PSA
Phone-paid Services Authority

Statement following consultation on revised Consent to Charge Guidance

13 February 2020

Contents

About the Phone-paid Services Authority

1. We are the UK regulator for content, goods and services charged to a phone bill. We act in the interests of consumers.

2. Phone-paid services are the goods and services that can be bought by charging the cost to the phone bill or pre-pay account. They include charity donations by text, music streaming, broadcast competitions, directory enquiries, voting on TV talent shows and in-app purchases. In law, phone-paid services are referred to as premium rate services (PRS).

3. We build consumer trust in phone-paid services and ensure they are well-served through supporting a healthy market that is innovative and competitive. We do this by:

    - establishing standards for the phone-paid services industry
    - verifying and supervising organisations and services operating in the market
    - gathering intelligence about the market and individual services
    - engaging closely with all stakeholders
    - enforcing our Code of Practice
    - delivering organisational excellence.

Executive summary

4. The PSA expects providers of phone-paid services to put consumer interests at the forefront of what they do. This includes providers not charging consumers for a phone-paid service without their informed consent. Any charging that takes place without a consumer's fully informed consent can cause financial detriment and affect ongoing trust in phone payment as a payment mechanism.

5. During the financial years 2017/18 and 2018/19 approximately 90% of consumer complaints were about subscription services and a significant proportion of consumers who contacted the PSA stated that they had been charged without their consent or knowledge.

6. In response to these issues, we undertook a review and consultation in relation to subscription services. Following the review, we introduced new Special conditions for Subscription Services that came into effect on 1 November 2019. We expect that the Special conditions will raise the standards of phone payment and meet consumer expectations of engaging with phone-paid subscription services.

7. The changes were made to support consistency for consumers, create greater alignment between the consumer experience of using phone payment and of using other digital payment mechanisms, and set clear requirements for providers. We expect these changes

to be effective in reducing the risk of harm to consumers, particularly harm caused from inadvertent sign-ups.

8. Alongside this, we consulted on draft revised Guidance on Consent to Charge. The work on consent to charge was aimed at ensuring that Level 1 aggregator payment platforms are operated to high standards, that any consent platform weaknesses that could lead to consumer consent issues are addressed, and that providers ensure they have and can supply robust and auditable records of informed consumer consent for every charge to a phone bill.

9. In undertaking the work on consent to charge, the PSA and the MNOs jointly contracted an independent security consultant to test the security of payment platforms accredited by the MNOs. The security consultant, Copper Horse, conducted penetration testing on several Level 1 aggregator platforms at the end of 2018 and in early 2019.

10. Following this testing, Copper Horse made specific recommendations to the providers of each of the platforms tested, as well as making general recommendations in the form of technical standards and general best practice recommendations. Some of these recommendations have already been implemented through updated MNO requirements, and others form the basis of the revised Guidance on which we have just consulted.

11. We issued our consultation on 14 August 2019 and it closed on 11 October 2019. We received eight responses to the consultation from individuals and organisations expressing a range of views. These views varied being from broadly supportive of our draft Guidance to some which acknowledged the need for guidance but disagreed with parts of it.

12. We have considered all responses carefully and revised the draft Guidance accordingly. The finalised Guidance is published as Annex A to this Statement. A high-level summary of the key changes we have made are as follows:

    - **Section Two of the Guidance on wifi and 3G/4G journeys:** as consulted on, the Guidance set different recommendations for consumer sign-up journeys depending on whether the sign-up took place on wifi or 3G/4G. Through consultation, we received feedback from some respondents seeking clarity on our expectations and querying the differences and the rationale for them.

      To clarify, our expectations are the same across wifi and 3G/4G journeys. Therefore, we have updated Section Two of the Guidance.

    - **Section Three of the Guidance on staffing and training:** through consultation we received feedback that the Guidance consulted on was too prescriptive about staffing and training. Following the feedback, we have amended the staffing and training expectations to focus on the outcome sought and provided some examples of how this could be achieved.

    - **Section Three of the Guidance on technical standards:** in response to feedback that there are a range of ways that technical standards could be met, we have re-named this section 'Technical Expectations' and amended it to focus on the

outcome we are seeking to achieve, with some examples of how the outcomes sought could be achieved.

13. These and other changes made to the Guidance are set out in further detail in this Statement. The updated Guidance is published alongside this Statement[1].

14. We have received feedback expressing the view that some time may be needed to implement elements of the guidance, especially Section Three. We believe that the revised Section Two sets out expectations in more detail than previously, but that in view of the changes already implemented to comply with Special Conditions for subscription services, it is reasonable for this section to be effective immediately on publication.

15. We acknowledge that some providers may need to take some action to meet the expectations set out in Section Three of the Guidance. We have therefore decided that the deadline for completing implementation of any actions needed to meet the requirements of Section Three should be 12 weeks after the publication of this statement as this represents a reasonable timeframe for any changes to be made by providers. The PSA would encourage providers to comply with the expectations set out in Section Three as soon as they are able to, but no later than 7 May 2020.

Background

Current PSA regulatory requirements and expectations

16. The 12th Edition of the PSA Code of Practice, and subsequent editions, including the current 14th Code, have all contained a rule which reads as follows:

    Consumers must not be charged for PRS without their consent. Level 2 providers must be able to provide evidence which establishes that consent[2].

17. As well as the Code provision set out above, there is Guidance in place which sets out the PSA's expectations about how to meet that provision. This Guidance was last reviewed in 2014 as part of the development of the 14th edition of the Code of Practice.

18. Since that time, the PSA has seen an increase in consumers reporting that they did not provide their consent to be charged and that they did not sign up to the service in question. This was particularly prevalent in 2017/18 and 2018/19 in relation to subscription services which at that time made up over 90% of total complaints to the PSA, and for which Special conditions are now in place.

[1] The changes made in the updated Guidance published with this Statement (including various clarifications and re-ordering of some paragraphs) have not been marked as this would have created significant readability issues.
[2] In practice, consent can be obtained by any party within the value chain on the Level 2 provider's behalf.

19. In addition, during the course of PSA investigations the PSA has seen consent records (presented by either Level 1 or 2 providers, or third-party consent/verification providers) that have been found not to be tamper proof.

20. A number of changes have occurred over the past two to three years which supported the need for revised Guidance on consent to charge. These include that:

    - the MNOs mandated that an increasing number of service and content types must use payment platforms accredited by them
    - there has been an increase in the number of companies offering third-party verification services, not all of whom sought advice from the PSA before commencing operation (as is recommended)
    - the PSA saw a general rise in complaints about services using direct carrier billing.

Joint security testing of Payforit platforms

21. Given this context and our shared interest in setting clearer standards for phone payment platforms, the MNOs and the PSA agreed to jointly fund testing of the Payforit accredited Level 1 provider platforms, to:

    - provide a system for categorising the type and severity of identified weaknesses
    - identify any issues required to be resolved on individual Level 1 provider platforms
    - allow MNOs to evaluate their contractual controls
    - support PSA to evaluate its current requirements and expectations against general recommendations to determine whether clearer standards are necessary.

22. The company selected via a tender process to carry out the testing was Copper Horse, an independent security consultancy. Testing was carried out according to a bespoke penetration testing methodology, with the first round of tests taking place between May and July 2018, and a second round during December 2018 and February 2019.

23. All Level 1 providers accredited under the Payforit scheme were tested during this time. Following the testing:

    - Level 1 providers received feedback and recommendations for strengthening their platform security
    - the PSA and the MNOs received anonymised feedback on the Level 1 platforms
    - general recommendations were made by Copper Horse, and these have informed the Guidance that the PSA consulted on.

Developing our proposals for consultation

Copper Horse findings and recommendations

24. Copper Horse found some degree of weakness in all tested Level 1 provider platforms. This is not unusual, as all digital payment platforms will contain some kind of weakness from time to time. Such weaknesses may be either:

    - inherent in the platform; or
    - due to a platform weakening over time as technical standards surpass it.

25. While it is not unusual that such weaknesses were found, these findings support our assertion that both the Level 1 accredited payment platforms and consumers would benefit from the application of clearer and more detailed standards and expectations for phone payment platforms.

26. Copper Horse's final report made some general recommendations relevant to those who are involved or have an interest in the operation of payment consent platforms, whether Level 1 providers, third parties, the MNOs, or the PSA. These recommendations can be grouped into three categories:

    1. **Technical** – specific technical standards that platforms should adopt
    2. **Staffing and training** – clarifications of roles and responsibilities, and the training, qualifications or skills that are necessary for those roles to be carried out effectively
    3. **Risk control and incident response** – processes that enable risk to be assessed and recorded, and that allow for immediate, comprehensive responses to such risks or incidents.

27. The MNOs have already updated their accreditation standards to include most of these recommendations (excluding the recommended Technical Standards that the PSA set out in its consultation on proposed Guidance).

28. The new MNO requirements include that all Level 1 providers that are accredited by the MNOs, and all third-party consent/verification providers, must have their payment platforms fully retested on an annual basis by a CREST[3] accredited tester.

29. The Guidance that the PSA consulted on set out general best practice and technical expectations that all payment platform providers and third-party verifiers should meet when operating in the phone-paid services market.

30. In developing the proposals set out in the draft Guidance that we consulted on, we considered the recommendations set out in the Copper Horse report, as well as the

[3] CREST (The Council for Registered Ethical Security Testers) is a UK accreditation body which provides professional certification for security penetration testers. More recently, CREST has become a globally recognized standard.

evidence-based regulatory changes we have made in other areas to meet consumer expectations, build trust, and ensure they are protected from harm in the market, such as changes to the regulation of phone-paid subscription services.

31. The proposals were focused on ensuring that consumers will not be charged for a phone-paid service without their consent and on updating our Guidance to align with current best practice.

32. Following the closing of the consultation, the PSA has carefully considered the input received, both through formal consultation responses and informal mechanisms (such as industry engagement) and has amended the Guidance we consulted on as a result.

33. To note, the PSA engaged with a range of parties throughout the consultation process through bilateral meetings, as well as a workshop held between the PSA, the MNOs and Level 1 providers. The input and discussions as part of this engagement have also been considered.

34. The PSA also made clarificatory amendments to the Guidance consulted on to ensure that the expectations set out are clear.

35. An overview of the input received through the consultation, the PSA's consideration of this input, and the subsequent changes that have been made to the Guidance consulted on as a result are summarised in the next section. The amended Guidance is set out at Annex A.

Responses to our proposals

36. We received eight responses to our consultation, from organisations and individuals. The input to each question and on each section of the guidance varied significantly with some respondents being broadly supportive of the proposed Guidance, and others expressing that they strongly disagreed with aspects of the proposals as set out.

37. We have balanced the range of views received against the evidence in the Copper Horse report and other evidence such as complaint data, anecdotal evidence received through consumer contacts, and our understanding of consumer expectations gathered through formal research undertaken over the past 12 to 18 months.

38. Responses received, our consideration of these, and any amendments made to the Guidance as a result are set out below.

Input received on consultation Question one: Do you agree with our definition of informed consent at paragraph 1.4? If not, why not?

39. Generally, respondents agreed with the PSA's definition of informed consent (now set out at paragraphs 1–2 of the updated Guidance). There were a few specific areas where some respondents felt additional clarity would be useful.

40. Areas where clarification or additional detail was sought by respondents were in relation to:

    - **the definition of 'tamper-proof independently and easily auditable consent':** some respondents sought clarity on what exactly is meant by the expectation that evidence of the tamper-proof methods used to obtain informed consent to charge must be available on request
    - **the difference between the existing Guidance and the new Guidance**: one respondent was of the view that there is little difference between the two, other than that the updated Guidance is more prescriptive
    - **key information:** and what is required to be recorded as part of evidencing what the consumer saw when providing consent to a phone-paid services charge
    - **screen grabs:** whether the Level 1 provider is responsible for all screen grabs in evidencing what the consumer saw as part of the sign-up process, and expressed the view that if so, this would be prohibitive
    - **fraud:** one respondent commented that the measures set out in the Guidance should be combined with an anti-fraud solution, and that more detail is required around the methods considered acceptable for obtaining robust consent to charge. This respondent also suggested that the PSA provide additional information about the methods of consent that are more or less at risk.

PSA assessment of the input received on Question one

41. In response to the clarity sought on the definition of 'tamper-proof', the PSA has amended the wording in the draft Guidance consulted on to include wording from the existing Guidance, as follows:

42. *Providers should be able to demonstrate that such records show genuine consumer consent and have not been tampered with in any way since they were created. The provider should be able to provide PSA with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed) and real-time access to this opt-in data, upon request. This may take the form of giving the PSA password-protected access to a system of opt-in records.*

43. The Guidance sets out the PSA's expectations around informed consent for a range of different consumer journeys. The PSA agrees that the principles and rationale for having guidance in place which sets out expectations on consent to charge remain the same:

    - it is necessary for providers to ensure that consumers are only charged when they have requested and consented to a charge
    - it is important for the PSA to set out best practice expectations that remain up to date and will ensure consumer protection
    - guidance will support compliance with the relevant Code provision(s) around consent to charge.

44. With this in mind, updates have been made to ensure that regulation is aligned with technical and market changes that have taken place since the Guidance was first published.

45. Following the responses received, we would also like to clarify that our expectations are the same whether a consumer is using wifi or their Network Internet Provision (IP). In either of these circumstances we would recommend that one of the methods set out in the updated Guidance is used to obtain robust consent to charge.

46. In addition, where service types and charging methods have other regulatory requirements in place, such as Special conditions, the relevant regulatory requirements for that service type must be complied with. For example, for subscription services a double opt-in consent to charge approach that complies with the Special conditions must be used, and the passing through of a consumer's mobile number to obtain consent would not comply with those requirements.

47. The PSA considers that a two-stage opt-in approach represents best practice when obtaining robust consumer consent to be charged. As is the case with all Guidance, whether or not Guidance has been adhered to may be considered by a Tribunal along with other evidence when considering any cases presented to it involving alleged breaches of the Code. However, following Guidance is not mandatory and it is for providers to decide whether to align themselves with the expectations set out in Guidance or whether they consider there are alternative methods that they consider would achieve the same result.

48. Some respondents sought clarification about the key information that is required to be recorded as part of a provider evidencing what the consumer saw when providing consent to a charge.

49. Firstly, providers are required to take note of the PSA's Guidance on the Retention of Data[4] ('Data Retention Guidance'). This Guidance sets out that all parties involved in the provision of premium rate services should retain all Relevant Data[5] for two years as a minimum from the point it was collected. In addition, Relevant DDRAC Data[6] should be retained by Network operators and Level 1 providers for three years as a minimum, from the point at which it is collected.

50. Providers should give due consideration to the Data Retention Guidance and the definitions of Relevant Data and Relevant DDRAC Data when considering what information to retain as part of evidencing that robust and informed consent to charge has been obtained.

[4] PSA Guidance on the Retention of Data
[5] This is defined as all information held by Network operators and providers that relate to the promotion, operation, content and provision of any premium rate service and any other information that may be of evidential value to a PSA enquiry or investigation.
[6] This is defined as all records of an information relating to due diligence and risk assessment and control which a Network operator or Level 1 provider in relation to their clients and or service operated by them.

51. The updated Guidance sets out the ways that robust consent from a consumer can be proven, in a range of circumstances – from phone calls, to text messages and purchases initiated via websites. As the Guidance sets out, in all circumstances providers should be able to demonstrate consent through records that are easily auditable and have not been tampered with in any way since they were created.

52. The PSA considers that its expectations around informed and robust consent are clear and set out the best practice expectations for the key information that should be recorded to enable a provider to evidence what the consumer saw when providing robust consent to be charged.

53. One respondent asked whether the Level 1 provider is responsible for all screen grabs and expressed the view that if so, this would be prohibitive. In the PSA's view it is for the parties in the value chain to agree roles and responsibilities around collecting and retaining information that ensure compliance with the law and PSA's regulatory framework, including that the appropriate responsible party is able to evidence robust and informed consent to charge.

54. The PSA notes the input asking that the PSA provide further information on which consent to charge methods it considers to be higher risk.

55. In developing the draft Guidance, the PSA assessed each of the methods set out as having the potential to ensure that robust consent to charge is obtained, and as being in alignment with the Copper Horse findings.

56. However, it is up to the provider and contracted parties in the value chain to consider the opportunities and risks associated with each possible consent method. This should be considered in the context of the expectations set out in the Guidance, and an assessment made of the method(s) they consider to be most effective and appropriate to obtaining robust and informed consent to charge, with regard to the whole consumer journey and the service that they are offering.

Input received on Question two: Do you agree with the changes to Section Two of the Guidance at paragraphs 2.9 to 2.13[7]? If not, why not?

57. Input from across the responses included some specific feedback on the information that the PSA set out that it expects to be provided. This included a number of respondents commenting on different aspects of the expectations set out around the use of a PIN, including:

    - **PIN placement**: querying the expectation that the PIN must be placed underneath where the consumer enters their mobile number, as part of the sign-up process
    - **requiring a PIN**: seeking clarification on whether a PIN is required when a consumer's network IP has been used to browse and make a purchase

[7] Now paragraphs 16 – 28 of the updated Guidance

- **alignment across regulation:** seeking clarity on the alignment between the PIN expectations set out in this Guidance, and the Special conditions for subscription services which go further and require a PIN to expire after a certain time
- **PIN end-points:** noting that these should be protected through both device-oriented parameters and user-event data as these are verifying two different things.

58. The PSA received mixed input on the expectations set out around the use of mobile terminating (MT) messages. For example, one respondent questioned the expectation that the service name and the cost of the service be included in MT messages used as part of a sign-up process, whereas another respondent was generally supportive of this being allowed, but not required.

59. One respondent suggested that malware is not always rare, and that the PSA should therefore reconsider the wording of paragraph 1.6 of the Guidance consulted on (paragraph 14 in Appendix A) that 'in extremely rare occurrences a consumer's mobile handset may have been affected with malware'. Another respondent stated that all forms of consent to charge are open to the threat of malware, and it is for industry to assess and manage the risks associated with each.

PSA assessment of the input received on Question two

60. The updated consent to charge Guidance sets out the PSA's expectations about the use of on-screen PIN and PIN loop to obtain consumer consent to be charged. The PSA notes that there are differences between the methods set out in the draft Guidance as consulted on, and the requirements set out in other regulation instruments, such as the Special conditions for subscription services.

61. However, Special conditions for specific service types are deliberately more prescriptive as they are intended to reduce the consumer harm or risk of harm associated with particular service types. The updated Guidance sets out our expectations more broadly around obtaining consumer consent to be charged and is therefore less prescriptive.

62. In relation to PIN placement we do not expect or require that the PIN entry box is always directly underneath where the consumer enters their mobile number. We want to provide flexibility so that providers can design and implement sign-up journeys that ensure robust consumer consent to be charged, while being suitable for their particular service(s). The Guidance has been amended to reflect this.

63. The PSA has not made any changes to set out whether MT messages should or should not include the service name and cost. The PSA considers that it is best practice for MT messages to contain this information and so has kept this in the Guidance.

64. Regarding those responses that highlighted the potential risks associated with malware, we consider that it is for verification providers or platform providers to take steps to protect against malware. The PSA has updated the wording in the Guidance so that it is not providing any view on how rare malware may or may not be.

65. The PSA has set a base level of expectations about the types of technical expectations that it expects providers to meet. The draft Technical Expectations are discussed in the next section and set out at Appendix A of the Guidance.

Input received on Question three: Do you agree with the proposed Technical Expectations? If not, why not?

66. Some respondents broadly agreed with the proposed recommendations providing they are reviewed regularly to ensure they are kept up to date.

67. Other respondents expressed a number of different views, as follows:

    - **overly specific:** one respondent was of the view that if the PSA is too specific in setting out the Technical Expectations, they will be considered a minimum standard to meet

    - **potentially limiting:** another respondent thought that while the Expectations as set out may be effective, they are not the only ways for a platform to be protected. This respondent was of the view that because the Expectations are set out in Guidance and not Special conditions, the PSA would need to allow for other methods to be used

    - **responsibilities:** one respondent suggested that the Technical Expectations are already managed in the contracts between Level 1s and MNOs so not needed in regulation, but another disagreed with this and felt the Technical Expectations ensure a base level of acceptable technical benchmark.

PSA assessment of the input received on Question three

68. The PSA has considered the range of input received, and as a result has made a number of amendments to the Technical Standards. We have also amended the title of this Guidance to refer to 'Technical Expectations' as this more accurately reflects the role of Guidance in setting our expectations. The PSA agrees with the respondent that noted that putting Technical Expectations in regulation ensures that expected standards are met and so has retained these expectations.

69. The PSA understands that there may be a range of solutions available for providers to use to meet the objective of ensuring that platform architecture and settings are secure, and interface securely with web pages and external systems. As explained in the draft Guidance, the PSA also recognises that universal standards do exist as to the underlying software which a platform uses to operate, and the protocols with which it communicates and interfaces with web pages and other external systems.

70. The PSA has therefore updated the Technical Expectations at Appendix A of the Guidance so that it is clearer that some of the expectations can be met by a range of solutions. In some areas, examples have been provided to demonstrate how an expectation may be met. Some of the Technical Expectations remain unchanged as the expectation is already sufficiently broad to enable it to be met in a range of ways.

71. To confirm, the Technical Expectations in the updated Guidance represent the PSA's position at the time of publication. As was set out in the draft Guidance, the PSA intends to review the position annually to ensure its expectations continue to align with universal standards, reflect best practice and remain up to date with emerging technologies and approaches in the market.

72. The PSA notes the comment from one respondent about how adherence to the Technical Expectations would be considered in the context of enforcement action (such as a Track 2 investigation). The PSA would like to clarify that while Guidance is not binding, it sets out the PSA's expectations in relation to the relevant outcomes and rules referred to in the Guidance. In particular the Guidance clarifies the platform security measures the PSA would expect providers to have in place and be able to demonstrate in the event of any PSA enquiry or investigation into potential breaches of relevant Code rules and outcomes. The Guidance is provided to assist providers in their understanding of how the PSA interprets and applies the relevant Code rules and outcomes.

73. A failure by a provider to adhere to relevant Guidance may be taken into account by the PSA when considering whether or not the relevant Code rules and outcomes are likely to have been met, and can form part of the evidence of any alleged breach(es) that may be placed before a Tribunal. Where Guidance sets out the PSA's expectations as to how a Code rule or outcome can be met, a provider should be able to demonstrate that it followed published Guidance or, alternatively, that it implemented suitable alternative measures to meet the relevant Code rules or outcomes.

Input received on Question Four: Do you agree with the proposed Staffing and Training Expectations? If not, why not?

74. A number of respondents disagreed with the staffing and training expectations as proposed in the draft Guidance, with many expressing that they thought the proposals are too prescriptive. Specifically, input was received on the following issues:

    - **the role of security firms:** the view of some respondents was that there needs to be scope for independent security firms to undertake security risk management and control. In their view, such firms are more likely to have specialist skills and may be able to identify and respond to risks more quickly than internal staff.

    - **cost impacts**: one respondent indicated that employing staff who meet the expectations as set out would be a barrier to entry for smaller organisations.

    - **approach:** PSA should consider a set of core competencies rather than cited qualifications, and these should be best practice rather than mandatory

    - **decisions and risks are for businesses to manage:** some respondents expressed the view that it is up to businesses to take risks and ensure they are appropriately managed with accountability at the appropriate level (i.e. Director level). In addition, specifically related to staffing, one respondent expressed the view that companies need to have the flexibility they need to select staff they feel can

achieve the overriding objectives without strict requirements or experience being set out.

75. Overall, this was the one question where there was general agreement across industry respondents that the expectations as consulted on were too prescriptive and would have a negative impact on the ability of providers to make decisions about staffing.

PSA assessment of the input received on Question four

76. The PSA has considered the input received, and in response has updated its expectations around staffing and training so that providers have greater flexibility in this area.

77. This section of the draft Guidance consulted on is intended to ensure that providers across the value chain have suitably qualified and skilled staff. However, the PSA acknowledges that there are a range of skills and experience that a person may possess and with which they could fulfil the expectations set out.

78. The PSA agrees that approaches to staff training and the salary levels and experience required to fulfil a particular role are decisions for a business to determine. However, the PSA:

    - considers it helpful to provide recommendations and examples of the types of skills and experience that someone would reasonably require to fulfil a Head of Security (or equivalent) role
    - expects that organisations have a single point of contact with responsibility for fraud and security.

79. In response to the input received through consultation, we have amended the Guidance consulted on. We have clarified that all organisations involved in payment or consent verification are expected to have suitably qualified and senior staff who are accountable for ensuring ongoing and adequate risk management, identification and control.

80. We have also retained the expectation that each platform provider has a nominated single point of contact for emerging security issues and that when this person is absent the responsibility should shift to another senior member of staff.

81. In addition, the PSA has retained the expectation that Level 1 providers should have appropriate mechanisms in place to suspend or terminate payment facilities to any Level 2 providers or third-party verification providers. The PSA acknowledges that when such mechanisms are triggered is a decision for Level 1 providers. However, we would expect such mechanisms to be available to ensure consumer protection.

82. The draft Guidance set out that 'evidence of how a payment and/or consent verification platform has met the expectations … should be available for immediate, independent assessment by the PSA'. The PSA received queries about what was meant by this.

83. To clarify, this section was intended to re-confirm to providers that this evidence must be made readily available to the PSA as part of any investigation and as governed by our existing investigations and enforcement powers.

Input received on Question five: Do you agree with the proposed Risk Control and Incident Response expectations? If not, why not?

84. Respondents to this question had a range of different views to a number of issues. These can be summarised below as follows:

    - **the expectations:** some respondents commented that they consider the expectations too onerous and not needed as most providers can already meet expectations within the existing regulatory framework
    - **the template:** one respondent sought clarity on whether the template set out in the draft Guidance consulted on is mandatory
    - **information sharing and issues reporting:** one respondent sought clarity on whether providers' risk control and incident response information would be required to be shared with the PSA or the MNOs. This respondent also commented that all tech platforms suffer numerous attempts and hacks and it is not normal for a regulator to require all such issues to be reported
    - **third-party providers:** some suggested that there is a need for third-party provider and audit house roles to be set out and for clarity around whether third-party providers, not regulated by the PSA, are required to adhere to the Guidance
    - **Action taken following issue identification:** one respondent commented on the expectation set out in the draft Guidance that Level 1 providers should terminate a payment facility if they think there has been non-compliant activity, and that this causes issues where a Level 2 provider uses different Level 1 providers for different parts of the business.

PSA assessment of the input received on Question five

85. The PSA does not agree with the assertion that Technical Expectations are unnecessary, or that providers are already meeting expectations. As set out in the consultation document, a lack of robust consumer consent to be charged has been an issue over the last few years. In addition, the MNOs had also identified similar weaknesses in some platforms, through their own monitoring.

86. Copper Horse testing identified varying categories and degrees of weakness in all tested Level 1 platforms. The Technical Expectations consulted on were developed following consideration of the recommendations made by Copper Horse following that testing.

87. A number of respondents commented on the Technical Expectations in their input on this question. The PSA's consideration of this input is set out under consultation Question three, considered between paragraphs 66–73 above.

88. Following the input received, the PSA has made minor updates to the Technical Expectations to reflect the feedback received, and with consideration of the findings of the Copper Horse report. Key changes are as follows:

- all platforms should be hosted strictly independently (i.e. without the control or influence) of any Level 2 provider (including their officers, staff, representatives or other persons with significant control). Where a Level 1 provider wishes to offer services on its own platform then it must retain ownership, control and responsibility for all aspects of the service
- all platforms should use the current version of the Transport Layer Security (TLS) protocols or as a minimum version TLS 1.2
- authentication cookies should be encrypted by default on all platforms and expire within a reasonable amount of time. We recommend that providers refer to the Information Commissioner's Office (ICO) to ensure that any authentication cookies and expiry times are in line with relevant legislation and the ICO's expectations
- payment pages should protect against click-jacking. For example, by use of HTTP Headers on a browser-based transaction
- any phone-paid transaction should only ever occur over correctly validated connections.

89. The remainder of the Technical Expectations remain unchanged, or only minor typographical amendments have been made. This is either because they are already sufficiently broad to enable a range of solutions to be used to meet the expectation, or because the expectation can only be achieved in the manner set out.

90. Regarding the other input received, the PSA would like to clarify that the template provided in Appendix C of the draft Guidance consulted on sets out the information that the PSA would expect providers to collect. However, there is no requirement to use the template. It is intended to assist providers, but it is up to each provider as to whether or not they choose to use it.

91. The PSA has not set out expectations relating to third-party providers who are not regulated by us. It is a requirement in the PSA Code of Practice that robust consent to charge is obtained from each consumer prior to their being charged for a phone-paid service. The responsibility for providing evidence that establishes such consent lies with the Level 2 provider. Our expectations as set out in the Guidance consulted on is that where verification of consent is undertaken by a third party, this party must be independent of the Level 2 provider. This verification should only be undertaken on behalf of the Level 1 provider. Where a Network operator contracts directly with a Level 2 provider this function can be undertaken by the Network operator.

92. The PSA recognises that sometimes there are complex value chains in place which may include parties not directly regulated by us. While we would expect that any party in the value chain that is regulated by us to pay due regard to the Guidance (as it is such parties that are responsible for achieving the Code outcomes), we consider that it would be in the interests of such parties to ensure that any parties that are not regulated by PSA who they contract with also have full regard to the expectations set out.

93. One respondent asked whether the PSA would require risk control and incident reporting to be shared with the PSA and MNOs. With regard to the MNOs it would be for them to determine what information they would require, within the context of the regulatory framework.

94. Providers may be required to share information with the PSA as part of an investigation of a potential or alleged breach of the PSA's Code of Practice. The expectations set out in the Guidance have been done so under our existing powers and do not represent a shift from these.

95. The PSA acknowledges that it is for the Level 1 providers to determine when to terminate a payment facility. The PSA has amended the expectations it had set out to clarify that it expects all parties in the value chain to collect information to ensure they are able to understand and appropriately respond to any security risks or issues to ensure consumers are protected from harm.

96. Providers should take effective and appropriate steps if there is evidence of consumers being charged without robust consent. Providers should satisfy themselves that such steps are sufficient to protect consumers and to comply with the other relevant Code outcomes, particularly those relating to Due Diligence Risk Assessment and Control. This may include Level 1 providers taking steps to terminate a Level 2 provider's payment facility as they deem appropriate to ensure such outcomes are achieved.

Other input received

97. Some respondents provided input outside of the questions set out in the consultation. Where such input has not been addressed elsewhere in this document we have sought to do so in this section.

98. One respondent asked whether regular-giving platforms are exempt from this Guidance. We can confirm that no service type or billing mechanic is exempted from meeting expectations intended to ensure robust consumer consent to be charged. While there may be aspects of the Guidance that are only applicable to particular billing mechanisms, there are aspects of the Guidance that apply to all providers and mechanics, and other parts that are only applicable to particular parts of the value chain or mechanic.

99. The PSA notes that one respondent commented on the sequencing of the publication of Special conditions for Subscription Services and the consultation on the Consent to Charge Guidance. The PSA does not agree with any assertion about the order or approach we have taken to these two distinct pieces of work. The subscriptions review made necessary changes to the regulatory framework to meet consumer expectations of engaging with phone-paid subscription services, reduce consumer harm arising from such services, and grow trust.

100. This Guidance is intended to assist networks and providers in complying with the PSA Code of Practice requirements to ensure robust consumer consent to be charged is

obtained. It includes both expectations around informed consent and consumer purchase journeys across all service types and charging mechanisms, as well as expectations on robust payment and verification platforms.

Respondents

101. In developing this Statement, the PSA has considered the feedback, evidence and input received through responses to this consultation, as well as through engagement with stakeholders. The stakeholders who responded to the consultation and indicated that they were happy for their responses to be published, either in part or in full, are as follows:

1. aimm
2. Anonymous
3. Donr
4. Fair Telecoms Campaign
5. Hutchison 3G UK Limited
6. MCP Insights
7. Payforitsucks.co.uk
8. Vodafone.

Next steps and implementation

102. Following the consultation and our consideration of all of the responses and other input received, the PSA will be implementing updated Guidance on Consent to Charge. The Guidance is published with this Statement.

103. Sections One and Two of the Guidance are effective immediately. The deadline for completing implementation of any actions needed to meet the requirements of Section Three is 12 weeks after the publication of this statement, that is 7 May 2020. However, the PSA would encourage providers to comply with the expectations set out in Section Three as soon as they are able to.

GENERAL GUIDANCE NOTE

Consent to Charge and Payment Platform Security

Who should read this?

All network operators and providers involved in the provision of premium rate services to consumers.

What is the purpose of the Guidance?

This Guidance is provided to assist networks and providers in their understanding of the relevant rules and how PSA interprets and applies them.

This Guidance should be read in conjunction with the Phone-paid Services Authority's other pieces of guidance. Specifically, the Guidance on Promoting Premium Rate Services and Guidance on Due Diligence Risk Assessment and Control:

The relevant rules

2.3.3

Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent.

and where relevant to achieving the aim of rule 2.3.3, the following Rules contained within Part 3 of the Code:

3.1.1

Network operators, Level 1 and Level 2 providers must ensure that PSA regulation is satisfactorily maintained by:

Taking all reasonable steps in the context of their roles, including the adoption and maintenance of internal arrangements to ensure that the rules set out in Part Two are complied with and the outcomes achieved in respect of all PRS with which they are concerned, and

Carrying out their own obligations under the Code promptly and effectively, and

Taking all reasonable steps to prevent the evasion of, and not to undermine, the regulation of PRS,

3.1.3

Network operators, Level 1 and Level 2 providers must assess the potential risks posed by any party with which they contract in respect of:

The provision of PRS, and

The promotion, marketing and content of the PRS which they provide or

facilitate and take and maintain reasonable continuing steps to control those

risks.

3.1.6

Network operators, Level 1 and Level 2 providers must carry out reasonable monitoring of PRS provided by any Level 1 or Level 2 provider with which they have contracted.

3.1.7

Network operators, Level 1 and Level 2 providers must use all reasonable endeavours in the context of their roles to ensure that all of the PRS with which they are involved are of adequate technical quality, including the mechanisms used to deliver services to an to enable exit from services by consumers.

What are the key points?

This Guidance covers the following areas:

- why informed and robust consent is important
- expectations around informed consent and consumer purchase journeys
- expectations around robust payment and verification platforms.

Section One: informed and robust consent

What is informed consent?

1. Informed consent refers to consumer consent given only when the consumer has the key information they need to make a decision as to whether to make a purchase or not.

2. The PSA would generally regard the consumer's consent as having been informed if it can be demonstrated via genuine, easily auditable records that have not been tampered with in any way since they were created, that a consumer has seen:

    - clear and legible pricing
    - service information (a clear explanation of what the service is)
    - charging frequency (such as whether the charge is a recurring subscription or a one-off)
    - any other relevant information (such as in relation to free trial periods).

What is robust consent?

3. Robust consent refers to consumer consent to a transaction, which can be properly audited in such a way as to prove that the consent could not have been given in any other way than by the consumer's specific actions. Robust consent can be proven through thefollowing:

    - **in the case of calls to voice-based services:** records which clearly set out the date, time and number which was called, and the consumer's number

    - **in the case of text messages sent by a consumer to purchase services which are promoted in print, on television, on websites, or other forms of advertising:** records which clearly set out the date and time when the consumer sent the text, their phone number, the mobile shortcode to which the text was sent, the dates and times when that shortcode received the consumers' message, and any other relevant messages the shortcode then sent in reply

    - **in the case of purchases initiated via websites:** records which clearly set out the dates, web addresses (including http headers) and exact times when and where a consumer purchased, and also record the pricing and other key information that the consumer saw on the relevant website at the time that they initiated and confirmed that purchase. For purchases resulting in a charge to a mobile phone bill, records should also include the consumer's device and mobile network.

4. In all three cases above, creation and storage of such records must be clear, and able to be independently and easily auditable (including by the PSA). Providers should be able to demonstrate that such records show genuine consumer consent and have not been tampered with in any way since they were created. The provider should be able to provide PSA with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed) and real-time access to this opt-in data, upon request. This may take the form of giving the PSA password-protected access to a system of opt-in records.

Why informed and robust consent is important

5. Phone-paid services allow a charge to be generated to a consumer's phone bill.

6. Ensuring consumers are only charged when they have requested or consented to a purchase is of critical importance to the PSA. Any charging without the consumer's informed and auditable consent can lead to financial detriment and have a wider effect on consumer trust in phone payment as a mechanism. Any lack of trust can also reduce consumer engagement with phone payment in the future. The PSA wants to support a healthy market that is innovative and competitive.

7. It is essential that providers at all stages of the value chain can supply robust, auditable records of informed consumer consent for every charge that is applied to a phone bill.

Section Two: Expectations around robust consent and consumer purchase journeys

8. This section sets out the PSA's expectations in relation to the following purchase initiation routes:

    - calls to voice-based premium rate numbers
    - text messages sent to a mobile shortcode
    - entry of a consumer's mobile number into a website
    - where the consumer is using a wifi connection or their network IP to connect to the internet
    - charges incurred each time the consumer views a new webpage, image or video on a website.

Third-party consent verification

9. Where verification is undertaken by a third party, this party should be independent of the Level 2 provider[8]. This verification should only be undertaken on behalf of the Level 1 provider. Where a Network operator contracts directly with a Level 2 provider the verification function can be undertaken by the Network operator.

10. As part of any contract between a Level 1 provider and a third-party consent verification platform, the Level 1 provider should satisfy themselves that the platform meets the standards and expectations on staff roles and responsibilities and risk management and control, as well as those set out at Appendix A.

11. In addition, the third party will be expected to provide data of payment records and other relevant information to mobile network operators and the PSA upon request. Mobile network operators should have in place contracts with Level 1 providers which allow for the random testing of third-party platforms at any time and should retain the right to refuse to accept verification by any third-party platform at their discretion.

12. In any event, where a Level 1 provider contracts with a third-party consent platform, the Level 1 will remain responsible for the verification.

Calls to voice-based premium rate numbers

13. In the case of calls to non-geographic numbers used for phone-paid services

[8] This means that neither party should be controlled or influenced in any way by the other, including through officers, staff, representatives or others with significant control within or connected to either party.

under PSA's remit (such as 118, 09, 087, or 084 in limited cases) or to voice shortcodes, robust verification can take the form of an originating Network operator's record of the consumer's initiation of the call.

14. UK networks have technical safeguards in place so that no charge can take place for a voice call until a consumer has dialled a number, and either picked up a receiver or pressed a call button on their phone. In addition, charging consumers to receive a call is generally prohibited by all consumer-facing networks in the UK (with the exception of "reverse charge" calls to a local or national number where the reversal is accepted by the called party).

15. When a consumer disputes such a charge, if the originating network provides PSA with their record of the call, we will generally accept that the charge was valid if there is no other evidence that would lead us to investigate further.

16. We note that this does not mean that the consumer's consent was necessarily informed – i.e. the promotion may have been inadequate or misleading, and in such cases we will investigate this where necessary.

Text messages sent to a mobile shortcode

17. Where a consumer sends a message to a mobile shortcode promoted in print, on television, or on a website, the message is known as a Mobile Originating (MO) message. As this message has been initiated by the consumer, we will generally accept the mobile network's record of the message being sent as robust consent, providing there is no other evidence that would lead us to investigate further, for example evidence that a consumer's mobile handset was infected with malware which initiated the MO message without their consent.

18. Again, the sending of an MO message by a consumer does not mean that the consumer's consent was informed or that the promotional material the consumer saw before sending the MO message complies with the Code, and we will investigate this where appropriate.

Entry of a consumer's mobile number into a website – where the consumer is using wi-fi or their Network IP

19. Some phone-paid service charges are initiated by a consumer entering a mobile number on a website. Consumers do not always appreciate that entering their number in this way can initiate a purchase which carries a charge to their mobile bill. There is a risk of harm if a consumer enters a mobile number belonging to someone else (either by mistake or deliberately), which could lead to a second consumer being charged.

20. In addition, where a consumer uses their Network IP, an encrypted version of

their mobile number can be passed through to the payment platform of the website where the consumer is browsing, enabling a charge to be made to their bill.

21. The PSA's expectations for providers obtaining robust consent from a consumer are the same, whether the consumer is using their Network IP or using wifi.

22. Normally in both of these circumstances, a consumer enters their mobile number into a field on the website, which initiates a Mobile Termination (MT) message from the service provider to the consumer's handset. Where a provider wishes to use this process, the PSA's expectations are as follows:

    - providers should make it clear to the consumer what the service is and who is providing it.

    - after a number has been entered, a free MT message should be sent to the related handset containing a PIN. The PIN should be initiated and confirmed by the Level 1 provider[9] through interaction with the consumer. We recommend the PIN is alphanumeric and contains no less than four truly random digits. The message should contain the PIN, the service name, the cost and frequency of charging, and that the PIN should be deleted if received in error. Other than this, the MT message should not contain any other content, and especially not content which could act as instructions for a consumer who had not previously visited the relevant website.

23. Any PIN sent to a consumer via an MT message should expire if, after three attempts, the consumer has not entered it correctly. In any event, a PIN should also expire within a reasonable time of being sent, and any purchase which has not been completed should be shut down and erased from the provider's records. Evidence of all PIN entry attempts, whether successful or not, should be recorded.

24. Instructions on the website should make clear that the consumer has to enter the PIN which they received within the MT message into a second field. Once the PIN is entered the consumer should be required to click on a confirmation button, where pricing and frequency of charge information are prominent and proximate to, or contained on, the button.

25. Some websites which promote phone-paid services invite the consumer to enter their number, and then send them an MT message containing a keyword. The consumer must then text a reply containing the keyword in order to consent to the charge. Where this is the case, we would expect that the message also contains the service name (and brand where different), and the

[9] This function may be undertaken by an independent third party on behalf of the Level 1 provider. Where a Network operator contracts directly with a Level 2 provider (i.e. there is no Level 1 provider involved in the provision of the service), the function may be undertaken by the Network operator.

cost and frequency of charging, in such a way as to make clear to the consumer that replying with the keyword will result in a charge.

26. Providers may also use a password-controlled account, with the consumer entering a password which they have selected and control to first confirm their identity, and then confirming consent to payment on a second screen, or by using biometric technology such as fingerprint or facial recognition.

27. Following the above steps will assist providers in achieving and demonstrating robust consent to charge in consumer journeys. However, where providers and/or specific services are subject to other PSA regulatory requirements, such as Special conditions, compliance with the above steps may not be sufficient to meet those requirements and therefore providers should ensure that they take all further steps necessary to achieve compliance with such requirements.

Charges incurred each time the consumer views a new webpage, image or video on a website[10]

28. In some circumstances, charges can be generated once consumers click on a website – often to view an image or a new page. The PSA's expectation is that each charge – i.e. each time the consumer clicks on a new image or page that triggers a charge – must be subject to robust consent verification, as set out above. In the alternative, consumers can give their consent to all subsequent charges when they enter the website, but they must be clearly and prominently informed, in very close proximity to the consent buttons, that this is what they are doing.

Section Three: Expectations around robust payment and verification platforms

What are robust payment and verification platforms?

29. Payment and/or consent verification platforms (and related web interfaces) which have adequate technical and risk control procedures, that demonstrate any records of charging cannot have been initiated in any way other than from the informed consent of a consumer.

Types and scope of expectations

30. Expectations around a robust payment/consent platform (and related interfaces), can be split into three categories:

[10] Providers should note that services which charge per page or Image viewed are subject to Special conditions regimes and must comply with the conditions within these regimes.

- technical expectations
- staff roles and responsibilities
- risk management and control.

31. The expectations set out under the headings below apply to all platforms. This includes payment/consent platforms provided by any Level 1 provider who is part of a value chain, and consent verification platforms provided by third parties (whether they sit within a value chain, or have been contracted by a Level 2 provider, Level 1 provider or network within it, or indirectly provide consent verification services to it).

Technical Expectations

32. In setting Technical Expectations for payment and consent verification platforms, the PSA notes it is possible to arrive at robust proof of informed consent via different approaches depending on the design of a platform's technical architecture. Nonetheless, there are universally accepted standards regarding the underlying software platforms use to operate, and the protocols they use to interface with web pages and other external systems. The Technical Expectations which we set focus on these universal standards. These are set out at Appendix A.

33. To ensure our expectations remain up to date, and prevent them being rendered obsolete by evolving technology, we will review them in conjunction with the mobile network operators on an annual basis and consult on any proposed revisions.

Staff roles and responsibilities

34. Payment/consent platforms can be compromised by bad judgement on the part of those who are responsible for them. The likelihood of this is heightened in an emergency, or when people do not have a clear idea of their responsibilities in relation to the platform and how to discharge them. To ensure that any risk is adequately identified, communicated, and controlled, the PSA has set out expectations around roles and responsibilities, and staff training.

35. The PSA recognises that staffing decisions are a matter for the company concerned. However, given the importance to the consumer interest of maintaining a sufficient level of platform security, the PSA's expectation is that all platform providers have adequate resource, either internal or externally contracted, focused on security and fraud. The PSA recommends that security staff should be suitably qualified (such as a degree in computer science or a related discipline) and/or experienced such that they are able to meet the following competencies:

- ability to evaluate risks in platforms and software, and research security incidents
- good understanding of web security and internet security tools
- understanding of threat modelling.

36. The PSA's expectation is that all platform providers have an assigned "Head of Security" or other equivalent senior role. The PSA recommends that a Head of Security or equivalent senior person should be suitably qualified and/or experienced such that they are able to meet the below competencies:

    - demonstrable knowledge of the latest security thinking and threat modelling-methods
    - ability to manage complex IT platform overhaul projects, if required
    - significant knowledge and experience of IT/web security to enable the effective identification, management and control of security and fraud risks
    - we recommend that the Head of Security or other equivalent senior person has significant knowledge and experience of security management systems and processes. Examples might be, but are not limited to, experience of working towards ISO/IEC 27001 certification and the National Cyber Security Centre (NCSC) "Cyber Essentials Plus" assurance, or current equivalent.

    Where such a role is vacant as a result of staff departure or absence, then responsibility should shift upwards to a more senior member of staff.

37. The PSA's expectation is that each platform provider should have a nominated Single Point of Contact (SPoC) whose details have been shared with the various industry stakeholders such that when an incident does occur, no time is wasted in investigating and rectifying issues.

38. We recommend that all providers ensure that platform development staff are trained in secure development techniques and have an understanding of relevant risks and threats to an appropriate level, which we recommend is at least at or akin to the NCSC "Cyber Essentials" level or current equivalent. Training should be undertaken periodically, to take account of threat and risk evolution and to keep skills current.

39. Our expectation is that all platform development staff should build their understanding of relevant risks and threats into any development work they carry out. Providers will be expected to be able to demonstrate this upon request or direction by the PSA.

40. The PSA's expectation is that all platform or other systems development – including but not limited to new protocols for phone-payments – should have their functionality reviewed by the security team before they go live.

41. The PSA recommends that the Head of Security (or equivalent senior person) should have the authority to veto any protocols or solutions and be able to make go-live subject to an audited assessment and approval from the security team. Where the decision is taken not to follow this recommendation, the provider should be able to demonstrate how they achieve an equivalent level of assurance. An example template for recording such assessment is attached at Appendix C. The use of this template is entirely voluntary and is intended to set out the level of detail the PSA would expect to receive about assessments where relevant to an investigation.

Risk management and control

42. It is important that all organisations involved in payment or consent verification have adequate processes to quickly identify, record, communicate, and control risk, and to incorporate lessons learned into processes.

43. All parties involved in provision of phone-paid services should maintain a security risk/issues register. The register should record any identified risks or issues on an ongoing basis, and set out as a minimum the following:

    - an explanation of the risk or issue – in the case of an issue, the explanation should also set out exactly when and how it was discovered, and by whom
    - the actions taken to mitigate/resolve the risk/issue – with a timestamped record of who has signed them off as being complete and when
    - any further, ongoing actions (which can be transferred to "actions taken" as above, once they are complete and signed off)
    - the individuals within the organisation responsible for ongoing actions.

44. In addition, the PSA recommends that active threat monitoring measures are implemented to monitor systems and alert staff in real time. These measures should aggregate data from across the platform, understand traffic patterns, and provide detailed information about potential attacks or exploits. This should include, but not be limited to:

    - leveraging threat intelligence from previously seen attacks
    - analysing consumer behaviour – e.g. transaction logs, transaction times, user agent/device, x-header requests, associated URLs, IP addresses, time deltas between double opt-ins, repeat transactions, unfinished transactions, repeat unfinished transactions and their frequency
    - analysing Level 2 provider behaviour – e.g. what kind of data they access and how frequently, whether apps are requesting payment pages
    - performing "Attacker Behaviour" analytics

- setting intruder traps – e.g. decoy network services or credentials
- conducting proactive threat hunts
- conducting "Red Team/Blue Team" penetration testing using discovered malware.

45. All parties involved in the provision of phone-paid services should act on any security alerts or flags, whether from their own monitoring or information shared by others, in a timely manner. An example template for recording security breaches, or attempted breaches, is attached at Appendix C. The use of this template is entirely voluntary; however, it does set out the level of detail the PSA would expect to receive around any security breaches or attempted breaches where relevant to an investigation.

46. The PSA recommends that each payment and/or consent verification platform should be tested by a CREST-accredited third party on an annual basis. Testing should identify and score exploits according to the OWASP taxonomy and the CVSS scale. The results of these tests should be made available to all mobile network operators and provided to the PSA upon direction. Any identified exploit with a CVSS score of 4.0 or over should be fixed immediately. The platform, and services that are using it (or in the case of third-party consent verification platforms, just the services that are using them) may be in breach of the relevant Code rules[11] until the fix has been completed, as independently verified by the tester.

47. In line with current due diligence and risk assessment obligations, Level 1 providers should have contracts in place which allow them to suspend or terminate payment facility to any Level 2 providers or third-party consent verification platforms on the basis of non-compliant activity, such as charging consumers without informed and robust consent, or where they reasonably suspect that such activity has or is occurring.

48. Also in line with current due diligence and risk assessment obligations, Mobile network operators should have contracts in place which allow them to suspend or terminate Level 1 providers in circumstances where non-compliant activity is discovered. In addition, they should take effective action against Level 1 providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the

[11] Only platforms which are part of the value chain may be considered by a PSA Tribunal to be in breach of Rule 2.3.3 of the Code – i.e. the requirement to have (and provide upon request) robust, auditable consent – and requirements at Part 3.1 of the Code for adequate risk control and technical quality. Third-party verification platforms are not part of the value chain, and therefore not registered parties with us. However, any services using a platform which does not comply may be considered by a PSA Tribunal to be in breach of Rule 2.3.3 of the Code.

case.

49. This should include clear, documented consideration of whether Level 1 providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

50. The PSA recommends that mobile network operators should have contracts in place which permit them to conduct further random CREST-accredited testing at any time on any Level 1 provider payment platform, and to document any findings, and when and how improvements are made as a result of them.

51. For the avoidance of doubt, we would be unlikely to consider the end of a direct contract to be a sufficient risk control measure on its own, if the Level 1 provider in question were still permitted to operate within the value chain through another Level 1 provider's platform – i.e. we would expect further assurance and risk control to be able to be demonstrated.

52. The PSA's Guidance on Due Diligence Risk Assessment and Control provides further guidance on the PSA's expectations in respect of risk management and control.

Appendix A – Technical Expectations

The following are a list of Technical Expectations which the PSA expects all payment and/or consent verification platforms to have in place while operating any phone-payment transactions. In order to prevent depreciation of the standards as technology and attack vectors evolve, this list will be reviewed and updated with consultation as appropriate by the PSA on an annual basis.

Where a provider's platform does not explicitly meet one or more of the specific expectations listed below, the PSA expects that the provider will be able to demonstrate on request how the objective expressed in that expectation is otherwise achieved. The expectations are as follows:

- all platforms should be hosted strictly independently of any Level 2 provider[12]. Where a Level 1 provider wishes to offer services on its own platform then it must retain ownership, control and responsibility for all aspects of the service
- all platforms should use the current version of the Transport Layer Security (TLS) protocols or as a minimum version TLS 1.2
- all platforms should have in place a strong Content Security Policy (CSP) to restrict resource usage
- browser Cross-site Scripting (XSS) mitigations should be enabled on all platforms by default
- HTTP Strict Transport Security (HSTS) headers should be enabled on all platforms by default
- payment pages should protect against click-jacking, for example by use of HTTP Headers
- any phone-paid transaction should only occur over correctly validated HTTP connections
- payload protection should be implemented in order that it cannot be edited part way through a transaction
- rate limiting should be in place for login attempts, in order that "brute force" password guessing is prevented
- authentication cookies should be encrypted by default on all platforms and expire within a reasonable amount of time.[13]

[12] This means without the control, or influence of any Level 2 provider, including their officers, staff, representatives or other persons with significant control.
[13] We recommend that providers refer to the Information Commissioner's Office (ICO) to ensure that any authentication cookies and expiry times are in line with relevant legislation and the ICO's expectations.

Appendix B – Glossary of technical terms

Attacker Behaviour Analytics

Where web and payment platforms analyse previously known patterns of cyber-attacker behaviour and use the trends in that data to identify repeats of those attacks, or the next potential variants of those attacks.

Authentication cookies

A cookie is a small piece of data sent from a website and stored on the user's device by the user's web browser while the user is browsing. This is usually to remember information such as any items a user has added to a shopping cart, or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited). They can also be used to remember information that the user previously entered into form fields such as names, addresses, passwords, and card details or phone numbers for payment.

Authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with.

Content Security Policy – (CSP)

CSP is a computer security standard introduced to prevent various types of attacks where malicious code is injected into a trusted web page. CSP works by providing a standard method for website owners to declare approved origins of content that browsers should be allowed to load on that website. Anything which is not approved cannot be loaded.

Council for Registered Ethical Security Testers (CREST)

CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provide internationally recognised accreditations for organisations, and professional-level certifications for individuals providing various types of cyber-security services.

Cross-Site Scripting (XSS)

XSS is a type of computer security vulnerability which typically exploits known vulnerabilities in web-based applications, their servers, or the plug-in systems in which they rely. An attacker "injects" malicious coding into the content being delivered by the web application. When the resulting "combined" content arrives at the user's web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system.

Common Vulnerability Scoring System (CVSS)

CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities, created following research by the US National Infrastructure Advisory Council in 2003/04. Vulnerabilities are rated on a scale of one to ten, with ten being the most severe.

Hyper Text Transfer Protocol (HTTP)

HTTP is the underlying protocol used by the World Wide Web, which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

HTTP Strict Transport Security (HSTS)

HSTS is a web security policy mechanism that allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure (HTTPS) connections, and never via the insecure HTTP protocol. A website using HSTS must never accept clear text HTTP and either not connect over HTTP or systematically redirect users to HTTPS.

Mobile Origination message (MO)

A text message which has been originated on, and sent from, a mobile device. These can be either free – i.e. the cost of sending the message is that of sending a standard text – or charged at a premium when the text is received by the mobile shortcode to which it was sent.

Mobile Termination message (MT)

A text message which is received by a mobile device. These can either be free – i.e. receiving the message costs the recipient nothing – or charged at a premium when the device receives the message. In the context of phone payment, MT messages are usually generated by a Level 1 provider in response to consumer interaction with a Level 2 provider merchant. Where they are not, it may be that the message and any associated charge was unsolicited.

National Cyber Security Centre – (NCSC)

The NCSC is an organisation of the UK Government that provides advice and support for the public and private sector on how to avoid computer security threats. One of their products is the NCSC Cyber Security Essentials certification, a set of basic technical controls to help organisations protect themselves against common online security threats.

Cyber Essentials is backed by industry including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organisations which are offering incentives for businesses. From 1October 2014, the Government has required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

Network internet provision

An Internet service provider (ISP) is an organisation that provides services for accessing, using, or participating in the Internet. Where a consumer uses the internet access provided by their mobile network to browse the web with their mobile device, this is known as "Network IP".

Open Web Security Application Project (OWASP)

OWASP is a worldwide not-for-profit charitable organisation focused on improving the security of software, so that individuals and organisations are able to make informed decisions. Operating as a community of like-minded professionals, OWASP issues free, open-source software tools and knowledge-based documentation on application security.

The OWASP Top 10 is a project to document the ten most critical categories of security risk to web applications. It represents a broad consensus of a variety of security experts from around the world, who share their expertise to revise the list on a regular basis.

Payload protection

The payload is any message sent by a user's device to a website or other web application, where that message contains, or has had added, malicious coding. Payload protection is any action or system which seeks to identify and block messages containing malware.

Personal Identification Number (PIN)

A PIN is a numeric or alpha-numeric password used to authenticate a user so they can access a website, web application, or any other system.

Rate limiting

Rate limiting is used to control the rate of traffic sent or received by a network interface controller. In the context of phone payment, it prevents repeated attempts by an attacker to send the same message or execute the same action. A common example is the rapid, and sequential, entry of every possible four-digit PIN until the correct one is entered, thus allowing an attacker who does not know the PIN to gain access through repetition.

Red Team/Blue Team testing

Where a security function divides into two teams in order to conduct penetration testing. One, the Red Team, uses malware the team has discovered to try and execute that malware on a "sandboxed" version of the platform, with the Blue Team attempting to identify and prevent any attempts.

Threats

Known malicious indicators that appear together during specific cyber-attacks. By recording and aggregating intelligence about threats, payment platforms and web applications can identify and prevent further attacks using the same methods and look to predict what variations on previous attacks may appear next.

Transport Layer Security (TLS)

TLS is an encryption protocol that protects data when it moves between computers or other devices. When two devices send data they agree to encrypt the information in a way they both understand. This prevents data being intercepted by a third party, or 'injected' with malicious code.

Time delta

Where a user interacts with a website or web application, and in particular where they click on-screen buttons, the time delta between clicks is an important way of ascertaining whether the interaction is genuine or is potentially being carried out by a device infected with malicious code. Sometimes an infected device will 'click'" more rapidly than a human being could or will click on the exact same pixel within a sequence of buttons which are presented.

Uniform Resource Locator (URL)

The formal term for a web address.

X-header request

The instruction sent by a device in order to 'pull' a specific website or webpage to it and display the page so a user can browse it. In effect the X-header request ID correlates the HTTP request between a user's device and the website or web application's server.

Appendix C – Example templates for security records

Assessment of New Platform or Systems Developments

Description of the proposed update/new protocol/development				
Person(s) responsible for security assessment				
Summary of the security assessment (e.g. methodology used to assess and test)				
Pass or Fail?				
If "pass", were there any dissenting views? Please provide details	*Person(s) who dissented*	*Reasons for dissent*	*Relevant OWASP category*	
If "fail" please provide details of the reasons for failure	*Description of the identified issue/weakness/risk*		*Relevant OWASP category*	
Will the proposal be re-submitted?				
If it will, what improvement actions are required?	*Description of the action*	*Who is responsible for the action?*	*Date the action is assessed as complete*	*Who signed it off as complete?*

Record of identified security incident

Description of identified breach or attempted attack	*Breach or attempted attack?*	*Description*	*Relevant OWASP category*	
When and how was it identified?	*Date*	*Time*	*How was it flagged?*	*Who was the SPoC?*
Person(s) who performed the initial assessment				
Summary of the incident and the SPoC's assessment				
Was the incident reported to:				

MNOs?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*
PSA?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*
ICO?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*

What immediate actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (date and time)*	*Who signed the action off as complete?*
What remedial actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (date and time)*	*Who signed the action off as complete?*