PSR's Consultation on

Authorised Push Payment (APP) Scams (CP21/10)

https://www.psr.org.uk/media/kg0bx5v3/psr-cp21-10-app-scams-consultation-paper-nov-2021.pdf

Submission by the Transparency Task Force, January 13th 2022

About the Transparency Task Force

The Transparency Task Force is a Certified Social Enterprise, meaning that we exist to make an impact, not profit.

The mission of the Transparency Task Force is to promote ongoing reform of the financial sector, so that it serves society better. Our vision is to build a large, influential and highly respected international institution that helps to ensure consumers are treated fairly by the financial sector. The primary beneficiaries of our work will be consumers; but the sector itself will also benefit through improved market conduct and increased trust in the services it provides.

Our objective is to carry out a broad range of activities that help to drive positive, progressive and purposeful finance reform, such as:

- Building a collaborative, campaigning community; the larger it is the more influence it can have in driving the change that is needed
- Raising awareness of issues; so that society better understands the problems that exist in the financial sector and how they can be dealt with
- Engaging with people who can make change happen; because through such dialogue we can influence thinking, policy making and market conduct

Our response to you has been produced by a highly collaborative group of TTF volunteers, our "Response Squad," working together to build consensus, whilst always remaining true to our "North Star" question: "What is best for the consumer?" For further information about the Transparency Task Force see: http://www.transparencytaskforce.org

Our Response

This response is all non-confidential.

Please note that all comments in this response are part of the response, and should be considered.

Some of this response is contained in answers to the PSR's specific questions below, but parts of the response not shown as direct answers to questions are equally part of this response, and for consideration by the PSR.

Terminology

Please note that in this response, the term bank is often used. This is because the vast majority of payments today are made through banks, and so in the majority of cases a consumer's PSP will be their bank.

For ease of reading therefore the term bank has been used widely.

However, the correct term in each case is actually PSP and not bank, and this response applies to all PSPs, whether banks or non-banks.

Introduction:

APP scams are a growing menace to our society, with hundreds of thousands of UK consumers and businesses suffering life changing (and sometimes life ending) loss each year.

The UK's Police and criminal-facing organisations do not have funding to investigate, and certainly not prosecute, the vast majority of cases that occur.

So APP Fraud cases keep increasing.

The PSR's consultation CP21/10 on APP Fraud is significantly misleading, and requires correction

Paragraphs 2.4 and 2.5 of the PSR's consultation state:

> 2.4 Before the CRM Code came into force in May 2019, there was no systematic protection for victims, with weak incentives for PSPs to work to prevent APP scams.

> Outcomes were uncertain and reimbursement levels were significantly lower. In its recent review of the Code, the Lending Standards Board (LSB)6 reported that the pre-Code industry average was 19% by value in the first half of 2019. This increased to 47% during 2020, for signatory banks, following the introduction of the CRM Code.
>
> 2.5 In light of this, the voluntary agreement by the signatories to the CRM Code was a major step forward, setting out standards for PSPs to improve fraud prevention and victim care.

These two paragraphs are significantly misleading, and need urgent amendment.

The Contingent Reimbursement Model Code (CRM) duplicates the pre-existing protection provided by the recent FCA Handbook change introduction (see https://www.fca.org.uk/publication/policy/ps18-22.pdf where the Handbook changes are detailed).

The protection offered to consumers by the FCA Handbook changes (hereafter referred to as the **FHC**) is in almost all cases superior to the protection provided by the CRM, so that the CRM was mostly superfluous.

Except in very rare instances, the CRM provided no extra protection (see below for a full explanation).

Consumers and businesses in the UK are generally unaware of the FHC protection, and the lack of any mention of the FHC in the CP21/10 consultation invalidates the consultation – as it ignores the most important statutory redress available to both consumers and small businesses.

The day after the PSR's consultation was released, this need for remedy of the Consultation was communicated to the PSR.

The PSR wrote back a week later stating:

> Both the extension of the complaints handling rules in the DISP section of the Handbook , and the extending of the jurisdiction of the Financial Ombudsman Service to include appeals regarding decisions under these (both under PS18/22) [together, the **FHC**] do indeed provide some coverage for APP scam victims. However, these provisions only concern cases where the banks have been at fault for not communicating in a timely way (where this was possible) to stop scammed money from being taken out of the system.

So the PSR acknowledged that their consultation ignores the strong FCH protection available (unbeknown) to consumers and small businesses.

But the PSR refused to correct the error in the consultation.

The PSR's response is more alarming however.

Firstly, the PSR's response is incorrect, as reading the FHC makes clear that the FHC applies in any situation where a bank did not do all it could to prevent an APP fraud.

This goes far, far beyond the PSR's claim of 'banks have been at fault for not communicating in a timely way (where this was possible)'. There are many, many more ways that a bank can prevent fraud than communication, and the banks are liable to the consumer under the FHC in any case where the bank has not done all it could to prevent the fraud.

Secondly, the FHC provides protection in vastly more situations than the CRM.

Compare in the following table:

	CRM Offers Protection	**FHC Offers Protection**
Consumer was partly at fault and paying bank was partly at fault	No	Yes
Consumer was partly at fault and receiving bank was partly at fault	No	Yes
Protection available to small businesses	No	Yes
Consumer can freely claim against payee bank as well as payer bank	Indirectly	Yes
Neither consumer nor any bank was at fault in any way	Yes	No

Thirdly, and most importantly, there are hardly any cases where the receiving bank was not at fault (see full explanation below).

So the number of APP fraud cases where the CRM is superior to the FHC is vanishingly small.

Whilst the number of APP fraud cases where the FHC is superior to the CRM is very large, and probably the majority.

The Consultation had every reason to include mention of the CRM. But omission of the FHC is unconscionable, and actually perpetuates the lack of knowledge of the important FHC protection available to consumers and small businesses.

The PSR needs to remedy this omission urgently, and issue an amended version of CP21/10 which takes account of the FHC in addition to the CRM.

Why are payment-receiving banks at fault in APP Fraud cases in nearly every case of APP Fraud recorded ?

[Taken from a submission to the PSR's Call for Views CP21/3, which was the predecessor to CP21/10, and from which CP21/10 resulted]

At this time, in virtually all APP fraud cases occurring today, the payee's bank is at least partly at fault for the APP fraud.

This is because the payee has either opened an account at the payee's bank with false ID, or the payee is operating as a mule account.

In the first case, the payee's bank accepted false ID, and is therefore partly at fault in the loss.

Now that machine readable passports are commonplace, which allow verified identity information and a photograph to be read off the passport with high certainty and confidence (as they are digitally and cryptographically signed), there is no reason why any bank should today open an account with false ID. It should be extremely difficult for a criminal or fraudster to do so – way beyond the capabilities of the ordinary crook.

We would ask the PSR to lobby the Government so that driving licences also become machine readable and crypto-signed, as at present driving licences are easily faked. This is a Government weakness, and the PSR should be pressing the Government to immediately address this issue, so that accounts can be opened for customers who have a driving licence but no passport).

In the second case, the payee is acting as an account mule.

Account mules are always caught by the Police, as they are committing crime in the open and do not hide their crime – that is the nature of an account mule.

The defence of account mules – which is effective at present – is they did not know they were doing wrong.

As a result, the Courts will not prosecute, and as a result the Police will not act (it is not worth their while, with no expected penalty resulting).

And as a result, account mules are free to continue unabated in a tsunami of fraud.

This is all the result of banks' failure to alert their clients to the illegality of account muling.

One of the contributors to this TTF consultation response has commented:

> "I have never received any communication from any of the various banks I personally bank with (and I personally bank with a few, to help me understand consumer experience with their banks) instructing me that I cannot receive a payment into my bank account for another party.
>
> If I was instructed by my bank that I can only receive payment into my bank account on my own behalf, and never for another person or another party, and that such receipt was actually potentially illegal and money laundering, then I would be aware that account muling was illegal. If I was told at the same time by my bank that such receipt can well lead to a fine or prison sentence, then I would take note.
>
> But I have never received such a message from any of the many banks I bank with."

As soon as banks take action to directly inform all their clients that the client is not allowed to receive payment into their bank account for another party, and that such receipt may be money laundering and subject to fine or prison sentence, then Courts will immediately on the basis of these warnings start prosecuting account mules.

And Police will immediately start arresting and taking to Court account mules, as the Police know they will have an easy conviction (and this will make them look very effective).

And account muling will stop, because no account mule will continue knowing they are committing crime in the open, and will be caught and prosecuted.

As payee banks have not made clear to their clients that account muling is not allowed and potentially illegal, the payee banks are all at fault if their accounts are used for account muling (the bank is also in breach of the Money Laundering Regulations 2017 – but that is a different matter).

So if an APP fraud takes places, and the payee turns out to be an account mule, then it is correct that the payee's bank should be liable, as the payee's bank did not warn and make crystal clear to the payee that acting as an account mule was not allowed and possibly could cause fine or imprisonment (which in turn allowed the account to be used to defraud the original payer).

The upshot is that a payee's Bank is currently almost always at fault (at least partially) in an APP fraud (whether due to false ID or account muling), and liability should always reside with a payee's bank unless i) they did not allow their account to be opened with false ID, and ii) they made clear to their customer that they could not receive payment for any other party at risk of a prison sentence.

And as made clear above, these two criteria are hardly ever currently both met by payees' banks.

It is our belief that when banks do finally start educating their clientele that accounts cannot be used to receive third-party payments, APP fraud will shrink in the UK by several levels of magnitude..

Paragraph 1.8

Paragraph 1.8 ascribes success to the CRM in preventing APP fraud, whereas evidence for such a claim is absent and lacking – indeed, rates of APP fraud are rising, so the claim seems unsubstantiated and quite possibly wrong.

As already noted, the FHC pre-dated the CRM by five months, and provides much superior protection in most cases. However, the protection provided by the FHC is generally unknown by those it protects, and so is not fully or even substantially utilised.

The TTF strongly endorses the creation and use of Confirmation of Payee (CoP), and believes that this is a critical tool in the fight against APP fraud.

Criminals will try to create novel payment situations where CoP will not apply, such as payments through electronic money rather than the Faster Payment Service, and the PSR must ensure that CoP is expanded and kept updated to prevent criminals utilising payment areas where CoP is not yet functioning.

Moreover, CoP has its shortcomings - specifically the reliance on name-checking rather than a precise digital identifier. Although all three measures suggested in the Consultation Paper are significant to bring transparency to the PSP market, still the foundational question - how to prevent fraudsters and APP scams from the very beginning - is yet to be addressed.

Particularly for Consumer-to-Business (C2B), Business-to-Business (B2B), Consumer-to-Government (C2G), or Government-to-Business (G2B) transactions, the Legal Entity Identifier (LEI) can be leveraged to set the first foundational step for a transparent payment chain. If all parties in the payment chain verify the LEI of the recipient business/government entity, the receiving PSP would have complete transparency before allocating funds. A recent Payment Market Practice Group (PMPG) report explains how the LEI can help enable more transparent, efficient and secure payments. Therefore, we suggest the addition of the LEI in the CoP as an extension of the service, together with the PSR encouraging Companies House in the UK to automatically issue LEIs to all registered UK companies, linked to their Companies House registered number.

Paragraph 1.14

We thank the PSR for raising the need to include telecoms companies and internet related services – such as social media companies – within the UK Government's response to APP fraud.

We recognise that these areas are outside the PSR's remit, but it is important that the PSR is bringing them to the Government's attention.

The UK Government's response in refusing to prevent APP fraud by including social media advertisement legislation in the forthcoming Online Harm Bill is far from reassuring though. This is of course outside the PSR's control.

Paragraph 1.15

This paragraph asks what else the PSR could be doing at this time to prevent or ameliorate APP fraud.

The answer is clearly i) force banks to educate their customers not to allow third-party payments through their accounts – at risk of prison - as this will stop most APP fraud in the UK as account-muling disappears, and ii) publicise the FHC so defrauded consumers and small businesses can understand the true statutory protection available to them.

Paragraph 1.16

The CRM code was drafted, negotiated and agreed on the one hand by consumer organisations, and on the other by the UK's 7 largest banks.

The UK's 7 largest banks managed to include several loopholes in the CRM which weaken its protection – for example, wording at R2(1) of the CRM states that if any of R2(1) (a) to (e) apply, then no reimbursement may be made if any of (a) to (e) would have had a 'material effect' on preventing the APP fraud. A 'material effect' could mean that it would, say, make the APP fraud 20% less likely.

So under the current wording, even if a bank did not meet the code and would otherwise be liable, under R2(1) if it can show that any of (a) to (e) is present and would have lessened the chance of fraud even to a small degree, then under the CRM strictly no liability will remain with the bank, and all the good of the CRM becomes worthless.

Looking back, it can be claimed that the consumer organisations that negotiated the CRM were naive in their acceptance of the code, and the code in reality falls far short of what they expected.

In addition, only the largest banks formulated and negotiated the CRM. The CRM takes their interests into account, but does not take the interests of smaller PSPs and banks into account.

The CRM is therefore anti-competitive, as it is written to best serve only the largest banks.

Whilst the CRM is a voluntary agreement, this presents no issue.

But in this paragraph the PSR are talking about the CRM being made mandatory for all banks and all PSPs. This is seriously anti-competitive and against the PSR's founding principles, as smaller PSPs and banks have had no opportunity to offer input to what until now has been a code drafted and formulated by the largest UK banks.

Paragraphs 2.4 & 2.5

As noted above, these two paragraphs are factually incorrect, and highly misleading, and require urgent correction.

The CRM was not a major step forward – some regard it as a diversionary tactic by banks, to try (successfully) prevent consumers and small businesses becoming aware of the much stronger FHC protection then newly available to them.

Paragraph 2.7

The third bullet point states: '*The overall level of reimbursement under the CRM Code has been less than 50%. It is unlikely that victims have not acted appropriately in 50% of cases.*'

The consultation is misleading as the test under the CRM is not whether a victim has acted appropriately or not ('appropriately' not being defined). The CRM lists a list of exclusions whereby banks can legitimately refuse any reimbursement under the CRM.

The FHC provides none of these exclusions, and the FHC is operative and provides protection in any case where any bank could have done more to prevent the APP fraud, regardless of the consumer's acts – a completely different scale of consumer protection.

Paragraph 2.8

This paragraph is at the core of the APP fraud problem, and is grossly understated.

Receiving banks should always be held liable for APP fraud if payment cannot be retrieved, except in currently rare cases where the receiving-bank can show that they neither allowed a false-id account to be opened, nor did they allow an account-mule to use their account without knowing they would face a prison sentence if they did so.

Paragraph 2.9

Once again, this paragraph is factually wrong. The discussion over the CRM that took place was only between the consumer groups and the largest 5 or so banks, as only the largest banks were signing up to the CRM code.

The vast majority of other banks and PSPs had no opportunity to shape or comment upon the CRM when it was drawn up.

Paragraph 3.44 – And why no fault reimbursement by PSPs can never be mandated

The FHC already quite correctly imposes mandatory reimbursement to consumers and small businesses where a bank (sending or receiving) was at fault.

But the CRM takes this a huge step further.

The CRM makes a bank or PSP liable for the customer's loss in cases where the bank or PSP did absolutely nothing wrong, and where the bank or PSP could not have avoided the customer instructing the bank to make a payment to the fraudster.

With the CRM on a voluntary basis this is fine.

But if the CRM is made mandatory, then it will destroy nearly all PSPs in the UK, and leave a monopoly of only the very largest banks to sweep up the payment space and make it a truly anti-competitive, dysfunctional, very expensive and ill-functioning environment for consumers.

Why ?

Payment firms earn pennies for handling each payment.

Those payments may be small, large or very large.

If a payment firm becomes liable for reimbursing a customer when the payment firm has done nothing wrong, and could not have avoided the customer's actions in sending money to a fraudster, then payment firms will face losses due to no-fault reimbursement higher than their revenue, and be forced to close down.

This will cause all but the largest payment firms to cease operation, as no payment firm can operate at a loss.

Only the largest banks temporarily cross-subsidising their losses from their other revenue will be able to continue for any length of time.

And once a monopoly of only the largest banks exists, payment charges will rise dramatically not only to charge for the loss to no-fault reimbursement, but also to take advantage of monopolistic profit power.

The PSR's own core principals forbid the PSR from precipitating such an anti-competitive situation.

So the PSR does not have the legal power to mandate no-fault reimbursement.

And the overturning of the legal principle that firms can be liable to their clients for enormous sums when the firm has done everything correctly with no fault is also a matter that may well be outside the PSR's legal ability to mandate, and will certainly be subject to legal challenge.

Please remember we are talking about cases where banks and PSPs may be liable for tens or hundreds of thousands of pounds or more, where the bank was not involved in the loss in any way.

Say, for example, a customer (and especially a vulnerable customer) is approached by a conman pretending to be from the bank, who tricks the consumer to make a life-changing payment to the fraudster.

In such a case, it is entirely possible that the bank may only learn of the fraud long after it has occurred, and it is entirely possible that the bank had done everything reasonable and proper to avoid such situations from occurring.

But fraudsters are excellent psychological manipulators, who can manipulate their victims into a state of panic and reasonably get them to take unreasonable actions.

At the moment, the voluntary CRM makes banks pay full reimbursement in these 'no-fault' situations – the consumer is regarded as not at fault, as they were reasonably panicked into performing an unreasonable act, and are regarded as not at fault.

And the bank took no part in the fraud whatsoever, and only learnt of it after the event had occurred, so of course was not at fault (if the bank takes deficient action, and allows itself to be impersonated, then the bank would be at fault, but in many situations the bank would not reasonably allow impersonation).

The PSR needs to ditch the fallacy that it can force banks to be responsible for consumers' loss where the bank was not at fault in any way.

Such a pipe-dream will lead to the UK payment industry shutting down, and a monopoly of only the largest banks increasing payment prices to monopolistic levels.

Remember, the FHC already correctly and properly imposes reimbursement liability on any and all banks where the bank is at fault in any way. This must be publicised, and consumers and small businesses need to know they already have this protection.

But where banks are not at fault in any way, no-fault reimbursement through a mandatory CRM would be catastrophic to the UK.

Paragraph 3.45

The PSR has presented no evidence that mandatory reimbursement will in time not lead to fraudsters creating mandatory reimbursement claims using compliant 'defrauded' consumer associates, to a staggering level.

If mandatory reimbursement becomes ingrained, it is obvious that very soon criminal gangs will target banks with customers who have genuinely lost money to APP fraud through no fault, but where the customer is really an associate of the fraudster. This would be untraceable.

It is inevitable that this will occur, and just because it has not yet begun to occur on a large scale does not mean that it will not soon commence. It is folly to believe otherwise.

Paragraph 3.46

The last sentence of this paragraph shows the contradiction in the PSR's position.

Banks cannot prevent no-fault APP frauds – as the bank by definition and by fact was not at fault in any way.

Yet the PSR states that bearing the cost of such reimbursements will ensure that these APP scams will be prevented.

This is a clear logical fallacy, and blows an unfixable hole in the PSR's rationale for no-fault reimbursements.

Paragraph 4.13

Despite what is written in this paragraph, organised criminal groups will peruse the data produced and try and leverage the information.

However, we strongly believe the benefit from the information to the public will far outweigh this detriment.

Question 1. Do you have comments on our proposed data metrics?

We welcome the proposed collection and publication of APP fraud statistics.

We believe there is a strong case for publishing the data on APP reimbursement in full, including the names of the banks and the reimbursement rates of each. There's an obvious competition angle here: consumers will shun the worst performers and flock to the best, so the market is not working until that data is published. There's also a regulatory argument: criminals will flock to the worst banks. Publishing their names will therefore provide a powerful incentive for them to raise their game on KYC/AML.

a) We do believe the focus of the figures is incorrect however.

At this time, almost every case of APP fraud will include fault to some degree by the receiving bank. Many APP fraud payments will not include any fault by the sending bank (although a significant number will).

So the statistics ought to be as or more detailed for receiving-banks than for sending-banks.

So it is important to amend the statistics so that receiving-bank APP fraud figures record i) numbers of cases of APP scam payments made to that receiving-bank, as well as total APP payments amounts made to that receiving-bank, and ii) the number of APP fraud cases where the receiving bank makes full reimbursement, and iii) the number of APP fraud cases where the receiving-bank makes partial reimbursement, as well as the proportion of APP fraud funds repaid in each case.

b) Banks and PSPs already supply twice-annual fraud data to the FCA.

It is a burden to impose two separate sets of fraud collection on banks and PSPs.

Instead of the PSR separately requiring banks and PSPs to supply data to the PSR, why does the PSR not work with the FCA to ensure that data collection is managed under the existing but amended FCA data collection requirement, and data relevant to the PSR can be passed to the PSR by the FCA ?

This will place a much lower burden on banks and PSPs (one set of data submission rather than two separate sets of forms and data submission).

Question 4. Do you have any comments on the draft direction at Annex 3?

a) Recital 1.1) is ambiguous and/or incorrect, as it seemingly only includes half of the definition of APP scams defined in later Recital 4.1.

The recital 1.1) should be clarified to match the two types of APP scam payment defined and enumerated in Recital 4.1 (b).

b) Why does Recital 6 only include consumer APP scam cases, and not include all APP scam cases (including small business and large business) ?

If a bank is suffering high rates of business APP fraud, it is only a matter of time before that bank also suffers consumer APP fraud, if it is not already.

Receiving banks may hold a personal account or a business account which receives APP fraud payment, but both may be the target of consumer APP fraud.

It is artificial to differentiate between consumer APP fraud and business APP fraud, and would be difficult to achieve. All cases of APP fraud should be included.

c) Recital 15.5 in the definition of ‘consumer’ states that micro-enterprises are to be included, but not small businesses.

Protection under the FHC extends to small businesses as well as micro-enterprises, and there seems no reason that small businesses should not also be included in the PSR’s statistics collection.

Question 5. Do you have comments on our proposal for which PSPs should initially be required to report and publish Measure 1 data?

The FHC apply to all PSPs and banks, and not just those using the Faster Payment Service.

Where large payment transaction flows are taking place in the UK, these should be captured by the PSR's data gathering order.

Large PSPs such as PayPal, that utilise non-Faster Payment payment flows, must also be included in the PSR's orders.

Otherwise, APP fraud through these large scale payment alternatives, which are also covered by the same payment protection regulation and legislation, will be missed.

8. Do you have comments on how and where data comparisons between PSPs are published, including our proposals to compare PSPs at PSP group level?

We remain concerned that for larger banks, a significant minority of their APP fraud cases will be 'on us' payments, where the bank is both the sending and receiving bank.

The PSR has indicated that it will ask for voluntary agreement to include these figures in the totals shown.

It is entirely possible that the larger banks will agree to do this, but display data on their websites which excluded the 'on-us' APP fraud data, making it appear their APP fraud rates are artificially low.

The PSR would have no recourse to prevent this.

We believe the PSR should have more robust plans to prevent this from occurring.

17. Do you agree with our position on improving intelligence against fraud? We welcome any further comments from stakeholders about this work.

Whilst UK Finance and some large banks have been invited to the Joint Working Group mentioned in Section 6, smaller PSPs have not been invited to take part, and have been largely unaware of this development.

Because developing standards for such a scheme has major implications for competitiveness in the payment landscape in the future, the largest banks designing the system whilst their smaller PSP competitors are excluded is extremely anti-competitive, and a breach of the PSR's core aims.

The PSR must ensure that membership and input of the Joint Working Group is open to all PSPs, so that a closed cartel of larger banks does not dominate the standard and tailor the proposals to their benefit.

Introduction to Chapter 6 – Last Paragraph.

The PSR states 'We believe that reimbursement of scam victims should be made mandatory.'

The PSR provides no rationale for this statement where there is no fault by the bank. It is a destructive, retrograde step which would destroy the payment sector in the UK.

Although a welcome safety-net for consumers who may be pressured into loss, it would destroy the UK economy, and cannot be allowed to occur.

If the PSR has evidence for imposing firm-breaking liability on firms in cases of no fault by the firm, and where the firm is not involved in the fraud, then the PSR should present such evidence.

The PSR has not done so, and until the PSR does (and it cannot), the PSR should remain within its own core principles and not seek the destruction of the UK payment landscape and the introduction of an anti-competitive payment landscape.

Paragraph 6.1

The claim by the PSR that the CRM is leading to improvement in outcomes is not borne out by fact, and this claim should be withdrawn, or evidence published.

Paragraph 6.2

The improvements in the past year of performance of compliance with the CRM has been minimal.

The PSR's claim that consumer outcomes under the code are likely to improve is not so, and the evidence presented is underwhelming.

The protection available to consumers and small businesses is already much greater under the FHC than the CRM – so the FHC should be prioritised.

[Remember, there are hardly any cases where the receiving-bank is not at least partly at fault in APP scams, and so receiving banks will virtually always be liable under the FHC. And in the very, very rare cases when no bank is at fault in an APP scam, then it would be wrong to make a bank bear the loss].

Question 18. Do you have any comments on our thinking on how the roles of the bodies currently involved in the CRM Code would differ between the two options under Measure 3?

With regard to option 3B (mandatory sign-up to a PSR approved code), it seems the PSR has got its thinking in a muddle.

All banks already have been signed up to an incredibly strict code, with mandatory enforcement.

That code states that the bank is liable if the bank has not done enough to prevent the APP fraud.

It is not possible to find a stricter or more stringent code.

That code is the FHC, and a core part of the current FCA Handbook which is already imposed on all banks and PSPs.

So the CRM and the LSB are irrelevant, as all banks are already part of the strictest and most stringent code possible.

The PSR just needs to publicise the FHC, so that consumers and small businesses can become aware of their existing protection under the FHC, and claim their rights.

The only area where the FHC does not provide protection is where no bank was at any fault.

And as we have highlighted and explained above, that is hardly ever the case, as the receiving-bank nearly always is at least partly to blame for the APP fraud.

In the very, very rare cases where no bank is at fault in the APP fraud case, then no bank should have liability imposed on it.

With respect to option 3A (Pay.UK changing Faster Payment rules), this would mark the destruction of Faster Payments!

Payment Providers would switch to other methods other than Faster payment, and change their systems to ensure their customers do not use Faster Payments, as the liability from no-fault Faster Payment APP fraud claims will bankrupt any bank that continues to use this payment rail.

Paragraph 6.25

It is critical to the UK economy that a payment method is available which is not susceptible to chargeback.

Whereas chargeback under credit card payments is a very useful consumer protection, there are some goods and services which cannot be sold using a payment method that can be subject to chargeback, as the risk of fraud to the seller from false chargeback exceeds the expected profit.

A well-functioning society requires at least one payment method that is not subject to chargeback, and that method at the moment is bank transfer.

It is a colossal error for the PSR in this paragraph to mull making bank transfer subject to chargeback, and this must not be allowed. The UK economy requires one payment rail available that is not subject to chargeback.

Separately, as is correctly pointed out in this paragraph, the balance of liability between sending and receiving banks requires examination and appropriate action, as at present the sending bank is the focus for customer reimbursement, when it should be the receiving bank.

Annex 2 Paragraph 2.7

Under the PSR's proposals, it is not economically viable for a bank or PSP to take on a customer who is at high risk of APP fraud in a case where the bank has no fault.

So vulnerable customers become unacceptable customers to banks.

The bank can hope to earn a matter of pennies or pounds from taking in such a customer, but the cost of expected no-fault loss by the bank to APP fraud from this customer could easily be tens or thousands of pounds.

The PSR may insist that banks must not discriminate against vulnerable customers, but no bank can survive leaking huge liability when there is no commensurate income – that defies the laws of economics.

So either banks necessarily discriminate to remain solvent, or banks become insolvent.

The PSR is attempting to defy the laws of economics, and the PSR is acting unfairly and irrationally here.

Finally, may I also persuade you please to make the APP compensation mandatory and not reliant on a voluntary code. Fraud, notably APP fraud is at epic levels and rising and clearly the voluntary code is not sufficient nor adequate to satisfactorily protect consumers. The Treasury Committee directed that the enforcement of APP fraud compensation should be backdated to September 2016 when Which Consumer research made their complaint on behalf of consumers. Their complaint was upheld however the FCA made the compensation effective

from 31st January 2019 and based on a rather ineffective voluntary code. Few if any victims have been compensated, underlining the ineffectiveness of voluntary practice in UK banking. Given the profits made by UK Banks from providing accounts to criminals please reconsider and make the compensation mandatory, and from 2016. The Banks were well aware of APP fraud from 2013 as Which pointed out in their complaint and have had more than adequate time to prepare. It's time for the FCA and PSR to do something meaningful for public protection and for victims of this heinous fraud.

Please let us know if you require any clarification or further information on the above.

Kind regards,

Andy

Andy Agathangelou FRSA

Founder, Transparency Task Force; a Certified Social Enterprise
Governor, Pensions Policy Institute
Chair, Secretariat Committee, APPG on Pension Scams
Chair, Secretariat Committee, APPG on Personal Banking and Fairer Financial Services
Chair, Violation Tracker UK Advisory Board
Policy Adviser to Parrhesia, the Whistleblower Research Charity
Telephone: +44 (0)7501 460308