Phone Paid Services Consultation discussion document on Code 15

Q1 Do you agree with our proposed overall approach to the review? Please provide an explanation as to why you agree or disagree.

We agree with the proposal in principal and believe that it is well intended. We see it as an opportunity to redress the balance, to become more in tune with consumers. We feel that for too long the PSA has focused on relationships with industry at the expense of consumers.

Q2 Is there anything else we should be considering?

In our view the PSA have closed avenues of communication with consumers, by blocking legitimate complaints on twitter, closing the PSA Facebook support page, and by not investigating individual complaints, the PSA is out of step with consumers. The addition of a Consumer Panel is welcome in theory, however this is no substitute to listening to the complaints of real consumers. The Consumer Panel is hand selected by the PSA, and is not representative of typical consumers who have experienced unexpected charges. We are doubtful any panel members have used any of the services. When individuals who have actually been scammed by the services have applied to join the PSA Consumer Panel they have been not been admitted to the panel, as the PSA do not want to hear negative criticism and prefer a Consumer Panel with no real insight or knowledge. Ultimately there is no substitution for day to day dialog with real consumers.

Q3 Do you agree with our assessment of the market? If not, why not? Is there anything else you think we need to consider?

There is massive scope for market growth, and we would not want to see the positive growth in the industry stifled. The good that comes from charitable donations etc must not be allowed to be dragged down by bad actors. Unfortunately we feel the PSA have not had sufficient powers to deal with rogue companies that have massively damaged consumer confidence in the industry. The large blue chip companies will be reluctant to associate themselves with a payment platform known to be full of scammers.

The ability to charge to bill has a lot of scope for streaming services but to be successful consumers need to have confidence and that confidence can only come from a robust 15 code of practice that has consumer protection at the heart. A robust code is required that gives more responsibility to the Mobile Network Operators. The MNO's host the services and although the MNO's should not be responsible for monitoring the content that they offer, the MNO's should be responsible for ensuring that service subscriptions and purchases are legitimate before handing over funds. Where they are not legitimate a consumer should not be chasing merchants for refunds. We can think of no other payment platform that requires consumers to chase refunds for purchases that the consumer claims are fraudulent. For the market to flourish, MNOs need to have robust processes in place to ensure consent to purchase is legitimate, and operate a fair chargeback mechanism where disputed claims can be reversed pending investigation.

Q4 Do you have any evidence of the market to share with us that you think would support our assessment?

Hundreds of TrustPilot reviews all extremely negative towards one company using the words scam and fraud with almost no positive reviews, examples like this makes “Charge to bill” synonymous with scams. Charge to bill needs to be more in tune with consumer’s expectations. There are examples of 3g routers being used as WIFI hotspots being charged to the router owner and very little consumer knowledge that it is even possible to incur charges in such a way.

Consumers have expectations of all payment processors, including the networks currently exempted from the PSD2 regulations

- They expect them to give help in identifying charges that the consumer does not recognise

- They expect the payment processor to secure evidence that a payment has been authorised by the account holder before the payment is transferred

- They expect them to have a disputes procedure where consumers can dispute unrecognised or unlawful charges

- They expect the payment processor to be able provide full details of any disputed transaction with dates and times and methods of verification secured at the time of the transaction.

- If the payment processor maintains that the payment was lawful, the consumer expects to be given a detailed explanation of the reasoning and justification behind this.

- They expect a transaction reference (other than account number) which they can use to help a supplier identify a charge they have made.

- They expect to be able to ask for disputed continuous payments to be stopped, so that no further charges are made.

- They expect refunds, where suppliers agree to them, to be paid by payment back into their account or better still by reversing the disputed transaction. They don’t expect to be asked to take a text to a Post Office.

- They expect refunds, where agreed, to be processed with the same speed and efficiency as the original disputed transaction. They do not expect to be asked to provide unnecessary personal information as a condition of being refunded.

- They expect the provider to be aware of suspected fraudulent activity and take action to protect them from abuses of the payment mechanism

- They expect to be able to opt-out of the payment mechanism completely, like for example stopping a card when it has been compromised or stolen. All consumers should be able to ask for a "charge to bill" bar, to prevent their phone account being used for 3rd party purchases. As a regulator PSA should be insisting that all networks offer this protection and recommend that it be used by vulnerable consumers.

- They expect the payment provider to be aware of complaints made against particular vendors and to exclude them from using the payment mechanism where they generate a disproportionate number of complaints.

- They expect the risk of fraudulent transactions to be very low, due to the payment processors having fraud detection and prevention measures in place.

- They expect the processor to be able to spot trends in complaints and take steps to perform additional verification on transactions which may be suspect. Consumers have these expectations because of their experience with reputable FCA regulated payment processors. The systems for "3rd party" charges made to phone bills have lagged behind developments in regulated payment systems and have, as a result, become a target for fraudsters. It is completely wrong that networks are requiring their customers to pay charges for which they hold no evidence of consent.

Q5 Do you agree with our assessment, based on research, of consumer behaviours, experience and expectations?

Broadly speaking we do not dispute your assessment. The assessment is based upon alignment with other payment platforms, and recognising that larger reputable blue-chip companies have a lot to bring to the market, and that in the past a lot of damage has been done by smaller market entrants who only operate mobile payment services. These services have offered weak products as a façade to exploit click jacking etc to gain subscriptions, and play a numbers game hoping many will not notice charges, and deliberately making refunds difficult in order to gain income.

Whilst we appreciate that the simplicity and friction free environment, in the past has made mobile payments a unique environment with big potential, many services in the past have exploited this friction free loophole and obtained payments without consent. Technology and legislation has changed since the previous code of practice was written, and technology and legislation will continue to change. Many mobile phone software markets now have a frictionless environment to confirm charges by mobile phone facial recognition or fingerprint authentication. Charge to mobile with its verification process has become more cumbersome to purchase software than the Apple App Store or Android Market Place. For charge to mobile to remain relevant, it must adapt. A frictionless environment with charges added to a phone bill has great potential, but only if managed correctly. Pre-purchase information must be provided with payment clearly shown. Security processes in place must be comparable with other payment methods, with secure customer passwords, or phone built security devices like facial recognition which must be verified by the MNO before taking payments. There should be a check out screens from the MNO displaying the consumers billing details, and text messages from the MNO about the charges are less likely to be ignored and unread. A way of managing the consumer's purchases and subscriptions should rest with the MNO, with consumers able edit subscription preferences, online via the MNO website, or by call to the MNO. Consumers are understandably reluctant to reply and text back scam messages.

The MNO's should serve as a point of contact for unauthorised transactions. Another requirement for a consumer friendly experience is a chargeback mechanism whereby disputed charges can simply reversed by the MNO.

Although consumers should always check their bills, we know that many do not, and small regular charges often go unnoticed. Bills being paid on behalf of vulnerable relatives or children often escape scrutiny by the bill payer. A text message reminder from a network is less likely to be blocked and unread.

I know that the PSA are aware of considerable consumer harm by certain services, yet appear to allow these scams to continue unchecked. For this reason I find it quite understandable that the PSA Facebook page became so toxic and critical of the PSA's inability to stop scams that you decided to close it. The PSA need to listen to consumers more, consumers do not generally complain in their thousands about scams without good cause. I feel all too often the consumer is blamed for the "unexpected charges" however, clearly many people are not aware that mobile phone paid services even exists.

Unfortunately, being an accountable public authority charged with balancing the health of an industry and the welfare of consumers, there will be no shortage of angry consumers if you get the balance incorrect. As regulator it is important that you interact with disgruntled consumers, not close your Facebook support page and block Twitter users that you disagree with. I've lost count of the number of scam victims I've emailed and spoken to who feel unrepresented.
It is positive that the PSA have a consumer panel, but sadly I feel that your PSA selected consumer panel is not representative of consumers. I would be surprised if anyone on your PSA panel had ever used any phone paid services, particularly the services that are causing harm. No email address on how to contact them is advertised on your website, and I cannot see where your panel are able to determine the nature of consumer harm some of the services are causing, and champion consumers. The PSA need to be more in tune with consumers, re-establishing the facebook page, holding meetings with consumers, and a method of contacting the consumer panel are all essential changes that need to be made.

Q6 Do you have any other evidence in this area that we need to consider?

We are disappointed that PSA are not routinely advising consumers that they can ask their network for a charge to mobile bar. There are some circumstances where phones may be purchased and being paid for by a responsible adult and supplied to the vulnerable or children. In these circumstances simply providing advice that a charge to bill bar can be an option to protect yourself is absolutely be appropriate. The PSA is there to protect children and vulnerable, and provide impartial advice for that means. Phones supplied to children and vulnerable adults seem to be disproportionately affected by these charges and no effort is made by PSA to inform bill payers of this option. Another common issue is that of 4G WiFi routers becoming subscribed to "services". There is no mystery to this. Any device connected to the router can subscribe it to a "service" using the "two click" method. Of course, the resulting subscription text messages will be sent to the router, which may or may not be able to handle them, and are unlikely to ever be seen by the router owner. We feel that 4G routers should be supplied with a charge to mobile bar already in place.

Q7 Do you agree with our assessment of what the future holds? Please provide an explanation as to why you agree or disagree.

Not sure this assessment is entirely how I see the future, if left as it is, "charge to mobile" in its current form, we believe does not have a future. As previously mentioned software can be purchased nearly completely friction free using a fingerprint or facial recognition easily from trusted market places with huge choice. In 2014 the PSA commissioned Deloitte to study the market and the report recommended that PRS must play to its strengths. The main strength was "The ability to make purchases without leaving the current screen and disrupting content." Unfortunately due to the massive harm of subscription services have caused, the requirement of two factor authentication does not allow the ability to make purchases without leaving the current screen anymore. Two factor authentication procedures in place are now somewhat cumbersome and inconvenient when compared to comparable technology. The scams synonymous with payforit, the no longer friction free nature for authentication, difficulty in obtaining refunds and poor regulation will see charge to mobile demise unless changes are made.

There may be scope for growth, if managed correctly as a mobile phone contract can add charges to a bill which is usually payable retrospectively. Adding charges to a bill is a convenient way to pay for something after pay-day if funds are not available at the time. Charge to mobile can only works as a viable payment platform if it can be as simple and friction free as other platforms and regulated appropriately and brought into line with the security, trust and safety offered by similar platforms.

Systems must modernise for charge to mobile to be a success, making use of phone in-built security features to authorise payments, or a failsafe purchase environment that is the MNO's responsibility to keep secure that is not susceptible to click jacking etc. must be the norm.

Q8 Are there any market developments which we have not factored into our assessment? How do you see these influencing the phone-paid services sector and associated regulatory challenges?

If this system does not completely change its implementation and modernise it has no future, an App on the phone managed by the MNO allowing purchases to be viewed, managed, and authenticated, creating a parallel marketplace to rival the existing software market places has massive potential, as it could remain frictionless, and be authenticated by the phones inbuilt verification methods (including future methods developed). There is massive potential to set up innovative, convenient, profitable services, but it requires collaboration. There must be modernisation and purchases should be managed, verified and authenticated, possibly through an App made by the MNO's or Level 1 Aggregators. Then it will be obvious to consumers they are making a purchase, and unexpected charges will reduce. This App would have phone inbuilt security measures and could prevent the thousands of complaints generated.

Q9 Do you agree with our proposed assessment framework? Please provide an explanation as to why you agree or disagree

We agree with the principals outlined, however the implementation is key. In the past there have been too many weak areas of the code of practice that have been cynically exploited doing massive consumer harm. The PSA should be aiming to make the code robust, and more capable of stamping out the bad actors that do the damage quickly.

Q12 What are your views with regards to how we can best ensure that all firms operating in the phone-paid services sector will follow, and be held to, the same standard of professionalism?

It is clear that the checks being made under Code 14 are wholly inadequate. The recent Veoo case illustrated the problem [redacted] as long as they are able to distance themselves from it sufficiently to avoid regulatory action against themselves. The only way to rectify this is to make Networks and Level 1 providers fully responsible for breaches of the code by their Level 2 "partners". In a case where a Level 2 provider, or one of the other parties lower down the "value chain" is found to have breached the code, the MNO and the Level 1 provider should have to prove that they took every possible measure to perform due diligence and risk assessment of the party guilty of the breach. In the absence of adequate proof, there needs to be a fine which more than removes the benefit from allowing a non-compliant service to operate.

One particular Level 1 provider has consistently worked with companies which have a very poor reputation for compliance and which generate large numbers of complaints. We believe that they are behaving as irresponsibly as Veoo did, but have so far avoided regulatory action. It is our belief that Level 1 providers that knowingly allow such services to use their platform would not do so, if the financial penalties were a sufficient deterrent.

PSA need to ensure that upward accountability of the type we describe above isn't just a theoretical concept, but that it is ruthlessly applied to remove the financial benefit to MNOs and Level 1 providers of fraud perpetrated by bad actors lower down the value chain..

Q13 What are your views with regards to developing appropriate 'Pre-purchase standards?

If the pre-purchase phase required the phone user to download a purpose built charge to mobile app that was required for authentication, management, billing history, etc this would have massive benefits for consumers. Existing technology of a safe phone app would remove the ability of rogue merchants to initiate payment without consent using clickjacking, because verification could be end to end encrypted through the App with the existing phone security features. The downloading of the App once would be a step informing consumers they were entering into a market place. Continued use of the MNO/Charge to mobile app would become a familiar setting, and could feature a market place for additional charge to mobile content, and way of managing subscriptions etc.

The charge to mobile payment flow could become frictionless once more, after a download of an app, agreement to terms and conditions, and confirmation the phone user is also the bill payer.

Q14 What are your views with regards to developing appropriate 'Purchase standards?

Mobile phones come pre-loaded with the ability to make purchases. Many people do not realise this fact and there needs to be more clarity that a consumer is entering into a market place. Until vulnerabilities like clickjacking or iframing etc are negated, I cannot see how there can ever be appropriate purchase standards. The whole premise of adding things to a phone bill is fundamentally flawed if rogue software can be implemented in malicious ways to obtain illegitimate consent, and fake One Time Only PIN codes. There must be greater security.

Q15 What are your views with regards to developing appropriate 'Post-purchase standards?

Unfortunately charge to mobile is fundamentally flawed, "unexpected charges" are a fairly unusual phenomenon experienced in other software market places, but common on phone paid charges. Digital Software is typically consumed and considered un-refundable in most circumstances. Get the pre-payment information, and the consumer aware they are in a purchase environment and there should be no huge need for refunds.

We welcome no quibble refunds for the purchases that are made without consent (eg made by children without adult consent etc) but the consumer should be able to obtain this refund from the MNO, and not have to chase the merchant.

Q16 What are your views with regards to how we can make our investigations and enforcement procedures more effective?

Having attempted to investigate fraudulent charges ourselves, we fully understand the difficulty encountered by the PSA. Just finding the route by which the consumer became "subscribed" can be extremely difficult. Even if this is possible, identifying the party behind the exploit is almost impossible, due to the secrecy around affiliate deals. This is why we believe that taking technical measures to prevent fraud is a preferable approach.

Unfortunately any measures introduced to protect consumers are likely to be circumvented. Within weeks of PSA introducing the use of a One Time PIN for subscription services, we discovered that some services were displaying the One Time PIN on the signup screen, completely defeating the intended purpose and resulting in complaints from consumers that they had somehow become subscribed to services they had never heard of.

Close monitoring of services, and of consumer complaints is essential. Where a service begins to attract large numbers of complaints, a close examination of those complaints might help identify the

cause. We encourage consumers, as well as reporting their problem to PSA, to leave the service a review on Trustpilot. There are often details in these reviews which help identify the likely cause.

One problem is that many consumers are not sure how to access their web history, which can often be very useful in obtaining the signup links used. Interestingly, few consumers report PSA asking for this vital information. The speed of investigations is also important. It does PSA no credit that some services are allowed to operate for months, making unlawful charges to consumers, when it is patently obvious that something is seriously wrong. PSA should have the power to suspend services generating a disproportionate numbers of complaints, pending investigation. They should also have the power to suspend services and issue administrative fines where a service does not cooperate with an investigation. Above all, the outcome of investigations should be communicated to consumers who have made a complaint, even if the investigation gave the service a clean bill of health.

Q17 What are your views with regards to how we might achieve better outcomes for consumers and uphold the reputation of the market through more effective deterrents by considering the range of sanctions available to us?

Outcomes for consumers would be much improved if services generating disproportionate number of complaints could be suspended while they are investigated. Maybe a threshold could be set for the proportion of charges resulting in a complaint. If this threshold was exceeded for more than a four weeks, the service could then be suspended, pending an investigation. Transparency is vital to public trust. All PSA investigations resulting in a Track1 or Track2 process should be reported. From a consumer's perspective it appears that PSA only investigate a tiny minority of cases and that many of the most serious breaches of the code go unpunished. Publishing details of the outcome of "informal investigations" might go some way towards correcting this view. There is a serious issue with non-collection of fines imposed by tribunals. Sanctions intended to remove the financial benefit of breaches of the code are consequently ineffective. The ability to make directors of companies personally liable would help. However, would this work for companies registered in, say, Belize? We'd also like to see PSA properly consider the possibility of criminal prosecution for fraud, where the evidence appears to support it. A high profile case such as that of Zenhya Tsvetnenko might act as a deterrent. [redacted]

Q18 What are your views on our existing funding model? Does it remain an effective model? Or do you think alternative funding models may provide a more sustainable approach going forward?

We'd like to see a funding model where services pay a levy based on the amount of work they create for PSA. If subscription services generate a higher volume of complaints, they should pay more. A "polluter pays" approach might help clean up the industry.

Q19 Do you consider the current categories of defined providers capture all relevant providers involved in the provision of phone-paid services and appropriately spreads regulatory responsibility throughout the value chain? Please provide an explanation as to why you agree or disagree.

We disagree. We have seen high levels of harm from affiliate marketers, and have recently seen issues with PIN service providers. Many services use Customer Service providers who act to prevent consumers contacting service providers directly and fail to provide satisfactory responses to consumer enquiries. We have seen service providers seek to blame these other companies for breaches of the Code. It needs to be clear, if regulation is only to apply the three categories identified, that providers will be held directly accountable for the failings of any third party marketing, customer service or PIN provider they use.

Q20 Do you think the current regulatory framework remains fit for purpose? Please provide an explanation as to why you agree or disagree.

No, we believe that the current regulatory framework is inadequate. It fails to properly protect consumers. The current framework is unduly complex with too many add-ons to the code which appear to be unenforceable (and to be fair are probably confusing to service providers). The new code needs to embody existing special conditions and guidance in an enforceable form. The "outcomes based" code has proved incapable of protecting consumers, and it is time to move to something more prescriptive.

Q21 Are there any areas of potential change proposed in this document which may have an impact which you believe should be considered? If so, please let us know, including any evidence you have as to the likely impact

We anticipate that the types of changes proposed will make it more difficult for bad actors to enter the market, and make code breaches unprofitable for service provider – thus encouraging and rewarding compliance with the Code. This would have a beneficial effect on consumer trust and the reputation of the industry.