To: Payment Services Call for Evidence

From: Transparency Task Force

Date: 27 March 2023

Review and Call for Evidence into the Payment Services Regulations

Transparency Task Force (TTF) is a Certified Social Enterprise operating as a non-profit with the sole purpose of driving positive, progressive, and purposeful finance reform.

Several of our members have been actively involved in the area of Payment Services for many years and given their insights we have chosen to feedback on three main areas covered by the Regulations. These are: -

(i) the pervasive nature of misleading promotions around cross-border payments

(ii) the need for greater pricing transparency earlier in the customer journey for cross-border payments

(iii) some detailed recommendations as to how to reduce the consumer harm from Authorized Push Payment Fraud

Accordingly, we have chosen to complete our response using thematic headings rather than reply strictly to the questions asked which in a number of cases are themselves based on assumptions that we feel are not justified.

1) Failure by the FCA to enforce the existing PSR re the use of Agents

TTF is concerned about the failure of the FCA to regulate cross border payments in accordance with the existing Payment Services Regulation 2017. In particular its persistent failure to recognise or act on widespread use of unregistered agents by APIs.

This is made considerably worse by the fact that the FCA then chooses to ignore the widespread use of misleading advertising practices by these unregistered agents as they respond to

complaints by saying these firms are outside the regulatory perimeter. In the specific case of misleading statements by these firms concerning payments involving currency conversion, the FCA have actually in effect stopped the Advertising Standards Authority from acting as they would normally do, as the FCA requested in 2016 that all misleading advertising complaints concerning payment services firms be made the responsibility of the FCA and not the ASA. The ASA has complied, but then the FCA has not stepped into the vacuum it created.

Given this highly unsatisfactory situation it is unsurprising that there are a wide range of misleading promotions, claims and practices. This is causing significant consumer detriment which TTF estimates to be at least £1.75bn per year as well as a competition issue which means smaller, innovative, and competitive firms are unable to participate in the market.

The current regulations are well written, comprehensive, and clear regarding the use of agents. An agent is any individual (or entity) acting on behalf of an API. The term "on behalf of" is broad and is intended to prevent firms from circumventing the requirement for registration by calling their agents "partners", "introducers", "affiliates" or other such non-applicable terms. APIs use agents to perform diverse functions, including originating business for the APIs. The intermediaries can be considered agents because (i) they are compensated by the APIs for services provided to the APIs and/or the customers, and (ii) the APIs hold out to the customers that they may deal with intermediaries in relation to payments services matters.

However, the FCA's failure to recognise what constitutes an "agent" and, therefore, what should be a registered organisation within its regulatory perimeter, means that entirely unqualified and unaccountable entities are misleading consumers on a colossal scale.

These entities include national newspapers, fake "comparison sites", overseas property magazines, "white label introducers" and even government agencies. They are telling consumers that their favoured API provides the "best rates", unsubstantiated savings against the banks, "fee free" transfers and a plethora of other misleading statements which all break the Advertising Standards rules.

This means consumers are being driven to a tiny group of large non-bank payments providers, on false pretences, and leaving smaller more competitive players without marketing channels.

The fault lies not with the regulations but with the FCA's comprehensive failure to enforce them. The following is needed:

1) A fundamental understanding by the FCA of what constitutes an "agent" under the PSR
2) Suspension of the use of any unregistered agent unless or until they have been properly registered
3) Clear instruction from the regulator about what messages an agent is permitted to give under the Regulations

Immediate action from the regulator as described above would ringfence the promotion of payment services and limit approval of promotions on their behalf to Authorised Payment Institutions themselves.

Further, the FCA must also either strengthen its own competency in the field of advertising law or work closely with the national expert in these matters, the ASA. At the moment the FCA appears to have neither the knowledge or expertise to recognise breaches of the ASA standards and, therefore, breaches of the Consumer Protection from Unfair Trading Regulations (CPRs) on which they are based.

Compliance with the CPRs is a pre-condition of API authorisation. In particular, the FCA has repeated demonstrated ignorance of the "misleading omission" aspect of the legislation with particular reference to upfront and transparent pricing.

TTF has obtained Counsel's opinion on this matter and is certain that the almost complete lack of upfront, accurate price information in credit transfer section of the payment industry would constitute a breach of the "misleading omission" requirement of the CPRs and, therefore, a breach of PSR authorisation criteria.

We believe that APIs should be showing clear, consistent pricing information as soon as possible in the consumer journey, i.e. on the Home page of their websites, to enable consumers to make an informed transactional decision about which provider(s) to register with. See further details in section below entitled "Greater Pricing Transparency for Cross Border Payments".

2) Greater Pricing Transparency for Cross-Border Payments

Cross-border payments are a very attractive activity for banks and other payment services providers as they can be subject to a variety of fees as well as margin on the FX conversion.

As a consumer or a SME, it is extremely difficult to obtain useful information on what a cross-border payment will cost you before signing up to a payment service provider and making the payment.

As we point out elsewhere in this submission the vast majority of promotions in this space are not regulated by either the Advertising Standards Authority or the Financial Conduct Authority, so even if you end up on a price comparison site you will probably be given only partial and misleading information.

Thus, for example, FXcompared.com, which also provides their service for moneysupermarket.com, boldly states on their front webpage "Compare the best international money transfer companies". In practice they only search a very small number of the larger payment services firms (it appears to be almost exclusively 4 firms namely OFX, Moneycorp, Currencies Direct and TorFX; with one in about 100 searches producing an alternative name such as Smart Currency Exchange) and then simply calls back a rotating three names and places

them in a rotating order (not linked to the amount received). It then has the gall to label them as the 'Top 3 Money Transfer Providers' for that specific currency payment. FXcompared.com gets paid commission as an "affiliate" for introducing this business to the payment services firms and yet the FCA chooses to believe that this explicit financial arrangement does not make FXcompared.com an agent of these firms under the PSR 2017 and thus this website is outside the regulatory perimeter, and they can thus continue to act in this highly misleading manner.

In addition to the upfront pricing information on individual websites detailed above, which we consider to be a requirement of the Consumer Protection from Unfair Trading Regulation (CPRs) , to radically improve the ability of consumers to shop around efficiently and effectively, we believe that there is a strong public benefit argument for establishing a not for profit, paid for by a modest levy from the industry, to build and maintain a market wide price comparison site. Banks and APIs would mandatorily have to contribute actual prices to this site, so that both consumers and SMEs could quickly and reliably access genuine comparable market pricing, which would include all fees and the FX margin measured against the interbank mid-rate for that currency pair. This enhanced transparency would have enormous public benefit for consumers (estimate of at least £1bn per annum) and increase the UK's competitiveness for small businesses looking to export or import (again a similar benefit of c. £1bn per annum for just small SMEs). There would be a one-off cost to establish the website (estimated at £2m) and then an ongoing cost to maintain of less than £1m per annum.

As a separate initiative to improve pricing transparency we would like to see clear, concise, accurate pricing information as early in the customer journey as possible i.e before a customer has been forced to sign up to the firm's terms and conditions.

The example below represents the simplest presentation of information that we'd expect to be included: -

- Sent and received amounts

  You send: £10,000
  Your payee's bank receives: €11,212.5

- Total cost of service

  Total cost of service: £250 (2.5%)

  The cost should be given in the base currency i.e. the currency that the customer started with

- Cost breakdown (in a pop-up)

  Cost breakdown:
  Currency conversion cost: £200 (2%)
  Payment service cost: £50 (0.5%)

- Your effective exchange rate (the effective rate the firm is offering to the customer after all costs)

  Your effective exchange rate: €1.12125 for every £1

- Market exchange rate (the mid-market interbank reference rate)

  Mid-market interbank exchange rate: €1.15 for every £1

- Time stamp

  Precise time down to the second the reference rate was fixed

3) Increasing the Threshold Conditions for larger APIs

Recent history, such as Wirecard or Premier FX, shows that APIs are potentially vulnerable to fraud by both owners and staff and that the losses arising from this fraud can be significant.

With potentially large daily turnover such firms are subject to money laundering risks, potential fraudulent diversion of funds or the making of payments to potential bad actors overseas. Yet the oversight for APIs engaging in such activities remains very light compared to banks.

TTF believe that the capital requirements and supervision fees should more accurately reflect the risk profile of the firms being regulated.

The two most obvious risk factors are size and whether a firm makes solely domestic payments or makes cross border payments and even for cross border payments different countries have different risk profiles.

We think that there is a strong argument for increasing the capital requirement calculated in method A from 10% of fixed overheads to 25% of fixed overheads (this would increase the capital required for larger firms without impacting smaller firms which are hit by the minimum fixed amount).

Whilst we would like to see Payment Services firms minimize the funds they hold before making payments we would like to see a new requirement for an annual external audit of client monies/safeguarded funds for all APIs above a certain volume threshold.

Overall, we also believe that the FCA resources allocated to Payment Services need to be increased/improved and if that requires an overall increase in supervisory fees for the industry then so be it. One of our broader observations is that we think that the FCA has been deliberately set up as a very poor relation to the PRA and the Bank and that this is clearly reflected in staff pay, pensions and even office location. This has the obvious impact of making the FCA a considerably less attractive place to work for ambitious and competent regulators.

If this change was combined with the FCA also putting pressure on banks to provide the necessary client accounts for FCA authorized APIs this would benefit competition in the UK.

4) Safeguarding of Funds vs Segregated Customer Accounts

TTF is concerned that funds paid by customers to APIs are subject to a confusing mix of segregated customer accounts and "safeguarding" accounts. This is because "safeguarding" only applies to a customer's funds in a very specific subset of circumstances. A first party payment is never safeguarded, however, long the payment delay and a third-party payment is only safeguarded after 2 nights delay with funds in the same currency as the proposed payment.

In particular, we are concerned that:

1. The criteria for safeguarding compared to segregation of client monies are so specific and complex that they cannot possibly be understood by even an informed consumer. A customer's money may go through both processes, but the customer will have no idea what level of protection they have at any one time. As safeguarding is designed to protect customer funds, a customer will not be able to make an informed decision about where and how to place their funds.

2. We do not have accurate numbers for the industry, but we believe that the total amount of funds meeting the safeguarding criteria is likely to be a modest percentage of the total funds held by APIs and a tiny percentage of the payments made. Yet safeguarding appears to take up a disproportionately large amount of time and resource for both APIs and the FCA. We believe that the FCA and APIs should be concentrating on ensuring that the vast amount of customer monies which are not "relevant" funds for safeguarding are properly segregated rather than just the minority of "relevant" funds.

3. The FCA Approach Document says:

10.22 The EMRs and PSRs 2017 safeguarding requirements only apply to relevant funds. Sometimes, however, such businesses will not know the precise portion of relevant funds and funds received in relation to the non-payment service provided, or the amount may be variable. In these circumstances, an institution may make a reasonable estimate on the basis of relevant historical data of the portion that is attributable to e-money/the execution of the payment transaction and so must be safeguarded. The institution would, if asked, need to supply us with evidence that the proportion actually safeguarded was a reasonable estimate. Relevant data might include the portion generally attributable to e-money or payment transactions by the customer in question or by similar customers generally.

This in effect means the process for deciding which funds to safeguard is itself imprecise, and thus muddies the boundary between segregated customer balances and safeguarding balances.

4. The cut-off time for deciding safeguarding of "funds which are going to be held overnight on the day following receipt by the API" appears to be an entirely arbitrary timeframe set by legislation. Why this timescale instead of any other? If safeguarding is such a good thing, why not insist that all customer balances are held in safeguarding accounts except for when being processed?

Whilst not legal experts, TTF would recommend that the UK look to align APIs (and EMIs) with other financial services firms such as insurers and investment firms who are required to hold customer monies in client accounts with banks and are subject to the clearly documented and well understood CASS requirements. This alignment would make it easier for consumers, firms, the FCA and external auditors to understand what protection is provided.

5) Inappropriate Termination of Payment Services Contracts

TTF believe that the minimum of two months' notice as set out in Regulation 51 is appropriate as it allows a reasonable time for the account holder to make alternative arrangements.

However, this provision only addresses the question of actual termination. Several banks are flouting this Regulation by imposing an immediate "freeze" on a customer's account, thus depriving them of both the money held in their account and the banking services that they are reliant on, without giving them any notice at all.

Such actions are similar to that of a property landlord who gives notice to terminate a tenancy but them immediately changes the locks, thus depriving the tenant of the use of the property during the notice period. Such actions are completely unacceptable and must be addressed in future regulations.

Providers must not be allowed to freeze <u>all</u> of the money held in a customer's account unless they have a reasonable basis for believing that <u>all</u> of the money in the account was obtained through fraud, or was the proceeds of crime, sanctions evasion or terrorist financing.

Where a Provider has a reasonable basis for believing that a specific inbound payment has been obtained through fraud, or was the proceeds of crime, sanctions evasion or terrorist financing then they must have processes in place to freeze only that specific inbound payment while their concerns are investigated.

Recognising the recent development of the "cancel" culture it is important that banks should not be allowed to behave in the way that a major bank did towards a charity by closing its account, apparently in response to pressure for another campaigning organisation that publicly opposes what the charity does. The bank's actions were unacceptable.

Providers must not be allowed to terminate a framework contract that was concluded for an indefinite period solely based on the views held by the account holder, provided that those views are held and expressed in a lawful manner.

6) Protecting Customers from Fraud

Most Providers have consistently failed over a period of many years to develop and implement systems and processes that would have protected customers from harm, specifically the financial and emotional harm caused by Authorised Push Payment Fraud (APPFraud).

TTF believe that all Providers of standard current accounts to retail customers must be required to develop, implement, and regularly update fraud prevention measures that address all known risks of fraud.

Confirmation of Payee

One example of the long-term failure of both the banks and the regulators to prevent fraud is Confirmation of Payee (CoP). One can describe this failure as "taking seven years to shut the stable door, but not bothering to build the back of barn".

In January 2012 Tidal Energy Limited became the victims of APPFraud when they gave an instruction to Bank of Scotland to make a payment of £217,781 to a supplier. Unbeknown to them, the unique identifier (i.e. the sort code and account number) that they had been given for the payment was that of the fraudster's account. This fraud would have been prevented if Tidal Energy had been able to confirm the name of the beneficiary account, however, when the Faster Payment System was introduced in 2008 the banks dropped any reference to the Payee name, as had been used with cheques, relying instead on the unverifiable unique identifier.

It was not until 2020 that the major banks introduced CoP, and they only did it then because they were Directed by the Regulator to do so. Although CoP covers the overwhelming majority of payments it is important to realise that the partial implementation, limited to just the top few Providers, has allowed fraudsters to move their accounts to the Providers that have not yet been able to join the "CoP Club". By way of a comparison, the SurePay system that was developed in Holland has validated over 99% of payment transactions across the entire Dutch financial system for several years.

The CoP system that was introduced by the major banks in 2020 was itself limited to validating the Payee name for a unique identifier (i.e. the sort code and account number) and did not validate the "Secondary Reference" that had been given by the Payer. The system has now been upgraded to support Secondary Reference validation, but this functionality has not yet been implemented by every Provider.

There are an increasing number of situations where the actual beneficiary account (or wallet) is not identified by the unique identifier, but by the "Secondary Reference". An obvious example is payments of income tax to HMRC. Payments are made to a single HMRC account and then credited to the individual's tax account by reference to the Tax Reference given in the Secondary Reference field. "Secondary References" are widely used in crypto-currency and FX transactions, making them attractive places for fraudsters to hide their accounts (or wallets).

TTF would like to see Confirmation of Payee, including verification of any Secondary Reference, be implemented by every Provider of standard consumer current accounts by no later than 31 December 2023.

Civil or criminal test for fraud?

The word "fraud" appears 16 times in the Review and Call for Evidence, but what is the standard of the test for fraud; civil or criminal?

There are an alarming number of cases where the Provider declines reimbursement of an APPFraud on the basis that it is a "civil dispute" and not fraud, meaning that the CRM Code does not apply.

Claims for reimbursement are civil claims so TTF believe that the test for "fraud" should be the civil test of "on the balance of probabilities", rather than the very much higher standard of the criminal test of "beyond reasonable doubt".

Adopting the civil standard would not only make it clearer for the Providers and FOS, but it would also recognise that whilst 40% of all crime is considered to be "economic crime" only 2% of Police budgets are allocated to responding to it. It is vital that Providers are not allowed to argue that an APPFraud is not fraud just because there is no criminal prosecution.

Who is "another person"?

Another aspect of "What is Fraud?" is expressed by considering the two phrases "another person" and "me-to-me".

Annex A of the FCA Policy Statement PS18/22, December 2018, inserted the definition of authorised push payment fraud into the glossary of the FCA Handbook, with effect from 31 January 2019, as:

> a transfer of funds by person A to person B, other than a transfer initiated by or through person B, where:
> (1) A intended to transfer the funds to a person other than B but was instead deceived into transferring the funds to B; or
> (2) A transferred funds to B for what they believed were legitimate purposes but which were in fact fraudulent.

The equivalent wording in section DS1(2)(a) of the CRM Code, introduced in May 2019, reads:

> (i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or
> (ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.

The difference in wording between the FCA Handbook and the CRM Code, and the different use of the same phrase in the CRM Code, create significant difficulties.

FCA(1) says "a person other than B" which could include "A", but CRM (i) says "to another person".

CRM (i) uses the phrase "to another person" to mean the intended payee, whilst CRM (ii) uses the phrase to mean the fraudster.

The unhelpfulness of the different wording is compounded by the question: Who is "another person" in the context of CRM (ii)?

Saying that a payment must have been made to "another person" to even possibly be considered to be fraudulent, is generally accepted to mean that if the payment is made to an account in the Payer's name, i.e. "me-to-me", then it cannot be fraud. We disagree with this simplistic approach because it relies on the name on the Payee's account rather than who controls that account. There are cases where the fraudsters created a new Payee account (or wallet) in the victim's name having obtained copies of their ID documents through deception. The account is in the victim's name, but the fraudsters also have the security credentials, giving them unrestricted access to any money that the victim puts into the account (or wallet).

TTF believe that future regulations need to bring clarity to the questions: "What is Fraud?" and "Who is "another person""?

Payment delay

The Call for Evidence proposes a review of the requirement for Providers to ensure that payments are credited to a receiving account by the end of the next working day ('Day+1').

We broadly support the suggestion that the sending Provider should be allowed to delay payments beyond Day+1 in a very tiny number of complex cases, but this consideration may be obscuring far more important developments in fraud prevention.

In November 2019 the Treasury Committee report "Economic Crime: Consumer View" endorsed my proposal, which I had already put to the major banks and UK Finance, that there should be "a mandatory 24-hour delay on all initial or first-time payments". This proposal was endorsed again in the recent House of Lords report "Fighting Fraud: Breaking the Chain".

The specific detail of my proposal for 24HrPD is simply that: “No high value payment should be released from the Payer’s account to a new Payee until a clear 24-hours after that Payee has been created within the Payer’s account”.

The “high value” limit for delaying “first-time payments” should be set by either HMT or FCA and apply consistently to all Providers. It could be as low as £500.

The rational for this proposal is that fraudsters frequently apply manipulative pressure on the victim of an APPFraud to make the payment, or move their money to a new “safe” account, immediately; thus removing the opportunity for them to “take-five” and consider if it might be fraud. A clear 24-hour delay would provide this opportunity for the victim to realise what was happening and stop the payment before it even leaves their account. It would also increase the window for the bank to review the payment.

UK Finance have publicly argued that such a delay is not permitted under PSR2017, but they have not provided any correctly applied regulatory support for their argument. Conversely, this Review clearly shows that delaying a payment until “Day+1” is already permitted.

This is another example of the banks knowing that they could do something to prevent both unauthorised transaction fraud and APPFraud, but have chosen to not do so.

It has also been argued that it would be very inconvenient for the customers, but does this argument have any validity? We believe not.

The question that I ask is: “When was the last time that you needed to make a payment of more than £500, to someone to whom you had never made a payment in the past, and did not have their account details at least 24-hours before they needed the money?”

In the five years that we have been asking this question we have had just one response where it would have been significantly inconvenient, and this could have been resolved very easily by a phone call to the bank; not forgetting that the banks regularly “hold” payments and require the customer to phone them.

A 24-hour Payment Delay should be the default status on high value payments to new payees.

In light of certain other types of fraud we suggest that the banks should also be required to allow customers to specify that all payments over a certain value, specified by the customer, should be delayed by 24-hours.

Second Party Notification

These two proposals open the way for a development of a new system that is specifically designed to reduce the risk of APPFraud on older or vulnerable, people. It is called "Second Party Notification" (2ndPN).

'2ndPN' would be an opt-in system whereby, whenever the bank sends an important text message or email to a customer, that message is also sent to a "Second Party". The second party would typically be a son or daughter, or parent, or carer; but it could be anyone who the account knows and trusts. The Second Party would not have access to the person's account; they would simply get the messages, giving them the opportunity of contacting the person and "just checking" that all is OK. We can identify cases where APPFrauds exceeding £100,000 each would most likely have been prevented if this system had been available.

New regulations should allow all Providers to offer Second Party Notification.

Assisting a claim for fraud

Although PSR 2017 Regulation 90 (4) is not specifically referenced in this review, we believe that changes should be considered as part of the overall approach to fraud.

This regulation comes under the heading of "Incorrect Unique Identifiers" and says:

"If the payer's payment service provider is unable to recover the funds it must, on receipt of a written request, provide to the payer all available relevant information in order for the payer to claim repayment of the funds."

The banks argue that this regulation does not apply to the majority of cases of APPFraud.

The question thus is: "Should the victim of an APPFraud be entitled to obtain the full details of the beneficiary account so that they can pursue a civil claim against the account holder in order to recover the money that they had paid to them as a result of the fraud?"

There clearly are important issues around GDPR but, it is TTF's view that the victim of an APPFraud should be able to take civil action against the fraudster who has stolen their money. A possible approach might be to say that the information could only be provided to a solicitor who had been instructed by the victim to pursue a civil claim.

7) Conclusion

The main individual contributors to this document were as follows:

For sections 1), 2), 3) and 4)

Ian Tyler, Chair, NED and Senior Advisor for a number of Fintechs (none operating in Payment Services)

For sections 5) and 6)

Richard Emery, Bank Fraud Consultant

Whilst most submissions to this Call for Evidence will unsurprisingly come from the industry itself, TTF believe it is important that the consumer voice is heard as part of the Call for Evidence. We are in favour of continued innovation and understand the essential role that payments play in a modern online economy.

However, we do believe that legislation should be adopted to provide greater protection against push payment fraud for the vulnerable, should legislate for earlier standard pricing transparency for cross-border payments and that the FCA should enforce the current PSR 2017 legislation properly with respect to Agents and thus seek to eliminate misleading promotions.

If there are any clarifying questions please reach out to IanTyler@fmcr.com in the first instance and he will ensure that the most appropriate person answers the question.

On behalf of the Transparency Task Force.

Andy Agathangelou FRSA

Founder, Transparency Task Force; a Certified Social Enterprise

Chair, Secretariat Committee, APPG on Personal Banking and Fairer Financial Services

Chair, Violation Tracker UK Advisory Board

Chair, RSA's Financial Services Network

Telephone: +44 (0)7501 460308