

Response to PSA Consultation on Business Plan 2019/20

Paul Muggleton (payforitsucks.co.uk)

Introduction

I am writing a response again this year because these consultations tend to get many responses from the industry, and few or none from the consumers that PSA are supposed to be protecting.

I began to campaign for reform of direct carrier billing in the UK after a member of my family was the victim of fraud via Payforit. She was signed up, without her consent, to a subscription service costing £4.50 per week. I was able to cap her losses at £4.50 by sending a STOP message within three hours of the initial subscription message.

However, the battle to get the £4.50 returned took eight weeks, twelve telephone calls, 17 emails, two 'signed for' letters and the threat of legal action. When she did, eventually, get a refund she had to queue for 20 minutes in the Post Office for a £4.50 refund. Hardly the "easily accessible" refund referred to in Para 2.6.4 of the current Code of Conduct. My battle to get an explanation of how she came to be subscribed was never resolved. PSA refused to take any action, refusing to enforce Para 2.6.4 of the Code and effectively accusing her of lying when she said she didn't consent to the charges.

I was astonished at the lack of any form of consumer protection against this fraud, and at the lack of cooperation or concern from the network, the level 1 provider and the regulator. I found the acquiescence of the regulator to widespread fraud quite appalling.

I founded the website payforitsucks.co.uk to assist consumers in dealing with these disputes. It is ridiculous that defrauded consumers have to turn to an amateur website, like mine, in order to get justice. The 'industry' and the regulator should be providing this support and putting its house in order. It is incredible that an archaic, vulnerable and insecure system like Payforit is allowed to exist in the 21st century.

A look through the user forums of the major networks will leave nobody in any doubt that there is a serious problem with fraudulent subscription services. Hardly a day goes by without a number of consumers claiming that they have been signed up, without consent, to subscription services costing £4.50 per week (or occasionally less). I refuse to believe that all these people are lying or stupid!

Payforit is a poorly designed and inherently insecure payment mechanism. PSA are well aware that it is vulnerable to exploits embedded in web pages and to android malware. However, it continues to accuse consumers who complain of Payforit fraud of lying, when they say they did not consent to the charges. They accept the "evidence" of consent presented by the rogue companies at face value, while knowing full well that it can be spoofed by malware on the consumer's phone or by exploits embedded in rogue web pages. By the time they get round to 'investigating', the exploits have been removed.

This is a fundamental flaw with Payforit and one solution is to defeat these exploits by using 2 factor authorisation, as has been implemented by EE in February 2018. My own preferred solution would be for the networks just to stop passing consumer phone numbers to third parties. This would force

Payforit to fall back to the WiFi path which appears to be comparatively safe and would be GDPR compliant.

Payforit 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. The networks claim to be unable to stop payments in the way that banks stop direct debit instructions. 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, and have fined companies for using them, but nothing has been done to plug the vulnerabilities. They sit on their hands instead of being proactive in bringing these frauds to a halt.

Consumers are becoming increasingly aware of the fraudulent use of direct carrier billing and are coming to regard the industry as a bit like the 'Wild West' with an ineffective and reluctant sheriff in the form of the PSA. Payforit is danger of becoming synonymous with scam.

Q1 Do our plans for 2019/20 sufficiently deliver our role as a regulator? What else do you think we should be doing or not doing?

I do not believe that PSA has met its role as a regulator in 2018/19, or indeed in years previous to that. I have no confidence that this situation will improve. PSA claims to have a twofold mission:

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

By continuing to support, and failing to reform the iniquitous Payforit system, PSA have failed to protect consumers from harm. Unscrupulous companies have been allowed to continue to shamelessly and deliberately defraud consumers, by utilising the known vulnerabilities of the Payforit system.


The forums of the network operators and other social media are awash with complaints about this system.






Despite a deluge of complaints, these companies have continued to operate with impunity throughout the year, with no apparent enforcement action from PSA.

I am aware that many issues are dealt with through "informal action". Unfortunately consumers who have not made a formal complaint are not then aware of the fact that PSA have ordered refunds.

PSA should publish details of informal action taken against service providers, particularly where this action includes an order to provide refunds to affected consumers.


A look at the Trustpilot reviews of two of the companies operating in this market shows the level of dissatisfaction.







Lasevia
Reviews 73 • Bad

[lasevia.com](#)
Visit this website


Claimed
This company has been claimed.







[Write a review](#)

Reviews 73
Filter by: **Rating** **English**

☐ Excellent 0%
☐ Great 0%
☐ Average 0%
☐ Poor 0%
☒ Bad 100%





Helen Key
3 reviews


2 days ago






Trustpilot Business
Improve SEO, invite customers to write reviews, and reply for free.
[Get Trustpilot Free](#)

Contact
United States

Share the company's rating





TrustScore 0.6 / 10
How we calculate a company's TrustScore.







Sb7mobile
Reviews 51 • Bad

[sb7mobile.com](#)
Visit this website

Claimed
This company has been claimed.


[Write a review](#)










Reviews 51
Filter by: **Rating** **English**

☐ Excellent 2%
☐ Great 0%
☐ Average 0%
☐ Poor 0%
☒ Bad 98%

Trustpilot Business
Improve SEO, invite customers to write reviews, and reply for free.
[Get Trustpilot Free](#)

Contact
United Kingdom

Share the company's rating




Instead of answering the criticisms, SB7 Mobile Ltd has even sought to suppress legitimate criticism of its abuse of Payfort by seeking to have critical Trustpilot reviews removed on spurious grounds. Hardly the action of an innocent party! I have even received the threat of legal action from this company. BBC Watchdog, the Daily Mail and the Independent have all featured the problem of Payfort scams during the year. Yet the Phone-paid Services Authority continues to bury its head in the sand and pretend that nothing is wrong.

An examination of these 'services' is instructive. Take Lasevia's Books4you service. For £4.50 per week (almost £20 per calendar month) you can subscribe to read "over 50 classic books" on your mobile. No indication of what these books are on the signup page, but most classic books are out of copyright anyway! Compare this with Amazon's Kindle Unlimited offering at £7.99 per month. The Books4you service appears to be a blatant attempt to use the vulnerabilities of Payfort to defraud consumers. It certainly isn't value for money! Of course, nobody is suggesting that there is anything wrong with a company offering a service that is of poor value. However, when numerous consumers claim that they have been fraudulently signed up to such a service, alarm bells should sound!

If these companies were genuinely not trying to defraud, and had an ounce of decency, they would refund rapidly and readily, unless there was evidence that the consumer had actually used the service they were charged for. Instead, they do everything possible to retain their ill-gotten gains. The mobile communications industry would be better off without companies like this.

“Services” like this do untold damage to the reputation of Phone-paid Services as a whole. I remain of the view that if payment for goods and services through a phone bill is to become more common, abuses like these need to be stamped out. The industry needs to drive out the “bottom feeders” who seek to profit from abusing the system and who generate a disproportionate number of complaints. Many networks allow consumers to subscribe to services like Spotify and make purchases from reputable App stores using “charge to bill”. These arrangements generate few complaints and offer scope for growth. However, the association of “charge to bill” with scams will destroy consumer trust. I’d rather pay for these services using a credit/debit card or by direct debit where I enjoy proper protection if things go wrong!

In para 4.1.1 of the 2018-19 Business plan, one of the proposed activities was:

“exploring the recruitment of a cost-effective consumer panel to give us further insight into the way that consumers interact with PRS.”

I applauded this idea, as I feel that the PSA is out of touch with consumers and needs to make a much greater effort to listen to their concerns. It comes as no surprise, but a great disappointment, that this idea appears to have been shelved. PSA spends far too much time and money considering the needs of the “industry” and seems completely out of touch with consumers. A cost effective consumer panel with members drawn from relevant consumer organisations, would really help them understand the views of the consumers they are supposed to be protecting.

PSA should reconsider this idea.

In February, EE began requiring two factor authorisation for **all** Payforit subscriptions (and not just those costing more than £4.50). The result was a massive drop in reports of these scams on that network.

If the PSA were to amend its Special Conditions for subscription services to require the other networks to follow the same practice, these scams could be almost eliminated. The fact that this has not yet been done reflects how slowly PSA moves and how unresponsive they are to consumer needs.

Consumers are taking the matter into their own hands with calls for the networks to take unilateral action to protect consumers.

Require 2 factor authentication to sign up for payforit texts



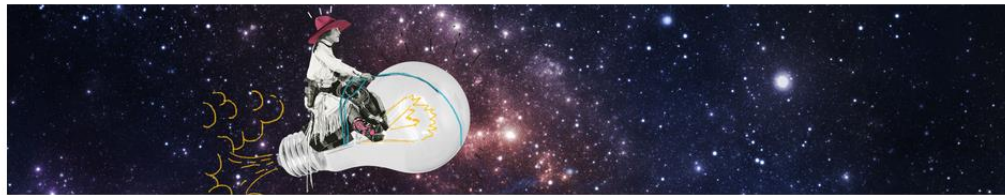
By: andy69 | 12-08-2018 18:00

Marvellous!

Not for me



238



A lot of people are asking about being charged for payforit texts when they didn't subscribe to them in the first place. And how to stop further charges and get your money back. One way would be to require that the initial text is not charged for but is replaced with a text asking you to authorise the subscription. If you want to receive them, then you just follow the instructions in the text to authorise it. It could be follow a link or reply by text. After authorisation, you receive the original text and are charged. If you don't authorise it, you just ignore and no charges are applied.




We're looking into it

GiffGaff Petition

O2 Community > Discussions and Feedback > Premium rate services petition to O2

Reply Topic Options « Message Listing « Previous Topic Next Topic »

« Previous 1 2 3 4 Next »



MIS
Level 94: Supreme
Posts: 82,789
Topics: 508
Registered: 04-04-2012

Premium rate services petition to O2

on 05-01-2019 09:52

EE have introduced a 2!step verification process for premium rate services.
Vodafone allow customers full control within the My Vodafone app.
O2 currently do nothing and many thousands of customers are scammed out of a lot of money every month.
What will you do O2!to keep up with the competition and protect your customers or are you happy to take a cut and leave customers exposed?
if you want to add your voice to this, please comment below.
Over to you, O2 ?

I have no affiliation whatsoever with O2 or any subsidiary companies. Comments posted are entirely of my own opinion. **This is not Customer Service so we are unable to help with account specific issues.**

Currently using:
OnePlus 6 (O2 & 5fr), Z3 Tablet (Three UK), iPhone7 (EE)

O2 Petition

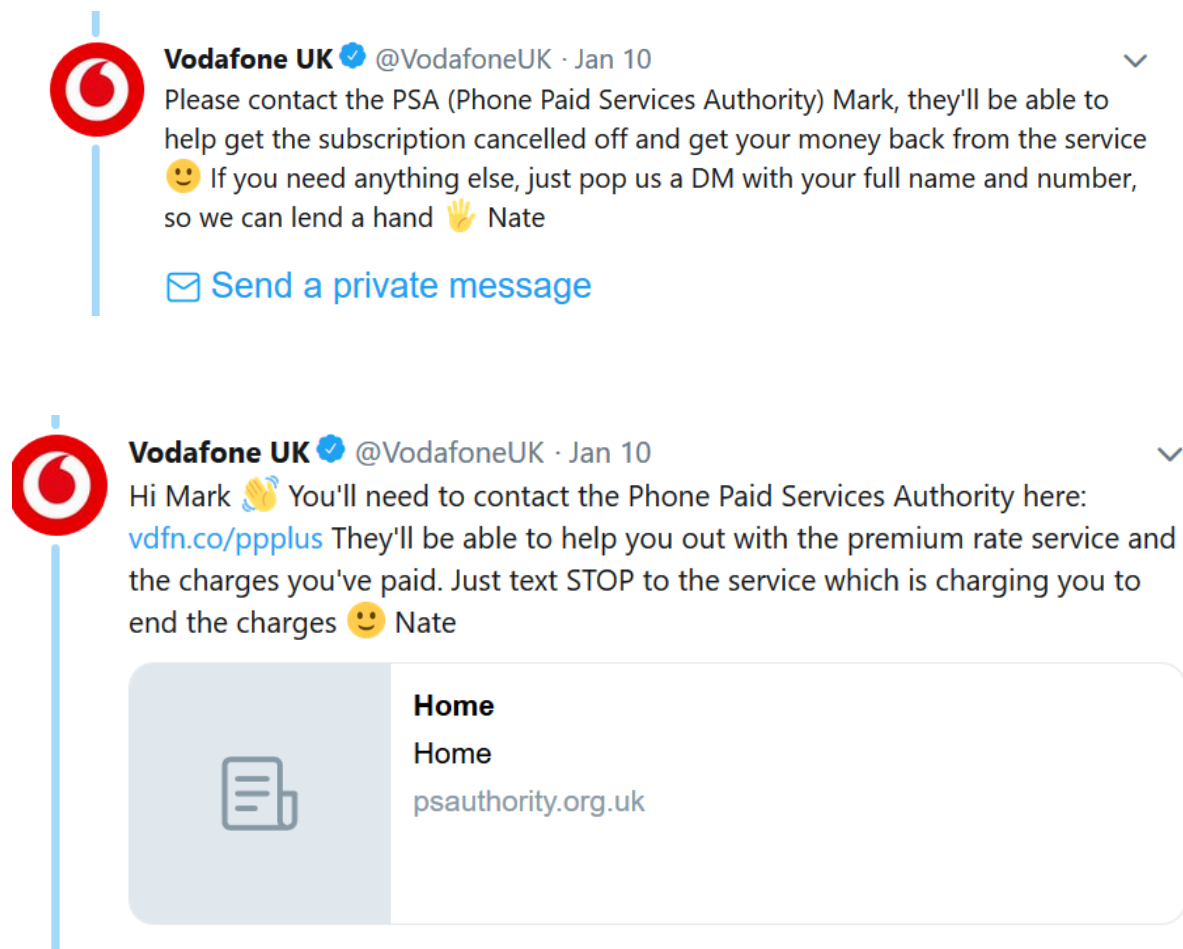
I believe these "Payforit scams" to be massively under-reported. Indeed, PSA are not interested in a case until after the consumer has contacted the third party who has taken their money. Some consumers are unhappy to deal with a company they consider has acted fraudulently, and accept the loss. These consumers are unable to report their case to PSA. Equally, if the third party issues a prompt refund, the consumer is unlikely to pursue the matter further. PSA will not know of the case, even though the original signup may well have been fraudulent.

The payforitsucks.co.uk website has seen an increasing volume of complaints in recent months. Many of these complaints relate to a small group of companies/services. PSA needs to make sure it is aware of these trends. Discouraging consumers from contacting them about their concerns will not help in this respect.

In order to make a proper assessment of the scale of the problem, PSA should encourage consumers to report Payforit fraud, whether or not they have contacted the company and whether or not they have received a refund.

The fact that PSA can't help consumers get redress is a further disincentive to reporting contraventions of the code. Through the payforitsucks.co.uk website I continue to advise consumers to report Payforit scams to PSA, whether or not they have received a refund. However, I know that the majority do not file a complaint. By their policies, PSA are effectively isolating themselves from consumer complaints and artificially reducing the reported level of this fraud.

The role of PSA is often misunderstood by consumers. Part of the reason for this is misleading information provided by the MNOs.



The MNOs need to be told to make it clear to consumers that they are “on their own” in dealing with Payforit scams. I think the customer service representatives of the networks are often embarrassed by this, (and so they should be!) but it is the truth. It wastes everyone's time when networks tell consumers “PSA will sort it out for you”. Nothing could be further from the truth! Consumers sometimes tell us that they are “waiting for PSA to get a refund”.

PSA need to insist that networks are honest with consumers that there is no help available to resolve individual disputes. Consumers should instead be referred to ADR (in the unlikely event it is available) or the Small Claims procedure.

In the absence of any help from PSA, it is left to websites like payforitsucks.co.uk to provide assistance. The lack of a mechanism for resolving Payforit disputes was highlighted in my response last year. Nothing has changed.

PSA has talked about ADR and refund mechanisms, but nothing has happened.

There is talk of an ADR scheme, but unless it is made **compulsory** for the service providers it is likely to prove ineffective as rogue services will refuse to use it. **Consumers currently have to be advised to use the Small Claims procedure to obtain a refund. In the past year I haven't seen a single case in which ADR has been offered.**

Ultimately it is not good enough to say that the MNO's are just providing a payment mechanism. They are responsible for the design and rules of that payment mechanism, agree to provide it to their customers, and profit from it. It is time that the regulator forced them to take their responsibilities seriously and provide support to customers who have been defrauded. Consumers should not need to resort to the Small Claims procedure when these companies refuse a refund.



Chun Wong, a partner at HJA solicitors says that by handing out phone numbers mobile network operators without explicit consent could be in breach of tough new laws introduced in May.

Under the General Data Protection Regulation (GDPR), consent to provide personal data must be explicit and active, says Ms Wong. Opting in cannot be assumed.

The Independent asked all four major networks how they believed the way they operate direct carrier billing complied with GDPR. Only O2 answered the question directly, saying that it was “necessary for the operation of the service”.

The Independent - 23rd December 2018

I am of the view that Payforit is legally, as well as ethically, flawed. GDPR requires that consumers give explicit permission for their personal information to be divulged to third parties. This is still not requested, even for new contracts. The presumed consent remains hidden in the “small print”. The networks defend their position by saying that divulging numbers in this way is essential to the function of their business, and so they are therefore exempt from the GDPR requirements. This is the so-called “Legitimate Interests basis”.

The ICO lays down a number of criteria for this basis, amongst them

- The processing must be necessary. **If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.**
- **You must balance your interests against the individual's.** If they would not reasonably expect the processing, or **if it would cause unjustified harm**, their interests are likely to override your legitimate interests.

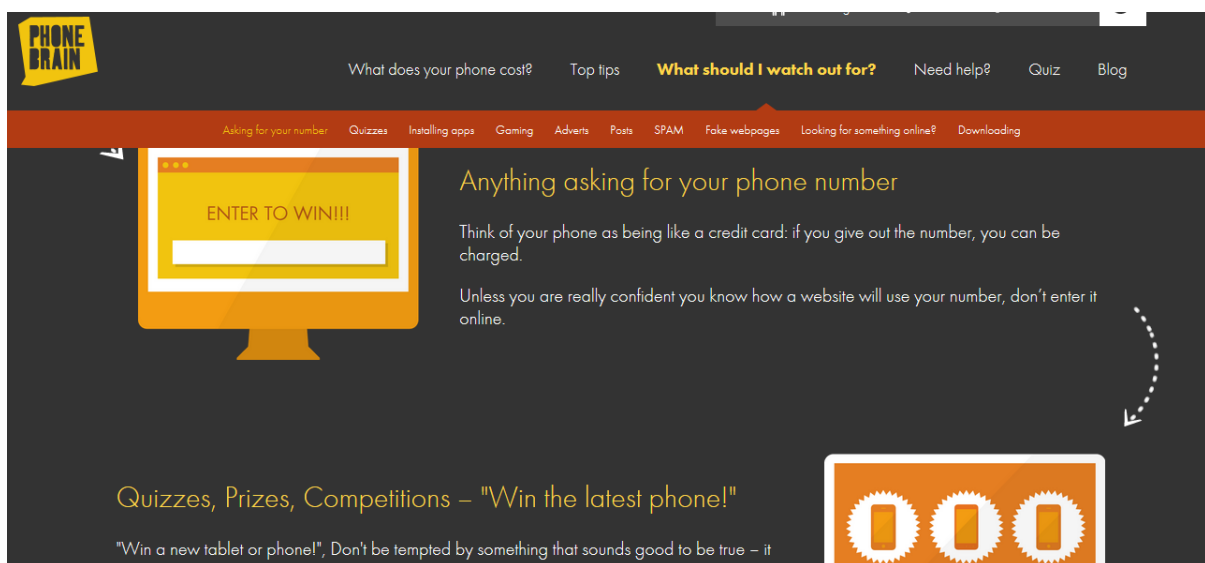
The processing is not necessary. This may be the case for some PRS, such as directory enquiries, but not for Payforit. It is quite possible for consumers to sign up to Payforit services using a WiFi connection where Payforit is unable to obtain the consumer's number from the network.

There is also ample evidence of unjustified consumer harm, with daily reports of consumers being defrauded. Consumers are often not aware that their numbers are passed to third parties when accessing the internet via mobile data. They expect identical protection to that available when they use WiFi and don't understand the need for this difference. There is no business necessity for the networks to be compromising their customers' phone numbers in this way.

Regulators seem unwilling to address this issue. PSA will not say whether the process is GDPR compliant, stating it is a matter for the Information Commissioner. The ICO won't give an opinion either, saying it is a matter for the PSA! Why do we bother to have regulators at all when they won't rule on issues like this?

PSA should liaise with the Information Commissioners Office to decide who is responsible for monitoring compliance of Payforit with GDPR. A ruling should then be made regarding the legitimacy of Payforit passing consumers numbers to third parties without their explicit permission.

In December PSA launched an advertisement advising parents to make sure that their children knew never to give their phone number to a 'third party'. It included the advice "Think of your phone like a credit card. If you give out the number you can be charged".



Great advice, which completely ignores the fact that Payforit does exactly that! It exposes the consumer's number, and allows all manner of shady companies to make charges against the consumer's account. PSA needs to look more carefully at this advice. **PSA need to educate consumers to make them much more aware that their network will leak their phone number to third parties when they access the internet via mobile data.**

PSA also advise consumers concerned about their vulnerability to Payforit fraud to ask their network to put a 'charge to bill' bar on their account. The Three network and MVNO GiffGaff both refuse to implement such a bar.

Consumers should not be forced to expose themselves to the risk of Payforit fraud, and the PSA should be encouraging these networks to provide their customers the protection which they recommend.

Another issue is that, even if the service provider accepts that a refund should be made, there is no proper mechanism for that to happen. There is a general principle in commerce (embodied in the Consumer Rights Act 2015) that refunds should go to the account from which the original payment was made. The law makes it clear that this should be the refund mechanism, unless the consumer agrees to another mechanism. Third party suppliers are being allowed to flout this legislation, safe in the knowledge that the regulator will not act and that the cost of a legal challenge is prohibitive.

Refunds for transactions made on a credit or debit card are made back to the same card. If a fraudulent payment occurs on my bank account, the refund is made to my bank account. When a PayPal payment is reversed, the refund will go back to the PayPal account from which it was taken.

Why can't refunded Payforit charges be returned to the account from which they were taken? Why can the refund not be made by the same method and with the same speed and ease as the transaction which is being reversed?

PSA are allowing widespread breaches of para 2.6.4 of the Code of Practice and taking no enforcement action. Given the speed and ease with which these payments are taken, I think it reasonable that when they are taken without consent the funds should be returned with equal speed and ease.

I would like to see the PSA actively enforcing para 2.6.4 of the Code, and demanding that the Payforit mechanism be modified to allow for simple and speedy refunds directly to consumers' phone accounts.

I recognise that PSA are not an enforcement agency for the purposes of the Consumer Rights Act 2015 and the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013.

However they are in a position to refer such concerns to Ofcom, and should also be mindful of Para 2.1 of the Code of Conduct which states:

Outcome

"That PRS comply with the law."

Rules

2.1.1

PRS must comply with the law.

2.1.2

PRS must not contain anything which is in breach of the law, nor omit anything which the law requires.

2.1.3

PRS must not facilitate or encourage anything which is in any way unlawful.

2.1.4

PRS providers and relevant individuals engaged in the provision of a service must hold all licences, permissions and qualifications required by law.

Thus I believe that the question of whether these PRS services are complying with relevant legislation (whether consumer rights law or GDPR) is an issue which should be of concern to PSA.

PSA claim that compliance with these laws is not a matter for them, so the service providers continue to flout the law in the knowledge that PSA will not act, and that a judicial review would be prohibitively expensive.

Once again, regardless of the legal arguments, I believe that PSA should be properly enforcing these aspects of the code. Such enforcement could help drive the scam operators out of business and dramatically improve the prospects for growth for genuine services.

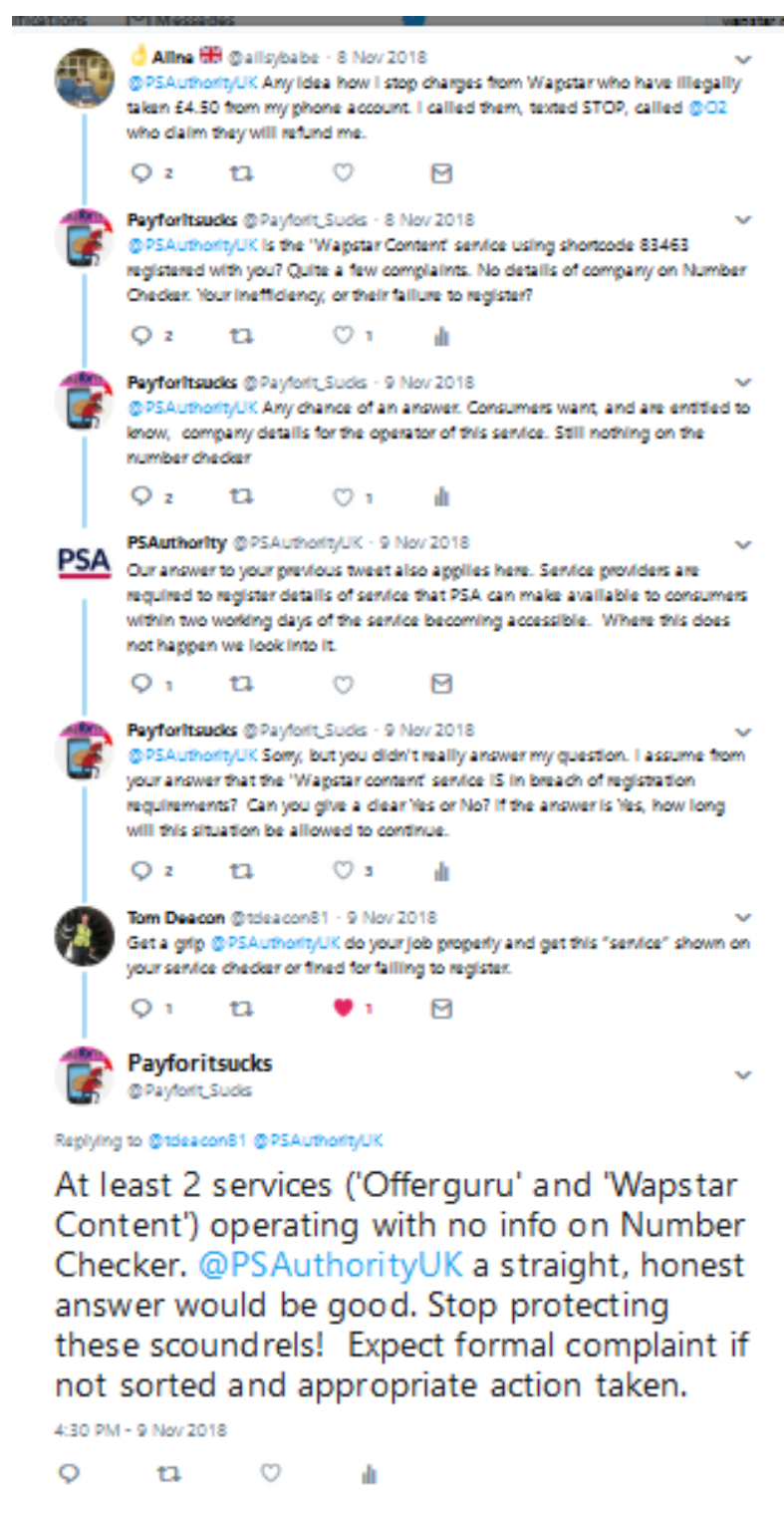
PSA have made much of their wish to minimise “friction” in consumer purchases of Premium Rate Services. It is this very lack of friction which results in thousands of consumers each year complaining that they have received charges, to which they have not consented. There are simply too many ways, many of them almost impossible to detect, that the intended safeguards are being circumvented.

It is now time to consider reducing the “friction” encountered in obtaining refunds for these fraudulent transactions.

During the year, PSA rolled out a new version of their number checker. Unfortunately this seems to have coincided with widespread non-compliance with registration requirements and/or problems with populating the number checker in a timely manner.

These problems have resulted in confusing and sometimes contradictory information being given to consumers. This has been a particular problem with shortcodes 83463 and 64055 where details of new services have failed to appear weeks after the services have started. PSA’s usual response is “we’re looking into it”.

Registration details are required to be supplied within 2 working days of a service starting. MNO’s are often unable to supply company details for companies involved in these services. I believe it to be negligent to allow a company to take money from consumers for an undefined service, when you hold no details of the company making the charge.



As an example, a service called “Offerguru” has been operating using shortcode 64055 since October 2018. I raised this as an issue on 9th November 2018, but it was never resolved. As of 14th January 2019 details of this service are still not shown on number checker. To add to the confusion, there are two separate listings for the “Fitguru” service with different contact details, and nothing to even indicate that this is a shared shortcode and the responsibility of mGage Ltd. It really is unacceptable for companies to be taking subscriptions from consumers for weeks with no information available about the service. These are shared shortcodes, but consumers don’t know or understand that. They

expect to see the service details for the service which is charging them and are confused when they see a number of other services, but not the one they are looking for.

Consumers already experience considerable difficulty making **meaningful** contact with service providers. This is made even more difficult when details of the service and its customer service arrangements are not available on Number Checker. It should not be necessary for consumers to contact the Level 1 provider in order to obtain a customer service number for the Level 2 supplier.

If the number checker is not to contain details of ALL services using a particular shared shortcode, then the number checker should ONLY show contact details for the level 1 provider. It should then be made clear to consumers that the level 1 provider should be contacted in respect of any service using that shortcode. In such cases the Level 1 supplier should be made to assume direct responsibility for handling the consumer's issues and not redirect the consumer. The consumer should not have to call multiple parties to resolve these issues.

It would be useful if a reverse lookup was available, where inputting the name of a service would reveal the shortcode being used and the contact details for the company operating the service. Failing this, maybe an alphabetical list of services and corresponding shortcodes could be automatically generated from the data held on Number Checker and published on a regular basis.

In 2017, PSA commissioned Futuresight to produce a report on Customer Care and Complaint Handling to help them and the industry improve the effectiveness of these aspects of PRS. Nothing seems to have been learnt. The practices identified in that report are still being used to defraud consumers and destroy consumer confidence in Phone-paid Services

These behavioural factors could be seen to be exploited by some Merchants, in at least three main ways: (i) using subscription models to debit relatively small amounts of money on a regular basis, (ii) lack of prominence and clarity in how to exit a service without being charged, and (iii) relying on the fact that many people delete subscription service spend reminders thinking them to be spam texts, rather than using them as a trigger to stop a recurring charge.

This could be seen to lead to a serious erosion of confidence and trust, not just in the service itself, but in the phone-paid services market as a whole. Claims of loss of trust were very evident in this study.

By the same token, it was clearly evident that confidence and trust was either maintained or increased by Merchants who operated in a way that is entirely fair to consumers.

These observations remain valid in 2019.

PSA have sought to lower the entry level for these services, despite this observation in the 2017 report:

⁸ In our in-depth interviews, a clear pattern was evident in Complainant responses between 'well-known' and 'unknown' Merchants. Typically, complaint resolution for well-known merchants tended to be more straightforward and easier to resolve. Very typically, well-known Merchants tended to be more responsive, were felt to have 'a reputation to protect' and had a formal complaints process in place. Compared to unknown or 'no-name' Merchants, this led in more cases to better outcomes and higher levels of satisfaction.

Lowering the bar to entry clearly has its risks and PSA seems to have ignored these.

In the past year, it has become increasingly obvious that iFraming and similar exploits continue to be used to fraudulently sign up consumers to some Phone-paid subscription services. PSA has failed to address this issue. These exploits are not necessarily the work of the service providers. They are often used by over-zealous affiliate marketers in order to boost results. Regardless of the perpetrator, PSA are largely unable to detect these exploits. A rogue web page can be replaced with a legitimate one in seconds and it takes the PSA weeks if not months to start an investigation.

The "evidence" which PSA currently requires to confirm a legitimate signup is easily spoofed, but PSA continues to accept it. These services take no heed of PSA's advice that subscription services should use two factor authorisation. **If consumers are insistent that they did not consent to a subscription, PSA should accept this and believe the consumer unless 2 factor authorisation has been used or there is evidence that the service has actually been used.**

Q2. Do you have any comments on the proposed budget for 2019/20? If you recommend any changes, please clearly identify which areas of activity you expect this to impact upon.

No Comment

Q3. Do you have any comments on the proposed levy for 2019/20?

I remain of the view that the levy should be apportioned depending upon the amount of work created by each type of service. Thus compliant services would pay less and those that result in high complaint volumes would pay a higher levy. If this resulted in some of the less reputable services becoming uneconomic that would be an added bonus.

Q4. What is your view on the estimated size of the market for 2019/20?

Undoubtedly there is scope for market growth, but this is likely to be severely hampered by consumer distrust and the lack of effective security, consumer protection and refund mechanisms. Any growth seems likely to come from reputable companies, which consumers already trust, offering payment through direct carrier billing. This is likely to be held back by the continuing association of this payment method with scams.

I can see no current benefits to paying through 'direct carrier billing' and many disadvantages, especially if I have a problem with my purchase. Given the choice between 'charge to bill' and credit/debit card or direct debit, I can think of no reason to choose direct carrier billing and many reasons why I shouldn't. It is ridiculous that there is no way a consumer can stop a Payforit subscription in the same way as they can stop payments made by other methods.

The many consumers who have been the victim of one of this year's Payforit scams, and have found out how difficult it is to obtain a resolution, will take a lot of convincing to use this flawed method of payment in the future. The industry badly needs to 'clean up its act'!

Q5. Do you have any other comments on the Business Plan and Budget 2019/20?

No Comment

Paul Muggleton

payforitsucks.co.uk