PSA
Phone-paid Services Authority

Consultation on revised guidance on Consent to Charge

14 August 2019

Contents

About the PSA

The Phone-paid Services Authority (PSA) is the UK regulator for content, goods and services charged to a phone bill. Our vision is a healthy and innovative market in which consumers can charge content, goods and services to their phone bill with confidence. Our mission in the phone-paid market is twofold:

- to protect consumers from harm
- to further consumers' interests through encouraging competition, innovation and growth.

We will seek to do this through:

- improving the consumer experience of phone-paid services
- applying and enforcing an outcomes-based Code of Practice
- delivering a balanced approach to regulation
- working in partnership with Government and other regulators
- delivering high standards of organisational support.

Executive summary

1. Consumers should not be charged 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 mechanic. It is the PSA's view that a lack of trust reduces future consumer engagement with phone payment, which lessens opportunities for market growth and development. For these reasons, it is essential that providers can supply robust, auditable records of informed consumer consent for every charge they levy to a phone bill.

2. During the financial years 2017/18 and 2018/19 the PSA has seen a significant rise in consumer complaints about Subscription Services[1]. This service type makes up over 90% of our total complaints and enquiries across the same period. While not all consumers allege they were charged by a service or signed up to a subscription without their knowledge, a significant proportion do. Therefore, in addition to work around ensuring robust consent to purchase through payment platforms which is set out here, this has also led to a separate review of how consumers interact and understand subscription payment journeys, which is detailed in our recent consultation on changes to Subscription Services Special conditions.

[1] During 2017/18 the average number of complaints per month was 1313, rising to 1689 in 2018/19.

3. In five cases since October 2018[2] (and with a further 4 cases from October 2017 to October 2018), the Code Adjudication Tribunal has found there was no robust evidence of a consumer's consent to be charged and sanctioned the provider accordingly[3]. PSA's own monitoring had also identified weaknesses in some payment platforms which could theoretically be exploited by a rogue merchant to spoof consent.

4. We wished to improve our understanding of mobile-based phone-payment platforms, in order that the expectations and requirements in our regulatory framework – including our existing Guidance on Consent to Charge - could be updated where necessary. It is important that our requirements keep pace with emerging risk, that our regulatory standards provide the required protections for consumers and that any allegations of non-compliance can continue to be investigated effectively.

5. At the same time, it became apparent that the UK Mobile Network Operators (MNOs) had identified similar weaknesses in some payment platforms highlighted by their own compliance monitoring. In light of this, and associated customer feedback, they were keen to identify any weakness in the payment platforms operated by the aggregators (these are referred to as "Level 1 providers" in the Code of Practice) with whom they contract that would result in opportunities for bad actors.

6. The PSA and the MNOs agreed to fund joint research to test those platforms which are accredited by the MNOs' "Payforit"[4] Scheme. The research company selected after a comprehensive, open tendering process was Copper Horse. Testing was carried out according to a bespoke penetration testing methodology, with the first round of tests conducted during May-July 2018, and a second round during December 2018 - February 2019.

7. Specific findings were fed back to the providers of each of the platforms tested, with the MNOs requiring that any identified exploits rated above a defined risk threshold were addressed by 31 March 2019. It is important to note that Copper Horse's findings referred to weaknesses which could be exploited to spoof consent, and as such did not prove that these weaknesses had been used to cause actual consumer harm.

8. In addition to specific recommendations made to individual Level 1 provider aggregators, Copper Horse also made some general recommendations. These were variously relevant to Level 1 providers, MNOs, the PSA, or combinations of all three, and were a mixture of technical standards and best practice internal procedures.

9. The PSA and MNOs evaluated the Copper Horse recommendations against their respective regulatory and contractual expectations. The MNOs have added relevant Copper Horse recommendations to updated Payforit accreditation standards. As at the time of publication of this consultation, we note that this includes the requirement for all Trusted

[2] Examples include Net Real Solutions SL, Flipcove Ltd and Xplosion Ltd.
[3] Between the longer period of 9 June 2016 and 11 July 2019 there were 23 adjudications with a common breach of a lack of evidence to establish consent to charge.
[4] Payforit is a payment method whereby accredited payment platforms agree to use prescribed, branded payment screens and payment mechanics, and as a consequence operate according to a set of rules which the Mobile Network Operators update to take account of market evolution.

Payment Intermediaries (Level 1 providers who are Payforit accredited) to have their platforms fully retested on an annual basis.

10. The main exceptions, in terms of recommendations which the MNOs have not included to date, were around technical standards. However, we propose to add Copper Horse's technical recommendations as part of the proposals within this consultation, which the MNOs have signalled their intention to align with, were the proposals to be adopted.

11. Having reviewed the Copper Horse recommendations, the PSA proposes to revise and update our existing Guidance on Consent to Charge. These changes will set out more detailed expectations around the standards by which Level 1 provider payment platforms are operated, maintained, and utilised, and around Level 1 provider risk assessment and control in relation to consent verification and record keeping. These changes incorporate all relevant Copper Horse recommendations. In addition, we propose adapting some of our existing Guidance to take account of market evolution – in particular around Subscription Services. A copy of the revised Guidance is attached at Annex A to this document.

12. While only Level 1 provider platforms which are accredited under the Payforit Scheme were tested, the PSA and MNOs have agreed that the standards and expectations should also apply to third party consent/verification platforms. These platforms are used by some services which do not sit behind the mobile networks' Payforit accreditation scheme. These platforms perform a consent verification function, in the same way as the tested Level 1 provider platforms do, and both PSA and the MNOs view it as sensible that they should adhere to the same standards. As a result, we note that MNOs will require third party consent/verification platforms to seek accreditation to the same standard as Payforit ones, and the PSA proposes that the expectations in its revised Consent to Charge Guidance will apply equally to all platforms that provide evidence of consent to a phone-paid charge.

Background

The development of premium rate services/phone-paid services and consent to charge

13. Premium rate services offered by providers other than BT were first available in the UK in the 1980s and were exclusively landline-based voice services. In the case of voice services, the consumer initiates the call and consent to charge issues rarely arise.

14. Text-based phone-paid services emerged and grew in the late 1990s/early 2000s . These included chat and update services, and downloadable phone "customisation" products such as ringtones and wallpapers. Consent for a charge to be levied for these services takes place when consumers text a mobile shortcode with a text containing a keyword. These text messages are known as Mobile Origination (MO) messages, because they originate from the consumer's device.

15. Once a consumer had texted an MO message to a shortcode, charging took place in one of two ways. Either a charge would be levied onto the consumer's bill by their mobile network

as soon as their MO message was received by the payment platform operated by a Level 1 provider on behalf of the merchant (having been acknowledged as having arrived by the mobile network), or the charge would not be levied until the merchant, again via their Level 1 provider's payment platform, had sent a Mobile Termination (MT) message in reply to the consumer's MO, and that MT message was acknowledged by the mobile network as having been received (i.e. "terminated") by the consumer's device.

16. While MO messages may appear to be analogous to voice services in that the message is initiated by the consumer, more issues are reported to the PSA. Consumers may be misled by advertising into texting a shortcode and the PSA also had to consider whether an MT charging message has been sent in legitimate response to a previous MO message sent by the consumer.

Evolution of web-based consent methods

17. Most people now own smartphones and phone payment has evolved into a payment option for a growing range of digital products and services.

18. This evolution of phone payment also added new methods by which a consumer can consent to a charge. One early method was that a consumer could enter their mobile number (known within the industry as a MSISDN[5]) into a field on a merchant's website, which would trigger an MT charging message. Unfortunately the entry of a mobile number on a website can be spoofed, and so having investigated a number of cases involving such practices in 2009-10, the PSA (then PhonepayPlus) gave notice to the industry that we would no longer accept such a mechanic on its own, without any other evidence of consumer consent.

19. The most common solution was the addition of a "PIN loop". This is where the entry of the consumer's mobile number into a merchant's website triggers a free MT message containing a Personal Identification Number (PIN). The consumer enters this PIN back into another field on the website to confirm the consent to the transaction (and charge). PIN loop systems are operated by Level 1 providers who are accredited as part of the mobile networks' "Payforit" scheme, and by third parties who provide consent/verification platforms to a Level 1 provider or merchant (referred to as "Level 2 provider" in the Code), but are not part of the revenue share from the purchase itself.

20. The other common method by which consumers make a phone-paid purchase from a website can only be utilised when they use their mobile network's internet provider (network IP), rather than wi-fi, to browse the web. When a consumer uses the network IP, then their mobile number is necessarily known to the network (otherwise it could not function as a phone) and by extension the IP is also known. When the consumer "lands" on a Level 2 provider's site, the network is able to pass their number ("MSISDN") through to the accredited Payforit Level 1 provider who performs consent/verification for that website. The Level 1 provider can then serve two consecutive payment consent buttons to the consumer, which the consumer clicks to initiate and then confirm the purchase.

[5] Mobile Station International Subscriber Directory Number

21. This "MSISDN passthrough" method is operated only by Level 1 providers who are accredited as part of the MNOs Payforit scheme. Under the rules of the scheme, the Level 1 provider must not pass the consumer's mobile number onto a Level 2 provider. So any browsing activity, or notification of a successful purchase (for which the Level 2 provider must send or make content available), must encrypt the consumer's number.

Current PSA Regulatory requirements and expectations

22. 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.*

23. "PRS" in this context refers to "premium rate services", the name by which phone payment is known in UK law. In practice consent can be provided by any party within the value chain on the Level 2 provider's behalf.

24. The requirement within the Code was supported by Guidance on Consent to Charge, which the PSA first consulted and issued alongside the 12th edition of the Code in 2011. This Guidance has been reviewed and re-consulted on two occasions since, in 2014 and then again in 2015 when the 13th and 14th editions of the Code were consulted and published.

Developments driving the review

25. Since Guidance on Consent to Charge was last reviewed alongside the 14th edition of the Code of Practice, the PSA has seen an increase in the following:

- consumer complaints which report that they did not engage with, or in some cases even visit the website concerneds
- records of consent – presented by Level 1 or Level 2 providers, or third party consent/verification providers, or more than one of them, during the course of PSA investigations – which are not tamperproof and therefore could have been altered after the event, or inserted without actual consumer interaction. This has resulted in recent PSA Tribunals finding that there was no robust evidence of consent to charge in relation to a service[6].

26. Over the past 2-3 years, MNOs have mandated that an increasing number of service and content types, and so an increasing proportion of the phone payment market, must use payment platforms accredited by individual MNOs via the requirements of the shared Payforit scheme. At the same time PSA saw a rise in complaints about operator billed services. The PSA

[6] Examples include Net Real Solutions SL, Flipcove Ltd and Xplosion Ltd.

planned a project to investigate the causes of this rise in complaints and in particular whether it might be attributed to weaknesses in Level 1 provider platforms.

27. During the same period, we note that MNOs also received increased consumer complaints and feedback about services using the Payforit platform. With phone payment growing as a payment option, market evolution and consumer expectation would naturally point towards higher security standards. MNOs advised that they were keen to ensure that any potential weaknesses in Payforit accredited platforms were identified and mitigated.

Joint security testing of Payforit platforms

28. Given the shared interest in setting higher, and more detailed, standards for phone payment platforms, the MNOs and PSA agreed to jointly fund testing of Level 1 provider platforms which were Payforit accredited. The testing was intended to achieve the following:

- to provide a system for categorisation of the type and severity of identified weaknesses, and to provide individual Level 1 providers with a report into any issues they would be required to resolve
- to allow MNOs to evaluate their current contractual controls, and PSA to evaluate its current requirements and expectations, against general recommendations and introduce new or more detailed standards where necessary.

29. The research 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 during May-July 2018, and a second round during December 2018-February 2019. All Level 1 providers accredited under the Payforit scheme were tested during this time.

Testing methodology

30. Each Payforit accredited Level 1 provider supplied Copper Horse with the same access and permissions to their platforms that a merchant using phone payment would normally receive. Copper Horse then conducted penetration testing in a variety of ways, to ascertain whether there were weaknesses within the platform which could allow a rogue merchant to directly fabricate consent. Or whether there were weaknesses which could allow a rogue merchant to access restricted information, indirectly allowing them to fabricate consent.

31. Copper Horse categorised each exploit they discovered according to the Open Web Access Security Protocol (OWASP)[7] "Top Ten" of web security risks and rated each exploit

[7] The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software, so that individuals and organizations 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.

according to the Common Vulnerability Scoring System (CVSS)[8]. Both of these are globally accepted taxonomy/scoring systems.

32. In discussion with Copper Horse, the PSA and MNOs determined that any exploit which scored above 4 out of 10 on the CVSS scale would be regarded as representing a credible risk to consumers. However, it is important to note that Copper Horse's findings in respect of any aggregator platform do not represent evidence that an identified weakness has actually been exploited to cause consumer harm.

33. Once testing was complete, Copper Horse provided anonymised feedback to each Level 1 provider (i.e. the PSA and MNO's were not present and received anonymised versions of each feedback report). The Mobile networks had already required that all exploits scoring above 4 out of 10 on the CVSS scale were fixed by 31 March 2019, with the possible suspension in whole or part of platforms which were found not to have met this deadline.

34. Copper Horse also made general recommendations and the PSA's consideration and proposals as a result of these recommendations is set out in the next section.

Growth of third-party consent/verification platforms

35. Finally, the last 18 months has seen an increase in third-party consent/verification platforms. Our current Guidance on Consent to Charge recommends that providers of such platforms seek advice from the PSA about their processes and technical standards before they begin to operate, and some platforms have done and continue to do so. However, a number of market entrants either did not contact PSA at all before operating or did not supply all the information we requested in order to give advice as to whether the platform was capable of operating compliantly.

36. This increase in third party verifiers has continued following the announcement that PSA and the MNOs would be conducting joint testing with a view to creating more detailed standards and expectations. Third-party platforms are:

- used exclusively for "PIN loop" consent, with a charge then being levied via a Mobile Termination message, as they are not accredited for the Payforit Scheme
- normally contracted directly by a merchant, rather than the Level 1 provider -which then processes the payment at the merchant's request.

These characteristics may indicate an unwillingness on the part of some merchants to place web-based payments behind Payforit, and/or have them fully controlled by the Level 1 provider. As such the PSA and MNOs agreed that any standards which resulted from the testing should apply to all consent/verification platforms, wherever they sit in relation to a service's value chain and whether accredited as part of Payforit or not.

[8] The Common Vulnerability Scoring System (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.

Consideration and proposals

Findings and recommendations

37. Copper Horse found varying categories and degrees of weakness in all tested Level 1 provider platforms. While of concern, this is not unusual in that all digital payment platforms will contain some kind of weakness, whether inherent or a platform weakening over time as technical standards surpass it. As such the PSA considers that its original hypothesis, that consumers will benefit from the application of new and more detailed standards and expectations for phone payment platforms, is validated.

38. As part of their final report, Copper Horse made some general recommendations. These were variously relevant to those who operate payment consent platforms (whether Level 1 providers or third parties), MNOs, the PSA, or combinations of all three, and can be grouped into the following categories:

- technical – i.e. specific technical standards that platforms should adopt
- staffing and training – i.e. clarification of roles and responsibilities, and the training and qualifications that identified roles should have or undertake
- risk control and incident response – i.e. such processes as allow risk to be assessed, recorded and acted upon, and that allow for immediate, comprehensive responses to any emerging incidents.

39. We note that the MNOs have added most of the relevant Copper Horse recommendations to updated Payforit accreditation standards. This includes a requirement for all Trusted Payment Intermediaries (Level 1 providers that are Payforit accredited), and third-party consent/verification providers, to have their platforms fully retested on an annual basis by a CREST[9] accredited tester.

PSA consideration

40. The PSA has considered Copper Horse's general recommendations against four options:

a) do nothing

b) guidance

c) special conditions

d) make changes to the code.

[9] 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.

41. Due to the findings during testing, which indicated some weaknesses across all Level 1 provider platforms which could, in theory, be used to cause consumer harm, we do not consider **do nothing** as a sustainable option. Even though these identified issues now appear to be fixed on Payforit platforms, and we note that MNOs have applied the same standards to all consent platforms whether Payforit or not, we consider that more detailed standards will provide greater clarity going forward. In particular, baseline technical standards can be updated regularly as technology, and security risks, evolve.

42. **Making Code changes** would require an extensive period of consultation, with the need to review all other parts of the Code at the same time. In addition, any revised Code would at present need to be laid before the EU Commission for review by member states. A Code revision can take at up to three years from start to finish.

43. We do not consider the current requirement within the Code – i.e. that consumers are not charged without their consent, and that providers must be able to provide evidence which establishes that consent – to be ineffective. This requirement has been consistent since the 12th edition of the Code and has proven an effective and clear principle against which we have been able to enforce. However, the standard for what constitutes established consent needs to be clarified and expanded upon, in order to take account of market evolution. As such, our view is that options other than a Code change will allow us to set standards in a far shorter time, and with greater flexibility to update them in line with further changes in the market. We retain the option of proposing a Code change at a later date, should that become necessary.

44. **Special conditions** are normally applied to specified service types or charging mechanics (such as Subscriptions or Recurring Donations to Charity) in order that merchants classed as Level 2 providers and/or Level 1 providers under our Code will be compelled to act to meet them. They are not applied to platforms, as they are neither service types nor charging mechanics, but rather facilitate these. In this case the PSA and MNOs have determined that it is Level 1 providers, who need to act as they control the platforms. Level 1 providers are required to comply with a number of Code provisions within section 3.1 of the Code (around risk assessment and control), as well as Rule 2.3.3. As such we do not consider that Special conditions are the most appropriate vehicle at this time.

45. The PSA has previously published, and updated, Guidance on Consent to Charge. Having ruled out Special conditions for the reasons above, **Guidance** is quicker to apply than changes to our Code and represents the least intervention to achieve the desired effect. In this case the Guidance will define the standard for the technical baseline and operation of a consent platform that PSA would expect to see met. As such, providers who do not meet the standards outlined, or demonstrate an acceptable alternative, may see a PSA Tribunal find that there has been no valid consent to charge, or evidence of such consent, in respect of any transactions they have facilitated.

46. As a result of this consideration, the PSA proposes to make changes and additions to the existing Consent to Charge Guidance. A copy of the proposed new Guidance is attached to this document at Annex A.

Summary of proposed changes to Guidance on Consent to Charge

47. In reviewing the existing Guidance, the PSA has taken into account two main considerations. Firstly, the findings and recommendations from the Copper Horse report in our view necessitate the addition of a new section to the Guidance. Secondly, we have also reviewed the existing sections of the Guidance, in particular to align with other changes made to our regulatory framework since this Guidance was last updated.

48. We have updated Section One of the Guidance – which sets out why informed and robust consent is important. This does not set any expectations for providers but does set out a definition of "informed consent" at paragraph 1.4. This sets out two key principles:

- PSA's expectations as to what providers should record in relation to transactions as proof of consent
- PSA's expectations that records should be clearly presented, independently and easily auditable (including by the PSA), and demonstrably tamper-proof.

49. For the avoidance of doubt, the expectation that records should be independently and easily auditable means that the PSA should, during the course of any investigation, be able to independently interrogate a database containing transaction records. This follows occasions when providers have refused to make such a facility available to the PSA during investigations and have instead expected that we rely on records which have been exported from a database and sent to us. Some PSA Tribunals have previously rejected such records on the grounds that they are not demonstrably tamper-proof.

Q1 – Do you agree with our definition of informed consent at paragraph 1.4? If not, why not?

50. Section 2 of the Guidance sets out our expectations as to informed consent in relation to various types of consumer purchase/consent journeys, as follows:

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

51. This section keeps the bulk of the text from the previous version of the Guidance. The text has been changed only where there is a need to take account of technical or market evolution, or to align our expectations with changes to our regulatory framework. In particular paragraphs 2.9 to 2.13 have been altered to take account of the evolution of consumer

expectations, the creation of Special conditions around consent to charge in relation to Online Adult and Competition Services, and recently published changes to Special conditions around consent to charge in relation to Subscription Services.

52. The key changes in terms of expectations include:

- additional expectations that where a consumer's number is required to be entered into a website, MT-based PINs sent to the consumer's handset (and the purchase sessions associated with them) should time out after a reasonable period, and in any case time out if the consumer entry of the PIN is unsuccessful three times
- additional expectations that web-based purchases – whether wi-fi or network IP-based – have a "two stage" confirmation
- expectations around the use of a password-based system in relation to network IP-based purchases
- addition of biometric technology to confirm a network IP-based purchase.

53. The PSA considers that these additional expectations are in line with the findings of consumer research that has been carried out for us over the past three years. Consumer research carried out by Jigsaw around phone-paid Subscription Services, and research by Craft in relation to high levels of complaint about Online Adult and Competition Services have reached consistent conclusions, which can be summarised as follows:

- it is quite possible for consumers browsing online to provide unintentional consent to a phone-paid purchase, as they do not always realize they have been taken into a purchase environment. In many cases consumers are unaware that they can be charged to their phone bill While browsing the web.
- Where a service has not been "sought" – i.e. the consumer has not gone onto the web expressly to make that purchase – then a degree of friction is helpful to the consumer to let them know they are in a purchase environment
- consumers expect clarity about what they are signing up to. In particular, price and the fact that a charge will be made to their phone bill.
- Established norms from other forms of mobile payment (i.e. not to the phone bill, but carried out using a handset) are helpful, as these are the cues consumers expect. Such as use of a password, fingerprint, or PIN number.

54. Requirements relating to the consumer experience of web-based phone payment have already been set for Subscription Services and some one-off purchases for some service types as part of Special conditions. We propose to reflect those expectations in this Guidance, on the grounds that it takes account of existing consumer expectations in other forms of digital payment, encourages consistency of consumer experience when using phone payment, and contributes to consumer understanding and confidence in all types of phone payment.

Q2 – Do you agree with the changes to Section 2 of the Guidance at paragraphs 2.9 to 2.13? If not, why not?

55. Section 3 of the Guidance is new. It takes account of the recommendations made by Copper Horse in their report following testing of Level 1 provider payment platforms. As with all PSA Guidance, these proposed expectations are not absolutely binding on providers in the way that the Code or Special conditions are. Providers may generally meet the expectations within Guidance by alternative means, provided they deliver the same consumer outcomes to equivalent standards. However, a failure to demonstrate that the expectations within Guidance have been met, either by compliance with the expectations or by properly evidenced alternatives to achieve the same result, may result in a PSA Tribunal refusing to accept any transactions carried out on a platform as having valid consent. The recommendations can be grouped as follows:

- technical – i.e. specific technical standards that platforms should adopt
- staffing and training – i.e. clarification of roles and responsibilities, and the training and qualifications that identified roles should have or undertake
- risk control and incident response – i.e. such processes as allow risk to be assessed, recorded and acted upon, and that allow for immediate, comprehensive responses to any emerging incidents.

Technical expectations

56. There are underlying standards which ensure that platforms operate using up-to-date software, are configured in such a way as to provide fundamental security within the platform architecture and settings, and interface securely with web pages and external systems. The technical expectations we have proposed reflect this consideration.

57. Lastly, we have attached the technical recommendations as an Appendix to the Draft Guidance. This is with the intention that the list will be reviewed and updated as appropriate by the PSA, subject to consultation, on an annual basis, in order to prevent depreciation of the standards as technology and attack vectors evolve.

Q3 – Do you agree with the proposed Technical Expectations? If not, why not?

Staffing and training expectations

58. No matter how technically secure, payment/consent platforms can be compromised by bad judgement on the part of those who are responsible for them. The likelihood of bad judgement is heightened in an emergency, or when staff do not have a clear idea of their responsibilities in relation to the platform and how to discharge them. One example would be a platform which was technically configured to identify attacks and raise alerts, but the alerts were not acted upon in a reasonable time due to staff illness or incompetence.

59. In order to ensure that relevant staff have the right qualifications, training, and clarity as to their responsibilities, the PSA has proposed expectations summarized as follows:

- all platform operators to have adequate staffing with roles focused on security and fraud prevention. These staff must have a veto over any platform updates and alterations which they deem to be unsecure and have appropriate qualifications and/or experience
- all platform operators to have a Head of Security, with appropriate qualifications and/or experience
- Single Point of Contact (SPoC) for any emerging threats or issues, which moves up the management chain when the SPoC is absent
- all platform development staff to be adequately trained in, and apply, secure development techniques on an ongoing basis.

60. In proposing these expectations, we acknowledge that we have set out further clarity around the expected qualifications and/or experience for security staff. However, these expectations have been drawn from existing and generally recognised standards for cyber security and web security, whether relating to phone payment or not, such as the National Cyber Security Centre expectations[10] in relation to their assurance. Given that security and development staff will be responsible for implementations and incident response in relation to national payment architecture, we do not consider these expectations to be disproportionate.

Q4 – Do you agree with the proposed Staffing and Training Expectations? If not, why not?

Risk control and incident response

61. As well as staff who are fully aware of their roles and responsibilities, and adequately trained to discharge them, it is also important that payment platform providers have adequate processes to quickly identify, record, communicate, and control risk, and to also ensure lessons are properly learned afterwards.

62. If platforms are not properly configured to identify threats, or if issues and actions are not recorded and learned from, then risk will not be properly reduced. An example would be a platform provider who quickly moved to identify and prevent or mitigate attacks, but did not then apply any lessons they had learned in order to re-configure the platform, or change their risk assessment of the Level 2 provider merchant(s) concerned.

[10] NCSC provide 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 CBI and a number of insurance organisations which are offering incentives for businesses. From 1 October 2014, the Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

63. In order to ensure that platform providers have proper threat monitoring in place and are able to dynamically assess and act on the risk posed by individual merchants, services, or types of unethical hack, the PSA proposes expectations which we have summarised below. As before, these have been drawn from the recommendations made in the Copper Horse testing report:

- maintenance of a risk register, which contains specified information about each recorded risk
- active threat monitoring measures, which can monitor systems and alert staff in real time, and specific expectations about how they will function and the types of threats or exploits they will search for
- security alerts or flags acted upon in a timely and appropriate way
- Level 1 providers to have in place contracts with merchants which allow suspension or termination of any fraudulent clients or traffic immediately
- MNOs to consider suspension and/or termination policy for Level 1 providers or other platform providers whose platforms are consistently and/or significantly compromised, and to have the necessary contractual arrangements in place to suspend or terminate quickly, for these reasons
- all platforms to undergo CREST accredited penetration testing on an annual basis, with results made available to MNOs and PSA.

64. In proposing these expectations, we acknowledge that we have set out detailed expectations around threat monitoring in particular. As before, these expectations are drawn from generally recognized security standards, and so we do not consider it disproportionate to apply them to a national payment architecture.

65. In proposing an expectation that all parties will undergo annual CREST accredited penetration testing, we note that this has already been added to the contractual requirements that MNOs set for Payforit accredited aggregators and for providers who use third party consent/verification platforms. However, we also note that penetration testing will need to be conducted according to a broadly consistent methodology, in order that a standard can be established and maintained as the market evolves. The PSA and MNOs will discuss how this can best be achieved, with a view to the first round of annual testing being conducted before the end of 2019, in order that any necessary actions that arise from testing can be taken before the close of the 2019/20 financial year.

66. Lastly, we note that some of the expectations set out here link to wider Due Diligence and Risk Assessment and Control (DDRAC) expectations. The PSA will review its existing Guidance and expectations around DDRAC later on this year, and will ensure that expectations in both sets of Guidance align where relevant.

Q5 – Do you agree with the proposed Risk Control and Incident Response expectations? If not, why not?

Impact assessment

67. In proposing the expectations previously set out, we have analysed potential impact in two main areas:

a) impact on the market

b) cost and other resource.

Impact on the market

68. Having considered the market impact of our proposals, we do not consider them to be disproportionate in terms of the effect on legitimate revenue.

69. Consumer research carried out for PSA over the last three years has consistently demonstrated that consumers are familiar with consent processes that carry additional friction in other forms of digital payment. Research has also demonstrated that consumers generally welcome extra friction and clarity as to when they have entered a payment process, where the product is one they wish to buy. We note that the Payment Services Regulations 2017, which implements the revised EU Payment Services Directive in the UK, requires additional verification steps for online purchases which are now being introduced by Payment Services Providers.

70. We recognize that some of the enhanced standards set out within Section Two of the Guidance have also formed part of the recently published Special conditions that apply to all forms of phone-paid Subscriptions, which carries a greater financial risk to consumers. However, it is also clear that the broader evolution of digital payment has led consumers to expect certain information and cues during a payment process. We consider that the application of a raised expectation within Guidance will help to create a consistent payment experience that will give consumers greater confidence in phone payment as a whole.

71. Copper Horse's testing, while not identifying immediate evidence of ongoing consumer harm, consistently identified weaknesses which could be exploited by rogue Level 2 provider merchants to fabricate consumer consent. Accordingly, the PSA's considerations and action as a result of the recommendations within the testing report, should not have an effect on revenue which can be clearly and robustly linked to consumer consent to a purchase.

72. We note that Level 1 providers could be suspended or even cut off completely (either by one or more MNOs, or as the result of a PSA Tribunal decision) if they fail to implement relevant measures to protect consumers. This carries some risk that legitimate traffic could also be affected. However, we note that legitimate traffic would be able to seek payment facilitation through other Level 1 providers and/or consent platforms, and so the longer-term effect would likely be to redistribute legitimate traffic rather than to force it out of the market.

73. In light of this consideration, we do not view that the proposed new Section 3 of the Guidance will affect legitimate market revenues.

Cost and other resource

74. We note a number of costs, either in terms of initial capital expenditure or ongoing costs, which will arise from our proposals. These are:

- potential cost of recruitment of appropriately qualified security staff
- cost of initial and ongoing training – for security staff and developers
- cost of upgrading threat monitoring capabilities on an ongoing basis
- cost of annual, CREST accredited, penetration testing.

75. We consider costs arising from deployment of existing staff time – such as to maintain a risk register – are not significant.

76. We note that some of the other costs listed at paragraph 74 above may be significant. Desk research suggests that the salary ranges for Cyber Security staff and a Head of Cyber Security would be £30k-£50k and £70k-£90k respectively. Assuming a daily rate of £3k for training, we would estimate a necessary budget of between £6k and £12k per year, depending on the number of staff being trained and the duration. In terms of upgrading threat monitoring, this is dependent in part on the existing capabilities of Level 1 provider's systems. For example, a system which already has the capability to identify threats and actively analyse threat data will carry less expenditure to update than a system which needs to be overhauled. Lastly, we would estimate between £5k and £10k for annual, CREST accredited penetration testing according to a standard methodology.

77. We would welcome any credible estimates associated with the costs and consideration above from respondents. In particular in relation to specific costs which would arise from specific details within our proposed expectations.

78. However, our general consideration is that the proposed expectations do not go beyond existing, nationally recognised standards for web security. As such it could be reasonably expected that credible phone payment/consent platforms with a national reach are already meeting these recommendations in whole or in part, which would in turn serve to defray the amount of initial capital expenditure and ensure ongoing costs are already budgeted for. We note, for example, that we are aware of aggregators who already have in place permanent, dedicated security staff, platforms which actively monitor and analyse threats, and conduct annual penetration testing by an independent party.

79. An additional consideration is that we note the majority of these expectations have already been set for Level 1 providers, other consent verification platforms, and Level 2 provider merchants as appropriate, as part of the MNOs revisions to their existing contractual requirements. This means that in most cases the costs referred to above will not be incurred solely as a result of PSA's proposed expectations.

Responding to this consultation

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 or have given to the Phone-paid Services Authority is used, stored and otherwise processed, so that the PSA can obtain your opinion about the PSA's proposed expectations and Guidance for Consent to Charge and publish them along with other views and the outcome of the consultation.

Further information about the personal data you give to the PSA can be found at https://psauthority.org.uk/privacy-policy.

The closing date for responses is 11 October 2019.

Where possible, comments should be submitted in writing using this form and sent by email to consultations@psauthority.org.uk.

Copies may also be sent by mail to:

Mark Collins
Phone-paid Services Authority
40 Bank Street
London, E14 5NR

If you have any queries about this consultation, please email using the above contact details.