PSA Consultation on revised Guidance for Consent to Charge

Attn: PSA, Mark Collins & Emma Bailey
40 Bank Street
London, E14 5NR

Response From: MCP [redacted]

General Foreword

MCP welcomes the Guidance consultation which updates what is considered 'robust consent to charge' (section 1-2 of the Guidance) because it closes loop holes that may have contributed to consumer harm and complaints. The proposed new Guidance also adds 'new' platform security recommendations (section 3 - from Copper Horse joint project work), to set out standards expected of payment / verification platforms and how they're maintained. While understanding the rationale for this, our view is that it makes the Guidance complex and overly cumbersome. Joining up Mobile Operator 'Payforit accreditation standards' with other 'technical standards' recommended by Copper Horse makes sense when addressing the technical security requirements of Industry payment platforms. However, the Guidance strays beyond a guide to meet the Code of Practice outcomes specifically in Section 3, where it details Staff Roles and Responsibilities and Risk Management and Control.

While this is 'Guidance' and not Code, PSA has made it clear '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'. By default, a PSA Tribunal will consider whether all Guidance was followed to achieve the Code outcome. So, Guidance needs to separate clearly what is essential to meet the Code outcome and what are best practice standards. As an example, meeting the Code outcome of Consent to Charge will fail if the stated requirements in section 1 of the guidance are not followed. There has been no evidence presented in the consultation where other factors have contributed to failures of Consent to Charge - eg having a Head of Security with 5-10 years experience in cyber security, leading a cyber security project, holding ISO27001, maintaining a ledger of every cyber security issue, having regular training etc. It is our view that these are non-essential to meeting the Code outcome and are best business practices rather than holding a place in regulatory Guidance. We feel that mobile operators and Industry partners will have alternative ways of reaching these best standards.

MCP also feel that PSA should have addressed the potential for fraud in a more meaningful and researched way, as a possible contributor to complaints about consent to charge failure. During the consultation MCP has discussed this with PSA and feedback is fraud is a criminal matter and to this extent is not relevant to providers meeting the test of consent to charge. However, our view is that

PSA and Industry has evidenced fraud as an issue (the scale of which has not been determined) and therefore it is not possible for providers to 'prove that the consent could not have been given in any other way than by the consumer's specific actions', other than combining the consent to charge requirements with an anti-fraud solution. It would be pragmatic for PSA to advise in Guidance that certain forms of opt-in / consent have a greater exposure to such threats and may not reach the standard expected for robust consent to charge unless these factors have been considered.

Q1 Do you agree with our definition of informed consent at para 1.4.

Generally, Yes.

There is no specific question relating to clause 1.5, 'robust consent' however we feel PSA should add more detail here to determine the consumer actions.

As part of the transaction, MCP captures very detailed information with regards to device identification, including extensive device finger printing with detailed user interaction parameters (mouse up / mouse down / click data / fingerprint radius). We capture over 160 parameters of this class of data. This tells us definitively if the user is human or programmatic. This absolutely proves that the consent could not be given in any other way than the consumer interaction.

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

Generally Yes, but we have other comments on this section.

Regarding general changes to section 2, we feel PSA should be consistent with reference to potential for fraud that may undermine proof of consent for each different consent method. All forms of consent to charge listed are open to fraud but Industry needs to judge the threat for each. PSA cites the potential for MO fraud and states that network technical barriers limit the potential for premium voice. In certain markets MCP sees malware on handsets generating fraudulent calls to voice services, likewise MO fraud. PSA states that the UK technical infrastructure is robust and the best approach is PSA to investigate given grounds to. We agree with what has been written by PSA regarding voice and MO. Looking at current services using MO, we would suggest that any beneficiary of fraud would be extremely limited/rare. So, we would suggest that PSA have a caveat statement across all forms of consent method, that L1s will need to consider the services running on their platform to assess whether there is a greater threat to 'robust consent to charge' and determine whether additional security fraud measures are required.

In our view, services running via other consent methods (aside from voice and MO) do require additional security / fraud measures. Regarding web and pin entry, we do not consider that the platform standards proposed in Section 3 will make for robust consent by themselves. All PIN-entry systems require a web end-point – a HTTP server that serves up a 'PIN entry page' for the user to

MCP Insight Ltd
Sovereign House, 155-157 High Street, Aldershot, Hampshire, GU11 1TT
VAT No. 916666301 – Company Registered No. 05502020

view, and acts as the recipient or end-point of the user's form POST – 'enter your PIN here'. This end-point is easy to hack by both fraudulent APKs on the handset or even server-side headless browsers.

Therefore all PIN end-points must be protected. This protection needs to address two groups of parameters – device-oriented parameters and user-event data. In simplistic terms device-oriented parameters are looking at the device fingerprint to see if the identifying parameters are being 'spoofed'. User-event data is different – it is checking to see if the events (page-up, mouse-down, click etc) show that the PIN has been entered by a human on a keyboard.

A PIN end-point without protection is wide open to this type of fraudulent behaviour.

Regarding 2.9 we would ask PSA to manage expectations of what is a reasonable time for PIN expiry? Is two hours reasonable, but 24 hours not?

Also, regarding PSA statement: 2.9 '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'. We would suggest alternative considerations eg the message could be in question form (virtual captcha) which is unique and requiring a simple human response.

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

Generally Yes.

The requirement in Section 3 is maintaining a robust consent to charge platform and we agree with the basic technical standards suggested in Appendix A and that these should be regularly updated. We also agree with necessary PEN testing to ensure platforms are stress tested and security standards maintained.

However, while L1s may have updated their platforms as a result of a 1+ year's Copper Horse work with mobile operators, these requirements are new for Verification companies. We would suggest that the timescales are tight if PSA want to introduce the Guidance by the end of 2019 and feel these expectations should be consulted on with such companies.

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

Generally No.

The vast majority of this section is too prescriptive on how a company performs its day to day operations and this section should be best practice.

PSA sets out in 1.5 what they consider to be robust consent state and achieving this will naturally

MCP Insight Ltd
Sovereign House, 155-157 High Street, Aldershot, Hampshire, GU11 1TT
VAT No. 916666301 – Company Registered No. 05502020

include certain security criteria (Appendix A) to ensure platforms are robust and data records cannot be tampered with. The Code outcome of demonstrating robust consent to charge can be achieved up to this point in Section 1-3. How staff are trained and the qualifications they possess may influence risk management but it is not something that should form part of Guidance to achieving a Code outcome. Companies should have the flexibility to select staff they feel can achieve the overriding objective, without strict lines on what qualifications and experience the staff should have. Certainly stating how many 'years of experience' is potentially discriminatory to include in regulation; and PSA should not be prescribing 'Project Lead' experience, ISO standards and NCSC certification. These are best practice standards. Guidance should at best recommend security training, rather than setting out expectations. PSA don't go as far to set out qualification and experience expectations for 'Compliance Managers' and so this is not consistent with other areas of meeting Code outcomes guidance.

We do agree that there should be a SPoC and senior responsibility for security standards.

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

Generally No

We agree that an internal register of issues and resolution should be kept as standard company good practice but not with the prescription of informing network operators, PSA and any other relevant authorities about issues ongoing, unless there is a legal requirement to do so.

Network Operators are at liberty to require information prescribed in this section in their contracts (including regular auditing, CVSS etc) and we know MNOs have done so.

While we appreciate the intent PSA may have for companies to report and share intel on security breaches, it is not normal for regulators to mandate/guide that providers report every security breach or issue. And it should not form part of meeting a Code of Practice outcome.

We do not agree with the prescription which follows around how the risk register is maintained and information shared. In keeping with all tech platforms the expectation is that platforms will suffer numerous attempted hacks and attacks. Procedures for risk control and risk mitigation are essential to any payment and verification platform. Good companies will adhere to well thought through processes and those with good security and fraud prevention systems will likely highlight more issues than those using lesser detection systems. PSA needs to consider the pragmatic sense of such shared information and whether it is in the individual interests of the provider to do so in a codified and prescribed manner. Generic findings may be shared but this may raise more questions to the validity of that data without detail.

We would also suggest companies build significant IP by countering attacks effectively. Maintaining a risk register and sharing the security data is not essential to achieve the Code outcome of robust Consent to Charge, it depreciates a company's IP (competitive advantage) when published and adds an unnecessary admin burden to keep all informed. There are numerous more established

platforms to share and research cyber security information and the resource requirement here seems to outweigh the value.

Conversely specialist companies like MCP, who run a risk register and analyse security breaches and fraud as a business, may benefit from advising others on how this is best done and publish data to generate brand awareness. But I don't think this is the point of the exercise.

Other – Verification Platforms

3.9 states, "Where a consent verification platform is operated by a third-party, who is not directly involved in the value chain, then the PSA will be unlikely to accept as compliant any payment verification which is not initiated by a Level 1 provider, with whom the third-party provider has contracted. As part of any contract between a Level 1 provider and a third-party consent verification platform, the Level 1 provider must satisfy themselves that the platform meets the standards and expectations at paragraphs 3.6 and 3.7". We would argue that robust consent to charge should be 'independently' provided by a third party, that does not have value chain commercial interest. The issues of complaint and lack of consent to charge raised in PSA cases demonstrate that the aggregator was at fault due to the lack of thorough due diligence on consent transactions. An example is porting opt-ins from one aggregator to another without checking (in a truly random fashion) that those transactions have robust consent. So, really PSA should be ruling that L1s contract with an independent verification company.

Irrespective, we are pleased to see that PSA has listened to MCP lobbying over recent years, to make necessary changes to the Guidance, and agree that a third party verification company should contract with the L1, to provide absolute transparency and proof that all transactions are verified.

PSA State that in addition, 'the third-party will be expected to provide data of payment records and other relevant information to mobile network operators'. Can PSA clarify this requirement because payment records are held by the L1 and not the responsibility of the Verification company?

As at 3.7.f), mobile network operators should have in place such 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.

3.7f) has no part in regulatory guidance. The Guidance sets out clearly that Verification platforms have to conform to a common standard as set out by PSA. As part of PSA Guidance, an MNO should therefore only be able to refuse to accept verification by a third-party platform where there is proven failure to meet the standards set by PSA. It is at the discretion of the MNO what they write in their own contracts but not for PSA to dictate so, otherwise this may be construed as anti-competitive.

MCP Insight Ltd
Sovereign House, 155-157 High Street, Aldershot, Hampshire, GU11 1TT
VAT No. 916666301 – Company Registered No. 05502020