofcom should, accordingly, assess what portion of fraud based on CLI spoofing the proposed intervention set out in the consultation will realistically address in the UK.

4.5. In July 2022, we started to block UK network and presentation numbers from entering the UK telephone network through our international gateway. The impact was immediate and significant:

Figure 1



Source: BT Analysis

4.6. Up to one million calls per day were being rejected from our network because of this blocking measure. Engagement with our CP customers showed that, with rare exceptions, this was unlikely to be legitimate traffic. The level of blocking has reduced over time, and we strongly suspect that scammers have attempted to circumvent our blocking measures. This would likely be by either moving to points of ingress in the network where blocking had not been implemented[7] or by spoofing UK mobile numbers.

---

[3] The UK Government itself acknowledging that 70% of all call and online scams have some international element (Fraud Strategy 2023 Tackling fraud and rebuilding trust (publishing.service.gov.uk) .)

[4] "New Ofcom rules to fight fake number fraud" New Ofcom rules to fight fake number fraud - Ofcom)

[5] Interestingly, this appears to be not just a UK phenomenon. The US Industry Traceback Group reported that 65% of the voice service providers identified as transmitting illegal robocalls were either foreign-based or gateway providers (2022, FCC CLOSES DOOR ON INTERNATIONAL ROBOCALL SCAMMERS, DOC-383499A1.pdf (fcc.gov)

[6] Progress combatting fraud (parliament.uk)

[7] Revised General Conditions C6 was implemented on 15th May. As a result, all CP should now be blocking overseas UK network number CLIs from entering the UK network -with agreed exceptions.

Presentation numbers

4.7. Current General Condition C6 requires CPs to block overseas calls that have a UK Network Number (with specific exceptions) but does not make the same obligation on Presentation Numbers. We argued as part of our response to the 2022 consultation *Improving the accuracy of Calling Line Identification (CLI) data* that this obligation should extend to Presentation Numbers. We repeat that view in this submission. BT is already going beyond the provisions of the General Conditions by blocking fixed UK Presentation Numbers.

4.8. Most numbers that we blocked from July 2022 when we implemented our new international blocking measures had both a UK Network and Presentation Number. We are conscious, however, that a scammer could choose to evade blocking on non-BT gateways by using a (possibly legitimate) international Network Number but with a UK Presentation Number.

4.9. Ofcom outlines in paragraph 4.30 the possibility of consulting on blocking Presentation Numbers through amending the General Conditions. We would support this. This would not necessarily be based on removing an existing problem but on removing a future option for scammers. Ofcom has, in that respect, long considered the challenge of preventing scamming as staying one step ahead of the scammers. In other words, we would propose removing the option of spoofing overseas Presentation Numbers before scammers use that to evade other blocking measures.

Mobile CLIs

4.10. The consultation refers only briefly to the limitations of ND1447 in that it currently only applies to blocking fixed Network Number CLIs. While difficult to verify, we strongly suspect that the gradual reduction in the numbers of overseas invalid and spoofed CLI calls being blocked by BT after July 2022 was due, in part, to scammers switching to mobile UK CLIs. Our view is a successful implementation on blocking these numbers would have a material impact on the quantity of spoofed CLIs entering the UK network.

4.11. There is a clear challenge in successfully implementing this as, unlike with fixed numbers, mobile devices may, by default, have a legitimate reason for use outside the UK. As the consultation sets out, other countries are now implementing solutions which are appropriate for their specific circumstances.

4.12. Exploratory discussions have taken place between BT, Vodafone, Three, Talk Talk, Gamma and VM02 to assess options for blocking UK mobile CLIs originating overseas and which are not roaming. Those discussions indicate that there is sufficient common ground amongst the major operators to initiate a work programme to work out the details of how an approach could work in the UK.

4.13. We have accordingly approached NICC to put in place a programme of work to explore the viability of implementing a mobile CLI blocking mechanism. Clearly, any mechanism would need to be supported by all MNOs and MVNOs.

4.14. These combined measures for additional international CLI blocking are critical in making real progress in reducing spoofing if we accept that a significant majority of spoofed calls are originating overseas. It represents a more effective way of addressing the primary source of the problem and would likely be of a much lower cost burden to industry than the approach set out in the consultation.

4.15. In terms of timing, it is unclear at this stage when these solutions could be implemented but we would expect them to be in place earlier than any implementation of the consultation's preferred approach (which, as we explain below, could be in the region of five years.)

4.16. We will also need to take account of the global moves toward VoLTE networks in any decision on how and when we implement any additional overseas mobile blocking measures. This is because VoLTE will significantly simplify the process for blocking invalid or spoofed mobile CL attempting to enter the UK network. We will, however, need to assess the timing of 2G and 3G switch-offs internationally to understand when those benefits would accrue.

5. The benefits of STIR would likely be minimal

5.1. The consultation otherwise focusses to a great extent on the benefits of its preferred approach, which we refer to as STIR. While the majority of scam calls likely come from overseas, this does not reduce the importance of stopping domestic scam traffic. We are, nonetheless, unconvinced that STIR is as effective as the consultation suggests. This is for three reasons:

- The new General Conditions, which came into force on 15 May, have considerably tightened the rules on operators blocking calls into the UK. Consistent and robust enforcement of those rules should materially reduce the instances of UK-originating invalid and spoof CLI calls. The key issue which needs to be addressed is dealing with CPs who flout those rules. As we set out above, an effective Traceback system is key to this but this does not need to be underpinned by STIR;
- It allows overseas spoofed mobile CLIs into the UK network; and
- The obligation to block would rest on whether the call has been attested by the originating provider. This is a binary process and contrasts with the US system where levels of confidence are reflected in the attestation process. We are unclear what this achieves in practice apart from being a helpful add-on to a Traceback process.

5.2. The Irish communications regulator, Comreg, recently published its own proposals[8] on combatting telephone and SMS scams. In that consultation document, it dismisses STIR SHAKEN on the basis that it will not address the problem of international invalid and spoofed CLI calls. Comreg states that the only way for STIR SHAKEN to be effective is with coordinated implementation at a global level. We agree with this assessment.

5.3. Given the consultation's version of STIR similarly does not effectively address the prevalence of overseas spoofed calls entering the UK Network, we would argue that the same principle applies here.

5.4. This is not to make the case that STIR, as proposed, would deliver no improvements in blocking UK originated spoof calls. Rather, we are convinced that the gains would be marginal compared to a more rigorous enforcement of the existing obligations and not commensurate with the high costs of implementation. We recommend that the possibility of a simpler non-STIR based call origin ID in the call signalling is investigated as part of the NICC work on Traceback.

5.5. Implementation of the consultation's preferred approach would likely be over a long timeframe. We believe that full implementation of CLI authentication across the UK will take in the region of 3-5 years, but most likely around 5 years. It is difficult to be precise on this timeframe at this early stage but we believe this to be plausible.

5.6. The design, deployment and full rollout of STIR would be a major delivery project for all CPs that implement it, requiring procurement processes, establishment of multi-skilled teams in the specialised subject area and deployment of new solutions to be operationally supported in the network.

5.7. We believe this is not just the case for BT, but more generally across Industry. There are a number of other factors that lead us to this timeline view:

- Timing of the closure of the PSTN and TDM networks;
- Replacement of legacy VoIP technology that won't support the preferred solution. BT has some key platform components in this situation, and we believe it likely that some other CPs could be likewise. This adds to the scale of the project; and
- Likely requirement for extended trials and phased introduction period that is likely to be required for this complex solution.

[8] ComReg consults on combatting scam calls and texts | Commission for Communications Regulation

6. Illustrative assessment of the effectiveness of the two approaches

6.1. We have attempted to set out, at an illustrative level, the likely effectiveness of both the consultation's preferred approach and our approach of enhanced international blocking with an industry Traceback mechanism. In doing so, we have been mindful that there are uncertainties that underpin this assessment and so we have had to use the most reasonable assumptions based on the evidence that is available to us.

6.2. This assessment is based on numbers of calls being blocked or identified on the network as opposed to any consequent harm suffered by the victims of the consequent fraud.

Assumptions in this assessment

6.3. The following are assumptions which we believe to be broadly plausible, based on best evidence available. They assume that GC6.6 has now been implemented in full and is being enforced.

Overseas calls

- 60%[9] of invalid or spoofed CLI calls on the UK network originate overseas;
- All overseas scammers have moved to mobile CLIs or UK PNs to enter the UK network as fixed UK CLI Network Numbers are being blocked;
- Blocking UK Presentation Numbers and mobile UK CLIs originating overseas would lead to ~90% of all overseas invalid and spoof UK CLI calls being blocked (on the basis that no system is 100% perfect).

UK calls

- 40% of invalid or spoofed CLI calls on the UK network originate in the UK;
- 90% of all UK originated invalid CLI calls are being blocked (on the basis that no system is 100% perfect).

These assumptions lead to the following outcomes:

Figure 2

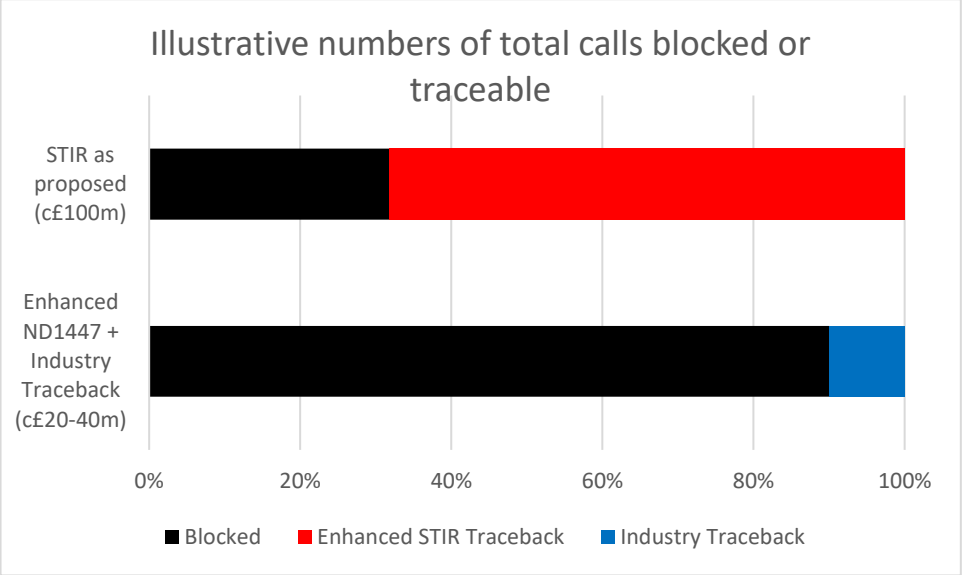
	Consultation approach	*BT approach*
UK-originated invalid and spoofed CLI calls	90% of calls are blocked 10% of calls can be identified through a STIR-supported Traceback system	90% of calls are blocked 10% of calls can be identified through an industry Traceback system
Overseas-originated invalid and spoofed CLI calls	All calls enter the UK network, but source can be identified through a STIR-supported Traceback system	90% of calls are blocked 10% of calls can be identified through a industry Traceback mechanism

Source: BT Analysis

6.4. The below sets out this impact. In summary, c90% of total calls could be blocked in our proposed approach in contrast with over c36% in the consultation's preferred approach. If we accept that STIR would lead to marginally easier Traceback provisions, we could conclude that the consultation's preferred approach could lead to marginally better Traceback for a larger number of calls. However, the approach we are setting out would block far more numbers from entering the network in the first place.

[9] Previous calculations of this figure have suggested a higher proportion, but we are taking a more conservative view for the purposes of this assessment and in light of the lack of certainty on the actual level.

Figure 3



Source: BT Analysis

6.5. We have included estimated costs for implementation of the two approaches in the above graph. However, given the lack of detailed information, these estimates will be necessarily speculative. Given the cost of implementation of STIR in the US was in the region of £500m, we believe that the magnitude of costs for a UK implementation would be in the region of £100m[10]. An initial estimate of the cost to industry of implementing enhanced ND1447 with an Industry Traceback system would be in the region of £20-40m.[11]

10 This is based on a US:UK population ratio of 5:1 reflecting the level of calls made on the respective networks. We cannot know with any precision how accurate this is until further investigation is taken by Ofcom. However, we suspect that fixed network costs may play a greater part in the total figure than we are assuming. This would suggest that £100m could be a conservative estimate.

11 This is based on a BT estimate on necessary systems development. This constitutes £1m for each MNO and MVNO and an additional £500k for each international gateway operator.

Annex 1: Consultation 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 agree with Ofcom's description of the way number spoofing is used.

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.

We agree that more needs to be done but disagree with the approach that the consultation has set out. As we set out above, the best approach to stopping spoofed calls on the UK network is through a combination of enhanced international blocking and an industry Traceback body. The latter approach would not necessarily require any element of STIR to be sufficiently effective.

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

The approach to CLI authentication as set out in the consultation is likely to be technically feasible and workable. However, we believe that there are better approaches that would deliver far better results for consumers. These should be explored by industry and Ofcom in the first instance.

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.

This approach would deliver *some* benefits. For example, it would clearly enhance any Traceback mechanism by making it easier to identify the source of invalid or spoofed CLI calls. However, as we set out above in more detail, a combination of enhanced international blocking and an effective industry Traceback body would deliver far better outcomes. It would remove bad traffic from the network in the first place while identifying the source of invalid and spoofed CLIs.

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

Our proposed approach would require robust enforcement of the existing General Conditions to ensure that all CPs are sufficiently incentivised to fulfil their regulatory obligations. This is particularly important in the case of scamming as the scammers will always be looking for a weak link in the network to exploit.

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?

As we set out above, while the rules may be fit for purpose for STIR, we do not consider that this is fundamentally the right approach.

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 this could be the case and is the one clear benefit of the proposed approach. However, our view is that there needs to be more focus on stopping invalid and spoofed CLIs from entering the network *in the first place*. That is why we have set out what we believe to be far more effective measures which could see c90% of all invalid and spoofed CLIs blocked.

While CLI authentication could improve Traceback mechanisms, the likely costs involved do not justify the limited benefits. Together with our MNO industry colleagues, we have initiated a workstream which will assess options for an industry Traceback mechanism. We would seek to make this at least as effective as that proposed in the consultation.

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

As we set out above, we believe that the timescales for implementation for CLI authentication could be in the region of five years.

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

While the administrative steps for any implementation appear broadly plausible, our view remains that CLI authentication is the wrong approach to follow. Ofcom should support industry in focussing on the measures that we propose in this submission.

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 leading on (a) the specification; and (b) the implementation?

While a common numbering database could support the implementation of CLI authentication, we do not consider that CLI authentication is the right approach to reducing invalid and spoofed CLIs on the network.

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 categories of cost and benefits proposed in the consultation but recommend that Ofcom:

- Assesses a wider range of policy options in the impact assessment, including the alternative and preferred approaches presented by BT and industry; and

Ofcom's final decision is based objectively on net benefits to consumers, which is a function of the portion of invalid/spoofed calls being blocked. Ofcom provides no initial guidance on which approach to cost-benefit analysis (CBA) will be used, but given that this intervention involves private investment, but public benefit, we recommend that the Spackman Approach is used[12]. This accounts for industry's cost of financing the initiative at its relevant cost of capital and at a time when capital is constrained by next generation network deployment.

The consultation's preliminary estimates suggest that the "total losses from scams using spoofed phone calls could plausibly be in excess of £100m annually"[13]. Using this figure as an initial estimate and assuming that the losses from scams using spoofed calls are proportional to the number of these calls, the high-level results of the CBA would be as below.

Table 1: CBA and high-level assumptions for policy options using the Spackman Approach over a ten-year timeframe.

	Consultation approach	BT approach
Upfront capital cost to operators	£100m	£40m
Capital cost conversion to annual annuities, 10 year review period	£15.7m	£6.3m
Annual opex and maintenance	£10m	£4m
WACC	7.8%	7.8%
Social Rate of Time Preference	3.5%	3.5%
Impact of policy on number of calls blocked	36%	90%
NPV of net social benefit, 5 year review period	**-£21m**	**£269m**
NPV of net social benefit, 10 year review period	**£71m**	**£603m**
NPV of net social benefit, 15 year review period	**£146m**	**£884m**

Source: BT analysis

This analysis is done for illustrative purposes, but it does highlight that we expect the NPV and benefits to consumers of our proposed approach to be orders of magnitude higher than STIR as proposed by the consultation.

The difference in expected upfront costs is significant, as is the cost to finance it. We have little data in this initial phase of the concept to make an accurate estimate on the ongoing annual costs of each option, so we have used a 10% of upfront cost figure for simplicity and to illustrate the concept. However, even if we ignore the costs for this reason and focus on the benefits, then the conclusion is the same. The benefit to the consumer is if the call is blocked. If the majority of spoofed calls still reach consumers, then even if the call can be traced the fraud will still take place, limiting the benefits of STIR.

[12] Ofcom, Research (ofcom.org.uk)

[13] Ofcom's final decision is based objectively on net benefits to consumers, which is a function of the portion of invalid/spoofed calls being blocked.

As robust data is still being gathered and the costs/benefits are uncertain, we have provided a sensitivity analysis table to show the range of possible outcomes under different capital costs and effectiveness of intervention.

Table 2: NPVs of net social benefit based on upfront capital costs and percentage of calls blocked using the Spackman Approach, £m, 10-year review period

	Cost to industry (£m)						
		20	30	40	50	75	100
Percentage of spoofed calls blocked	20%	112	91	71	51	0	-51
	30%	188	167	147	127	76	25
	36%	233	213	193	172	121	71
	50%	340	319	299	279	228	177
	60%	416	396	375	355	304	253
	75%	530	510	489	469	418	367
	90%	644	624	603	583	532	481

Source: BT Analysis

The initial estimates suggest that STIR will need to be at least 30% effective in reducing scams to produce a positive business case. Even though initial estimates suggest that its benefits will be in this region, the business case is marginal and uncertain, and we expect its net social benefit to be substantially lower than other policy options.