Q1: What are your views on the review objectives set out on page 4? Has the PSA got the right scope or are there areas the PSA should include or exclude?

Unfortunately, current consumer experience with Phone-paid subscription services is overwhelmingly negative. It is hard to find any positive reviews of these services online. A look at the Trustpilot reviews of [redacted] will show numerous negative reviews from consumers who believe themselves to be defrauded and not a single positive review (at the time of writing). Indeed, [redacted] have sought to suppress valid criticism, rather than answer it.

This suggests that compliance with the regulatory framework is failing to protect consumers from harm or that compliance is not being properly monitored or enforced.

Q2: Some subscriptions generate high levels of complaints, whereas others with similar numbers of subscribers generate very few. Do you have any views on the regulatory measures that would better support growth and innovation across the subscriptions, whilst ensuring consumers are protected from harm?

Whilst being aware that there are other subscription methods (which generate few complaints), the main source of consumer harm appears to be subscriptions collected via 'Payforit' .

Payforit is an archaic and inherently insecure payment mechanism. It has not adapted to reduce the incidence of fraud as other payment mechanisms have. It doesn't have a centralised service for complaints and disputes. It doesn't have a refund mechanism. PSA are well aware of these shortcomings, but do nothing to encourage reform. They know that malicious code in a web page, or in a downloaded App can sign users up to these services, without the consumer being aware that it has happened. They have been aware of the use of these exploits for several years, but nothing has been done to prevent them. They sit on their hands instead of being proactive in bringing these frauds to a halt.

Consumers will compare the consumer protection offered by phone paid services with those of other payment methods (Paypal, Contactless Payments, Direct Debits, Credit Cards, Debit Cards etc). The providers of all these payment methods provide clear mechanisms for the resolution of disputed transactions. Payforit and other direct operator billing methods offer no clearly defined or published mechanism for the resolution of disputes.

If I dispute a direct debit with my bank, the burden of proof will rest on the payee to prove that the debit was authorised and not with the payer to prove that it wasn't! If I report fraudulent transactions to my bank, they will take the matter seriously and put a stop on any further fraudulent payments. The [redacted] don't even offer this minimal level of support. Instead, they ask the consumer to send a message to the fraudster asking them to STOP. To add insult to injury, they are charged for sending this message!

Payforit expects the consumer to negotiate directly with the originator of the charge. What is worse is that, if the recipient of the payment fails to respond, there is no process to follow to resolve the issue. In the absence of a defined process, these uncooperative companies continue to trade for months, until the volume of complaints is such that PSA cannot ignore them.

It is not the role of PSA to adjudicate on individual disputes. However, it could insist on the introduction of a mechanism by which consumers can receive swift refunds when they are defrauded by rogue companies. Much of this could be automated, as it is with other payment mechanisms.

The problem is not that fraud happens. It will happen to some extent with any payment system regardless of the security and authentication measures put in place. Fraudsters are continually refining their methods and finding new ones. Most payment systems respond to attempted fraud by putting effort in to fraud prevention, but this has not happened with the arrangements for charging to a phone bill.

The problem is the lack of any defined process for the consumer to resolve their complaint (within a reasonable timescale) and obtain a refund if one is adjudged to be appropriate. Current arrangements would appear to be in breach of the Consumer Rights Act 2015 as it applies to digital services, in terms of methods and timescales for dealing with consumer complaints, and in terms of the refund process.

Large numbers of consumers have experienced unexpected charges as a result of these 'Payforit' subscription services. Although the amounts involved are usually small (£4.50 per week or less), the companies take advantage of the fact that many consumers do not check their bills, and many consumers lose significant amounts. This 'cramming' fraud has been a persistent problem, not just in the UK but in many other countries. In the USA and Australia, there have been a number of high profile cases where MNO's have been held accountable for fraudulent subscriptions.

https://www.itnews.com.au/news/telstra-hauled-before-court-over-premium-mobile-billing-487699

https://www.consumeraffairs.com/news/verizon-sprint-to-pay-158-million-for-illegal-cramming-of-customers-mobile-phones-051215.html

Many consumers have experienced great difficulty in getting fraudulent subscriptions stopped. The 'Payforit' system can be very confusing, particularly for consumers who do not receive an itemised bill. The text containing the subscription is often deleted as spam. The 'payforit' receipt text does not say which service it relates to. The number to which STOP is to be sent is often different to the number from which the subscription text was sent.

There is no disputes mechanism. Many consumers have been successful in getting a resolution using the UK Small Claims procedure, but this is not available for companies based outside the UK. Currently the EU Small Claims procedure is an option for companies based in EU countries, but this may not be available after March this year. It is not acceptable that defrauded consumers are unable to seek redress because of the high costs of taking proceedings in a foreign court.

There needs to be an independent ombudsman to consider all cases where consumers claim to have been fraudulently charged. Given the ease with which these frauds can be perpetrated, and the inability of the regulator to recognise them, a refund should be given unless there is clear evidence that the consumer knowingly and intentionally entered into a contract.

Direct carrier billing currently enjoys a limited exemption from the requirements of the Payment Services Directive v2 (PSD2).

In fairness, direct carrier billing services should be subject to the same regulations as the payment services they are competing with. The directive provides additional safeguards to consumers. It reduces their potential losses from fraud, and requires the Service Providers to provide robust, two factor, authentication. The directive also forces Payment Service Providers to provide a proper dispute mechanism. Consumers using 'Payforit' are denied the additional protection these safeguards would have afforded them.

In February this year, EE , to their credit, introduced a system requiring a two factor authorisation with PIN for all subscription services. (PSA currently only require this for services charging more than £4.50 per week). There has been a dramatic reduction in complaints of fraudulent subscriptions from EE customers. This suggests that EE's approach has worked. As a minimum, PSA should introduce a Special Condition requiring this for all networks.

It is notable, that although PSA currently recommend the use of two factor authorisation with PIN for services costing £4.50 or less per week, this is ignored by most, if not all, providers. I do not believe this to be accidental, as two factor authorisation with PIN will defeat most of the exploits currently used to implement fraudulent subscriptions.

Q3: Do you agree that different subscription services may require different regulatory responses? Do you have any thoughts on what this variation could look like?

Unfortunately, Phone-paid Services subscriptions have had a high level of fraud complaints for many years. The move from PSMS to 'Payforit' resulted in a temporary drop in these complaints, but these have since increased again. It is probably true to say that as soon as one door is closed, the fraudsters will find another. This means that it is likely that, given time, the fraudsters will find a way of circumventing any protection put in place.

There are two possible solutions:

- More speedy and robust applcation and adaptation of the code of practice to protect consumers as soon as a problem is identified. Currently, one service has been causing high volume of complaints since the beginning of May. At the beginning of October, it is still operating!

or

- A speedy, impartial and simple method of resolving disputes and providing refunds to consumers for charges where consent cannot be indisputably proven. This could be funded by a charge to the service for each case referred, so encouraging these companies to behave responsibly. It would not be fair for these costs to be shared evenly between services since, as you have stated, some services generate much larger levels of complaints (and currently lack any concern about this!)

Where a subscription service carefully monitors usage of the service, and offers speedy refunds when the service has not been used (or has been used only once at the time of subscription), then the current levels of regulation might be appropriate. In Australia, where most third party subscriptions can no longer use direct carrier billing, some services, such as Google Play and Netflix, have been allowed to continue. By only allowing authorised, reputable companies to access the payment mechanism, the risk of consumer harm is much reduced.

It is clear from the numbers of recent cases that the current 'Payforit' system is highly vulnerable to fraud. Furthermore, PSA are, on their own admission, unable to tell the difference between a legitimate signup and one caused by malicious code.

OFCOM, in 2012, wrote:

Internet diallers

6.77 During 2004 PP+ received 57,743 complaints about services using internet dialler software. These included consumers being misled into clicking on an icon or banner, or accessing a website, which, without their knowledge, would trigger the download of software to their PC. That software then used their internet dial-up account to call premium rate numbers operated by the dialler software's owner.

6.78 This scam demonstrates how a fragmented supply chain, with separation between the service provider and the billing party, can be exploited in an (unlawfully) opportunistic way. The greater transparency of PFI services would not prevent this harm. Rogue software can be embedded in such a way as to circumvent any verifiable method of consumer consent to charges (like a PFI checkout).

It follows that any supposed 'consent' from a consumer has to be viewed with suspicion, especially when that consumer is adamant that they did not consent. PSA seem too willing to accept such 'proof' of consent unquestioningly, and place the burden of proof on the defrauded consumer rather than the service provider. The system needs to be reformed so that automatic refunds are provided unless the service provider can **prove** consent **indisputably**. (currently not possible for the reasons above).

Some 'services' for example those operated by [redacted] and [redacted] appear to have been created solely to exploit this vulnerability. Trustpilot reviews of these service are enlightening. There is no evidence that these services have any genuine subscribers, and a great deal of evidence that they are causing consumer harm (despite the efforts of [redacted] to suppress valid criticism on Trustpilot). Services like these damage the reputation of the entire industry.

Companies that genuinely wish to provide a service to consumers should be putting pressure on the PSA to put an end to the fraud and clean up the industry.

Q4: Is there any other information or evidence that you would like to provide to PSA to assist it to undertake more detailed analysis of the existing framework, including around where you see subscriptions heading?

The Phone-paid Services industry needs to modernise and provide the levels of consumer support and fraud prevention that are expected of modern payment mechanisms. Consumers should be able to report problems with these subscriptions to their networks and have them dealt with in one phone call, not be passed from pillar to post in an effort to get a resolution. The fact that the networks process these, often fraudulent, transactions and then claim to be unable to refund or even stop them does not sit well with consumers.

Consumers should be able to opt out of the 'Payforit' system and not have their numbers passed automatically to third parties. The only way this can be achieved currently is by the consumer using a VPN. They should also be able to opt out of third party charges to their account. Currently this is not offered by all UK networks, but is a legal requirement in many other juristictions such as Germany. I would go a stage further and suggest that consumers should have to opt in to the ability to subscribe to these third party services (in the same way as currently happens for adult services). There would be two major advantages to this:

1. By having to opt in, consumers would be made more aware of the fact that clicking links on websites could result in unwanted subscriptions
2. Children and other vulnerable groups could be protected from harm. Many complaints relate to children becoming subscribed to Phone-paid services. Parents want to be able to give their children a phone without the worry of them running up unexpected bills. Many consumers believe that by blocking premium calls/texts, or by putting a spending limit on an account they can protect themselves, but that is not the case.

In Australia, where there have been ongoing problems with 'charge to bill' or 'cramming' fraud, the networks were eventually forced by public opinion (and potentially expensive law suits) to remove the ability to subscribe to these services.

https://yescrowd.optus.com.au/t5/Blog/Third-Party-content-closure-for-Optus-Postpaid-and-Prepaid/ba-p/447448

https://www.telstra.com.au/mobile-phones/moreonyourmobile/premium-direct-billing-exit

The same could happen here if the industry does not put its house in order! There are many other, more secure, payment methods which could be used to pay for such services. There is no evidence that the benefits of the simplicity of 'Payforit' justify the high levels of consumer harm caused by the exploitation of its vulnerabilities.

If consumers are not to be properly protected, I would prefer to see legitimate services moving to these other payment mechanisms, and Phone-paid subscriptions abandoned as they have been in Australia.

Sent from ProtonMail Mobile