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
Organisation name	Vodafone UK
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: Remove my name
Your response: Please indicate how much of your response you want to keep confidential.	Delete as appropriate: None except: [redacted]
For confidential responses, can the PSA refer to the contents of your response in any statement or other publication? Your identity will remain confidential.	Yes

Vodafone Pre-response Statement

Vodafone is supportive of the need for the United Kingdom to have proportionate and balanced regulation in the Charge to Mobile market and we are supportive of the requirement for a clear Consent to Charge guidance as an output of the Security Research Project. This project was conducted during 2018-19) and was specifically researching the Charge to Bill/Direct Carrier Billing (CTB/DCB) platforms that are directly connected to the MNOs.

The guidance will work alongside the MNO created Security Framework Declaration (also an output) already is in place in the UK. It is important to clarify that all L1s signed their network specific Security Framework Declaration before the 31st March 2019 and are already required to deliver Charge to Bill/DCB payment platform security to this declaration.

The MNO Security Framework Declaration was only possible after the concerted efforts of industry to cooperate with both the PSA and MNOs and was entirely focused on the CTB platforms. Vodafone covers off the issue of fraudulent actors using Premium SMS (PSMS) by only accepting Mobile Originated messages that have been recorded using the Vodafone Mobile Switching Centre (MSC) as valid and by excluding subscription services from PSMS. Attempts to circumvent the subscription mandate are vigorously rebutted.

The Security Research Project conducted on behalf of the UK MNOs and the PSA started in 2018 was devised and delivered because it was evident that more work was required in the value chain to ensure that proper consent to charge on CTB is obtained from customers that is free from influence of unseen actors on the transaction.

It is clear from the work that Vodafone has conducted in parallel to the development of the Security Framework Declaration is that real time fraud prevention mechanics are required at the point of purchase to prevent malware, clever programming, advertising bots and corrupted Apps from implementing auto-subscription techniques. Vodafone calls on the PSA for the second time to require MNOs to implement this style of service and perhaps the first part of

taking this bold step forward in fraud prevention is to include it as a requirement for MNO CTB platforms in the upcoming Consent to Charge Guidance.

Your response

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

Consultation questions	**Your response**
Q1. Do you agree with our definition of informed consent at paragraph 1.4? If not, why not?	Confidential? No Vodafone agrees that this is fair representation of informed consent however the introduction of the phrase "tamper-proof" must be clearly defined because the inference behind this is that records are held in a block-chain style environment. Currently this style of record keeping is not available in the telecoms market.
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? Yes [redacted]
Q3. Do you agree with the proposed Technical Expectations? If not, why not?	Confidential? Yes [redacted]

	[redacted]
Q4. Do you agree with the proposed Staffing and Training Expectations? If not, why not?	Confidential? No Vodafone remains convinced that a business must remain free to make decisions based on perceived business risk. If a member of staff believes a security risk is present or is about to be introduced then the proper cause of action is to assess that risk and introduce mitigations to control it. The proper and correct process is to fully maintain the RISK Register mandated in the MNO Security Framework Declaration. If the risk identified then materialises it is incumbent on the business to respond to and neutralise that eventuality and refund (as appropriate) customers impacted but a business should not be prevented from taking business forward simply based on an identified theoretical risk. The PSA should make it clear if a risk was NOT entered into the Security RISK Register then it is the Senior members of the company who are directly responsible for this failure and not the Security SPOC employee. The employee will be subject to undisclosed pressure from the business to limit the published risk.
Q5. Do you agree with the proposed Risk Control and Incident Response expectations? If not, why not?	Confidential? No As the response to question four. The full implementation of the Security Framework Declaration provides for the active maintenance of the Security Risk Register and the PSA must hold the Director with signed responsibility for Security responsible for failures to maintain the Security Risk Register

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.