Consultation response form

Consultation on revised guidance on Consent to Charge

Please complete this form in full and return by email to consultations@psauthority.org.uk or by post to Mark Collins, Phone-paid Services Authority, 40 Bank Street, London, E14 5NR.

Full name	[redacted]
Contact phone number	[redacted]
Representing	Organisation (delete as appropriate)
Organisation name	aimm – Association for Interactive Media and Micropayments
Email address	[redacted]

If you wish to send your response with your company logo, please paste it here:

We plan to publish the outcome of this consultation and to make available all responses received. If you want all or part of your submission to remain confidential, please clearly identify where this applies along with your reasons for doing so.

Personal data, such as your name and contact details, that you give/have given to the PSA is used, stored and otherwise processed, so that the PSA can obtain opinions of members of the public and representatives of organisations or companies about the PSA's subscriptions review and publish the findings.

Further information about the personal data you give to the PSA, including who to complain to, can be found at psauthority.org.uk/privacy-policy.

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how the PSA handles your personal information and your corresponding rights, please see our privacy policy.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential?	Delete as appropriate: Nothing
Your response: Please indicate how much of your response you want to keep confidential.	Delete as appropriate: None
For confidential responses, can the PSA refer to the contents of your response in any statement or other publication? Your identity will remain confidential.	N/A

Your response

Please enter your response to each of the consultation questions in the appropriate box below.

aimm welcomes the opportunity to respond to the Phone-paid Services Authority (PSA) consultation on revised guidance to Consent to Charge. To assist aimm in providing a comprehensive input to the Phone-paid Services Authority, aimm communicated with its Members in the following manner;

- Written input from Members
- One-to-one telephone discussions
- Conference calls
- Individual meetings

Information gathered from all those who attended/submitted feedback in all these ways is presented below.

aimm Members who operate in the Phone Paid Services markets are broadly split into seven categories although there is some overlap inside individual Member businesses.

Fixed Line Networks who are often Fixed line L1

Mobile Networks

Mobile L1 aggregators

L2 providers of traditional PRS services (fixed line, PSMS, and DCB)

Broadcasters (who are often L2 providers)

Charities and Charity enablers (who are often L2 providers)

Industry Support companies

aimm sought responses from Members mainly across the L1 community but also received feedback from some Mobile Network Operators, Level 2 providers and Industry Support Businesses (specifically in the area of Anti-Frand/Compliance/Verification) and in this paper varying views are represented.

Some of aimm's Members may input their response directly to the PSA through their regulatory staff or regulatory representatives. Wherever possible, we ensure that views of members made through independent responses are in synergy with aimm's collective views.

As our response is guided and supported by Members input, some views may be expressed that are not necessarily those of the aimm Executive or aimm's Board of Directors

Overview

Consulted Members are keen that accepted standards apply to phone-paid services in order that they be seen by consumers as a credible alternative to other payment types.

There was some discussion across the Membership consulted around the consultation document and whether it should be in fact two separate consultations, one on Consent to Charge and one on Platform Security. Two issues are being covered here. Data from the subscription services consultation is being used for the Consent to Charge piece and findings from the Copper Horse research are being referred to for Platform Security. Whilst it is agreed that an unsecure platform could pose a risk to consent this is not the same as consent to charge rules.

Proposals under the heading of Questions 1 and 2 are generally less contentious with Members (mainly due to the acknowledgement of legal obligations and consumer rights), though are not without their own concerns and questions; however the push back on Security is stronger. Members understand that much work has gone into the Copper Horse project, and that findings from this are covered off, in the main, in contractual relationships between Mobile Network Operators and their partners. However there is a general feeling that as Guidance, the proposals should be less prescriptive (a phrase you will see repeatedly throughout this response). The PSA are charged at some points of overstepping their remit as a consumer protection body, that claims to regulate with an Outcomes led code, in a fair and proportionate manner. Some Members also feel that the ICO are better placed to regulate in some areas around data security, being the regulatory experts in this field.

There are Members that firmly believe that this consultation should have been proposed prior to the Phone Paid Subscription Services Consultation, and then been allowed to 'bed in', in order to

address the main complaint which the PSA receive - "I didn't sign up for this". This would've then mitigated the need for the onerous Special Conditions that have occurred as a result of the Subscription Consultation process – particularly for some industry sectors that were acknowledged to have caused negligible levels of complaints, such as Charity donations.

One Mobile Network Operator feels confident that the Security Research Project remains one of the best pieces of collaborative work in the value chain with those involved moving from a poor understanding of the requirements of a secure payment environment to radical reform; and that some really good news stories will emerge from the compilation of risk registers and the second security declaration sign off. They do have a concern that historical reading may be out of context as the project moves on. They note that as a Guidance document, the guidance has come with significantly more teeth than has been seen in previous Guidance notes - which may make the value chain nervous, particularly in respect of Point 57 which states that: "*a failure to demonstrate that the expectations within Guidance have been met, either by compliance with the expectations or by properly evidenced alternatives to achieve the same result, may result in a PSA Tribunal refusing to accept any transactions carried out on a platform as having valid consent".*

Finally, the majority of Members consulted were in agreement that consultation after consultation, one after the other, is becoming prohibitive to industry growth and the ability of the individual business to get on with their day job.

Consultation questions	**Your response**
Q1. Do you agree with our definition of informed consent at paragraph 1.4? If not, why not?	Confidential? No Partly. It was generally agreed that the definition was clear and well organised and there was overall approval for the wording used in 1.4. There was however a question mark raised by some Members around the definition of the phrase 'tamper-proof'. Some discussion was had as to the absolute characterisation of a 'tamper-proof' record, in that it this is difficult to prove. There is no standard for 'tamper-proof' making this an impossible criterion to comply with. Some Members would like to receive clarification from the PSA on the burden of proof required here. L1's believe that as an outcome, data records should be robust. There should be an acknowledgement that L1s would not tamper with their data as that would be illegal, but attempting to make records 100% tamper – proof likely is impossible and achieving (for example) a

	military-grade standard could have disproportionate cost and resource implications. Members all believe that the expectation should be that the data records would be robust, and that there are security measures in place to achieve this. If there is a third party security standard that the PSA could suggest (which is industry accepted/best practice) this would be useful as a best practice guide rather than Guidance. Additionally, there were concerns raised about the term 'independently and easily auditable records'. Members seek more clarification on what is acceptable under this heading. Is a data extract from a database enough? Will the PSA look to come on site and view records? Will access be given to an independent party to interrogate? Or is this referring to records being held using an independent storage resource such as Amazon S3? Some of the record requirements may contain sensitive data which individual businesses would be naturally cautious about handing over. Understandably the uncertainty in this area is causing concern. An outcomes approach is generally well received and where the outcome is described prescriptively this is also acceptable. However here the PSA are prescriptively informing industry about **how** they should be achieving these outcomes, which is very different. Representations from outside of the L1 sector - specifically in the Anti-Fraud market noted that 1.4, and indeed much of the Introduction to the consultation – could be more succinct by simply presenting the law around Distance Selling as per any payment mechanism, as well as consumer rights in this area. By laying this out, this covers off the reasons why informed consent is essential – which is not to satisfy the PSA – but to comply with legal requirements. They feel that this would show that the PSA are conversant with other regulatory areas, rather than working in isolation and that - as this is the law, the Guidance is reinforcement, not new regulation. L1s question the process of proving informed and robust consent where they do not handle the payment pages and seek clarification as to who is responsible for screen grabbing/witnessing the pages in these

	situations. If an L1 – in their relationships with their clients – trust them to provide robust verification of purchase then they will pass that responsibility down the chain, through a contractual process. L1s feel that putting the responsibility on them will be prohibitive. These Members feel it would be sufficient to cover this off in the agreements held between the two parties or with their chosen Verification company.
Q2. Do you agree with the changes to Section Two of the Guidance at paragraphs 2.9 to 2.13? If not, why not?	Confidential? No Not all. Throughout the L1 community, it was agreed that some processes and flows of this nature are already in place. However, some L1 and L2 Members had the view that, because the PSA don't offer products to the market, their knowledge is limited to what is in practice at any one moment in time. This could make for a limitation of options for industry to utilise as technology moves on and other options make themselves known. Some Members suggested that in their view, Special Conditions prescribe the "how", and Guidance focuses on the "what". As such, this feels more like a precursor to Special Conditions, and doesn't read like a Guidance or Best Practice document. Whilst there is an awareness that the PSA are open to hearing about new technology and potentially operating a pilot to test the resilience of such technology, there is a concern that without the in depth technical understanding required here, there may be an inherent distrust for new methods proposed in this area. This in turn will stifle innovation. Innovation in itself involves uncertainty, and to encourage innovation and commercial growth, pilots need to be very easy to introduce. Making the introduction of a pilot easy to bring to fruition would be very valuable to the market, so perhaps the PSA could look to minimise risk in another way (maybe capping initial revenue?) whilst encouraging the introduction of new technology that seeks to prove a new model. Bringing new opportunities into this sector, by having complex boxes to tick to gain

	approval for a pilot feels like one too many hoops to jump through. Additionally, due to large brand app store sign ups that happen when consumers turn on their phones for the first time, Members running smaller businesses feel that this makes it difficult for them to compete as they can't serve the same pages to their customers. One Verification Company Member noted that whilst Consent to Charge is being nailed down here -where there is a consumer present- they are disappointed that at no stage is third party security verification recommended. As 'button pressing' can be done by malware this will continue even after the introduction of PIN flows if it is a fraudulent transaction with no consumer. They note that Credit card companies have independent third parties looking at how transactions occurred and that by having that level of verification, records may become more 'tamper-proof, independently and easily auditable'. They note that it should be stated in Guidance that an anti-fraud solution should be part of the payment process. Whilst this question only covers 2.9-2.13, one L1 had a concern about 2.5/6. They noted that whilst they appreciate the intention within these two points, they felt there was a danger in the way that -in particular- 2.6 had been explained. In 2.6 it states that malware on handsets – initiating MO messages - is extremely rare. They do not believe this is necessarily the case. Handsets are all hackable, but this is not always reported as it can't be detected. They would suggest the following amendment as a better reflection of the actual picture: There may be occurrences where a handset may be infected or an MO has been generated without the consumer's knowledge. In these cases the PSA will investigate on a case by case basis as per the Code of Practise. At 2.9, the use of the term 'reasonable' has been questioned in terms of PIN expiry. What seems reasonable for a business might not seem reasonable to the PSA. This is not clear here so there is room for doubt and potential investigation if this is not understood in advance.

	A couple of Members had concerns about 2.10 and worry that this option could be open to misuse, whereby spam SMS messages could be sent to database lists of numbers, and – being that they contain service name, cost and frequency – could trigger a positive response from a consumer who unwittingly received the message. At 2.12, we ask for clarification on the wording used. The sentence seems to suggest that the entering of a MSISDN to trigger a PIN is not required, but this could be read as the triggering of a PIN itself is not required. aimm would ask that the PSA confirm that a PIN is/is not required here. Clarification is further requested at 2.13. Can the PSA confirm if single purchases/donations are included in this point? Finally it was questioned whether point 71 refers to SCA verification. If this is the case then it should be noted that the implementation date of the 14th September has passed and PIN flow has not been introduced as part of additional verification in the UK.
Q3. Do you agree with the proposed Technical Expectations? If not, why not?	Confidential? No Partly. L1s consulted agreed that the Technical Expectations were in line with what they have encountered in their work with Copper Horse, though some feel that these could become outdated fairly quickly and that the PSA will need to follow through on their intention to review on a regular basis. It was also agreed that there should only be one Technical Expectations list, with no conflict or discrepancies across network or between contractual relationships that are already in place, and regulation. Members agreed that a technical standard is a good thing and that there should be an acceptable base level in order for mobile payments to be recognised as a credible payment alternative. Some are broadly happy with the listings in Appendix A, although this was acknowledged to be a very costly business. Achieving

	the standards has taken up time and cost, and the Crest Accreditation adds another layer of cost on top. L1 Members almost in their entirety strongly believe that the Technical Expectations of L1s are managed in their contractual partnerships with each Mobile Network Operator and do not need replicating in regulation. One Member disagreed with this however and felt that – whilst contracts are in place – these can be broad, making it difficult to apply sanctions if standards fall short of what they should, and that this needs to be detailed in regulation to ensure a base level of acceptable technical benchmark. Additionally, some Members stated that this guidance takes account of findings made by Copper Horse, which have not been made explicit thus not enabling businesses to carry out a risk/benefit exercise. Indeed at point 73 it was noted that 'Copper Horse 's testing, while not identifying immediate evidence of ongoing consumer harm, consistently identified weaknesses which could be exploited by rogue Level 2 provider merchants to fabricate consumer consent ". As such, some Members are troubled that this consultation is based on unknown findings of incidents that have not happened. With this in mind, these members also raise concerns about point 57 which states that whilst Guidance is not 'absolutely binding', a 'failure to demonstrate that the expectations within Guidance have been met, either with compliance with the expectations or by properly evidenced alternatives to achieve the same result, may result in a PSA Tribunal refusing to accept any transactions carried out on a platform as having valid consent.' Members do seek clarity on Appendix A and the Guidance that states that providers can meet expectations by alternative means than the others stated, but then follows this up with a prescriptive list in Appendix A of technical standards 'which the PSA expects all payment and/or consent verification platforms to have in place'. The concern is mainly around timeline for implementation. If the consultation closes on the 11th October and then responses must be reviewed and a standard written, this does not give much time before annual penetration testing is to be conducted before the end of 2019 (point 67. Additionally some Members feel that – as those impacted by this testing they should be involved in the

	PSA/MNO conversations on how best this can be achieved). Members sought clarification on the following in Appendix A: *'all platforms should be hosted strictly independently of any Level 2 provider'* In particular Members questioned whether this is an issue around L2s being able to exert a level of 'control/influence' on the verification platform through corporate linkage? There is an agreement that there needs to be a high level of awareness of Security in the field of mobile payments. As other payment facilities are tightening up security continually, mobile payments must keep up. Some Members however feel that this consultation should concentrate further on areas of fraud – where no consumer is present. One Member also suggested that there is a high level of risk with any adjudication piece that might occur following this Guidance. They state that an adjudication panel would need the services of a (potentially very expensive) expert compliance witness to independently participate in order to ensure that the process was robust. This expert would also need to be able to educate others on the panel in the complex technicalities that would be imperative to a fair process. With these costs being not insignificant, the PSA should clarify how they would intend to recover them (for example, only in cases where the breach involved the issue covered by the expert, and after considering whether the breach was intentional or reckless). One Member consulted suggested that a potential problem has emerged from these Copper Horse expectations, as follows; If the ideal scenario is for the L1 to host the whole payment experience, a part of that would be that the L1 should host all assets including Javascript files. If the L1s do host – this means they need to give the L2 ability to upload their content. It is believed that Copper Horse do not want to allow Javascript uploads as they see this as a security risk. The reality of course is that L1s would be working with contracted partners who would not upload malicious code, but if this there

	becomes a requirement for this to be checked prior to upload then this will have time and resource implications. Some Members queried the journey for those using SMS. Pages used to acquire customers into SMS build services are largely hosted by third parties. In this instance, there is an obligation to collect the same level of consent but the differential is that L1s don't host payment pages. In these cases the platform is hosted independently. The PIN may be provided but the pages in which the consumer enters the PIN and payment may be provided by a third party. So currently the L1s have a lot less to do in the SMS world. Some L1 Members have no intention to host SMS acquisition pages (assuming their DDRC indentifies their chosen partner as a trustworthy business) and require urgent clarification that this is/is not what is being asked of them. If this is the case then this needs to be explicit, will require long lead time, and a change to contracts and commercials.
Q4. Do you agree with the proposed Staffing and Training Expectations? If not, why not?	Confidential? No Almost in entirety, no. All except one Member (and all L1s) strongly oppose the proposed Staffing and Training Expectations as laid out in the consultation document. They feel that this is exceeding the regulatory remit to protect the consumer in a fair and proportionate manner, and is far from outcomes based. Members question whether personnel at the PSA who regulate this environment themselves have to have a set number of years of experience before commencing their employment? Indeed, it was suggested that by specifying a certain number of years of experience (rather than just a skill set) this is bordering on age discrimination. One member noted that the PSA don't go as far as to asset out the qualification and experience expectations for Compliance Managers, so this is not consistent with other areas meeting Code outcomes. One Member however felt that this is a security benchmark that should be reached as a minimum for

	those in the value chain that charges payments to your mobile phone bill. L1s are happy to step up to the plate and take more responsibility for operating compliant, trustworthy services but all strenuously believe that this is too onerous a request on them. In this industry, with businesses of varying sizes, this is limiting the market, being advantageous in the extreme to larger companies who may have traditional roles such as this in place. Smaller businesses – or indeed those starting out – may only consist of a few personnel. Perhaps even the CEO is the CTO and COO initially! Businesses with small numbers may not be able to afford a Head of Security position where individual staff wear many hats. This feels like a sizeable barrier to entry with costs far exceeding the £100,000 mark, and maybe reaching £200,000 when NI and pensions contributions as well as extra employment benefits and training are added to the suggested salary band expenditure. Additionally, all Members question the value of some of the accreditations mentioned in the Guidance. Back in 2016 the Higher Education Funding Council for England commissioned a major review into the way Computer Science is taught at UK universities due to rates of unemployment and 'concerns from industry about the skills, agility and work readiness of the country's Computer Science alumni'. Whilst this may now be being addressed, this highlights the risks of prescriptively narrowing the expectations put forward in Guidance so that providers are apprehensive about taking their own course which may actually deliver the outcomes in a better way. Equally it was felt strongly, amongst nearly all Members consulted that the PSA should not be prescribing Project Lead experience related to ISO and NCSC. If the Code outcome of demonstrating robust consent to charge is being achieved, how staff are trained and the qualifications they have are less important. Guidance recommending security training, rather than specifying particular criteria, would be more useful. Members feel that – with an outcomes based code, the PSA should be as light touch as possible where they can be, and here they are overstepping the mark in an area outside of their experience. This is prescriptive to a high degree. What would have been more helpful

	would've been research in this area and a Best Practice document for staffing security standards. Each business consulted felt that they know their staff – who may have no accreditation but may be at the cutting edge of security standards – and absolutely do not want the PSA to get involved in their recruitment. They themselves should have the autonomy to decide which personnel are best placed to meet the outcomes expected. In terms of training, there is much available other than that specified in the document. Whilst the sentiment of training staff makes perfect sense, again this is too prescriptive. Accreditation and training is a business by business consideration, depending on the requirements that each individual company need to run compliant services on a day to day basis. Members are concerned that in a case of genuine human error, companies will start to be judged on their training certificates and accreditations and propose that a set of suggested competencies would be a useful framework instead. One Member felt strongly that it should be mandated in this document that Security and Fraud should be a Director level decision and responsibility.
Q5. Do you agree with the proposed Risk Control and Incident Response expectations? If not, why not?	Confidential? No Not all. Businesses consulted agree with the concept of Risk Control and Incident Response, and all manage this within their own companies with agreed processes and procedures already. It was agreed that the processes within the document are more onerous than required and could be prohibitive for smaller businesses on a day to day basis. Members generally questioned what the PSA plan to do with this information. Will they have the right to audit these documents in the case of an error occurring? If this is guidance then it shouldn't be so prescriptive and shouldn't be used as a template of the only effective way of processing risk and incident response. Again a best practice guide – following research in this area would be more useful, rather than

	Guidance which -in reality- reads as if it is a set of rules, and has little understanding of how smaller businesses operate to manage risk. In parallel with this, some verification businesses felt that it would've been useful to detail the services they offer at this point. They do not find such Risk Control and Incident Response processes onerous as it is their modus operandi, where L1s may find this more arduous. Additionally, they felt that they could offer support in producing robust auditable records as an independent party. They did make comment however that it is the reputable businesses, seeking to offer trustworthy services – that record their risks and incident responses meaning that they may be penalised by the PSA for robust record keeping using their own evidence whilst the 'bad guys' carry on not reporting Risks and Incidents. In keeping with all tech platforms the expectation is that platforms will suffer numerous attempted hacks and attacks. Procedures for risk control and risk mitigation are essential to any payment and verification platform and good companies will adhere to well thought through processes. Those with good security and fraud prevention systems will likely highlight more issues than those using lesser detection systems. So, while Members agree there are best practice elements to be set out, there is significant IP which companies own by countering these attacks effectively. Maintaining a risk register and sharing the security data is not essential to achieve the Code outcome of robust Consent to Charge, and also depreciates a company's IP (competitive advantage) whilst adding an unnecessary administrative burden. Members agree that an internal register of issues and resolution should be kept as standard best practice. Once again there was a suggestion that Risk Control and Incident Response should be accounted for at Director level. One Member felt that well maintained risk registers will in fact prove to be very reassuring to industry and will allow it to grow. Some Members also felt it would have been useful if standards for other billing mechanisms had been referenced, and these Members ask if this has been researched and if so, could it be presented? With payment methods converging, it would be useful to ensure that mobile payments are as easy as others

	to manage in this area. If we have jarring and prohibitive processes it will naturally be harder to compete as a payment alternative. Members ask that the PSA research other payment mechanisms to understand what is available (and thus avoid reinventing the wheel). This would also help facilitate economies of scale where the same solution can be applied for phone paid and other mechanisms. Members are also concerned that in requesting credible estimates associated with costs and considerations in the areas of security, risk and incident response, the PSA has not run a comprehensive cost vs benefit analysis to enable the consultation to be assuredly proposed.

If you have any supporting imagery for your responses, you can paste them in your responses in the table above or here:

Submit your response

To send your responses to the PSA please email this completed form to consultations@psauthority.org.uk or by post to Mark Collins, Phone-paid Services Authority, 40 Bank Street, London, E14 5NR.