Lyddon
CONSULTING

+44 (0) 7979 132 341
enquiries @lyddonconsulting.com
www.lyddonconsulting.com

Payment Services Regulations - Review and Call for Evidence

9th March 2023

Response submitted by: Bob Lyddon, Lyddon Consulting (www.lyddonconsulting.com)

What is Lyddon Consulting?

The 'trading-as' style of Bob Lyddon, a specialist consultant in payments and electronic banking. We have recently acted as advisor to:

- A law firm regarding the degree of malpractice against regulations for Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) involved in Payment Service Providers (PSPs) issuing non-existent account numbers and disguising the intermediary PSPs involved in a payment chain;
- An Electronic Money Institution on transitioning from using Virtual International Bank Account Numbers (IBANs) to using ones identifiable to itself;
- The UK Association of Payment Institutions regarding access to bank accounts at UK banks for payment operations and for safeguarding;
- A Payment Institution about the nature of its payments between its own accounts, given the upshot of financial regulators' position that payments have to be put at the disposal of the payee before the funds for that payment can be released from a safeguarding arrangement; and
- A global payments communications cooperative regarding opportunities and threats emanating from changes in the UK payments landscape.

Contact details

Lyddon Consulting
6 The Glebe
Wells-next-the-Sea NR23 1AZ

07939 – 132341

bob@lyddonconsulting.com

www.lyddonconsulting.com

Call for evidence: questions for stakeholders and our responses

General questions

How should the payment services framework evolve – and what should be the government's priorities – to better promote the following government objectives for payments regulation:

A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector

B. Ensuring appropriate trust and protection for consumers

C. Ensuring the resilience and integrity of the UK's payment market

D. Fostering competition, in the interests of consumers

In answering the above, the government would welcome concrete reflections from stakeholders for future policy, rather than the principles which should underpin regulation/regulatory change.

A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector

There is a non-sequitur at the heart of this formulation. The 'international competitiveness of the UK economy' is not a function of the 'growth and innovation in the UK payments sector'. The payments sector serves the wider economy but does not create GDP growth in its own right and separately from the underlying economy.

People and businesses do not make more payments just because there are different and supposedly innovative ways of making them.

What has happened in the UK is the fostering of digital means of payment at the expense of non-digital ones (cash, bank drafts and cheques) in a zero-sum game in terms of volumes of payments and in a questionable manner in terms of the distribution – between Payment Service User (PSU) and PSP – of the rewards, costs and risks:

- Lower costs for PSPs through the fostering of instant credit transfers via Faster Payments but a higher risk of fraud for PSUs (i.e. Authorized Push Payment Fraud or APPF);
- Higher revenues for PSPs in terms of deductions-from-face-value on card payments, which have achieved high market penetration, and with consequential increases in prices on all goods and services for people and businesses, a contributor to inflation.

This is laid out in our recent paper entitled 'CAPTURE – BigTech and Digital Payment Giants dominate the committees evaluating the replacement of physical cash with 'Britcoin' – a UK 'Central Bank Digital Currency''.

You can find a click-through to the full paper here:
http://www.lyddonconsulting.com/capture-a-major-new-paper-on-the-committees-considering-a-uk-central-bank-digital-currency/

This blog acts as a summary:

http://www.lyddonconsulting.com/digital-payment-failures-fraud-and-card-deductions/

B. Ensuring appropriate trust and protection for consumers

This has gone badly adrift in the case of APPF. We refer you to Appendix 4 on p. 97 of our Central Bank Digital Currency paper 'Solution to Authorised Push Payment Fraud (APPF)':

QUOTE

Background
This problem occurs because payment services providers (PSPs), addressable through the Faster Payments scheme, do not ensure that they pay the payee named in the payment. The payer names the payee in the underlying payment order – it is mandatory information, without which the payer's PSP will not accept the payment order for execution. It is transported through the Faster Payments system to the payee's PSP, but the payee's PSP does not check that the name in the payment is consistent with the name associated with the account as identified by the Sort Code and account number. The Sort Code and account number are required in the payment order, and travel through to the payee's PSP. They constitute a 'Unique Identifier'. Under current UK case law, the 'Unique Identifier' is a sufficient basis for the payee's PSP to credit an account, without checking the name. This is costing UK businesses and individuals hundreds of millions of pounds per annum, and efforts over an 8-year period by the 'payments industry' have delivered ineffective measures such as the Contingent Reimbursement Model and Confirmation of Payee. Under this latter process, PSPs do check the name against the Sort Code and account number associated with it, demonstrating that the name check is technically and operationally possible.

Solution
The 2017 Payment Services Regulations need to be amended to make the payee name part of the payer's contract with the payer's PSP, and to specify that this is a provision that cannot be opted out of in a Framework Contract.

The Funds Transfer Regulation needs to be amended so as to withdraw the dispensation that a national payment in £pounds can be completed solely on the basis of a 'Unique Identifier'.

Outcome
The payer's PSP will have a payment contract with the payer under which it must honour all of the payee name, Sort Code and account number. If it effects payment to an account with any element in this data out-of-line with the contract, the payer's PSP is guilty of defective execution of the payment contract and must provide full restitution to the payer. There will be no get-out as is provided by Funds Transfer Regulation now, that permits processing only on the basis of the 'Unique Identifier', whether that be the Sort Code and account number for a national payment in £pounds, or IBAN (International Bank Account Number) for a cross-border payment or one in foreign currency.

Pushback
There will be pushback from PSPs that they cannot be expected to check the details on the payee's account when it is not an account in their books but in the books of a different PSP. The rejoinder to that is, firstly, that if it is possible in the case of Confirmation of Payee, it is possible for every payment. Secondly, the PSPs designed the Faster Payments scheme as it is today, so they are free to re-design it or invest in another scheme so as to address this issue. If they decide amongst themselves that they do not want to invest in either a re-design or a new system, they can bear the losses from APPF, but it is not fair that the issue remain unresolved and that end users continue to suffer losses emanating from it.

Conclusion

APPF may occur through the CHAPS scheme and through the BACS scheme, but the vast bulk occurs through the Faster Payments scheme. Concentrating on Faster Payments and implementing the proposed legal changes will eliminate for the end user a major portion of APPF, by simply making the payer's PSP legally liable to the payer for getting the basics right: for paying the payee that the payer named. Achieving this degree of end user protection was the purpose of the 2017 Payment Services Regulations but there is a loophole. Plugging that loophole establishes the correct baseline of responsibilities and risks when end users have their payments made through a system designed by their PSPs.

UNQUOTE

Fraud protection and PISPs

Fraud protection for the PSU has been further damaged by Payment Initiation Services Providers or 'PISPs', from whom the main payment option is a Faster Payment. We refer you to p. 18 of our Central Bank Digital Currency paper within the section entitled 'Open Banking pitfalls – including Authorised Push Payment Fraud':

QUOTE

A PISP cannot hold customer funds but it relays customers' payment orders to customers' banks. The value of the PISP is convenience: a customer gives it the security credentials for all their bank accounts, enabling the convenience of not having to log in separately to each bank's eBanking service with differences of process, devices, User IDs, passwords and so on. The customer need only concern themselves with the credentials to log in to the PISP's service. This means that a fraudster, obtaining the customer's credentials for their relationship with the PISP, can empty all of the customer's accounts in one go. Major banks are reputedly afraid to raise this issue to the Competition and Markets Authority for fear of being labelled anti-competitive.

UNQUOTE

PISPs and Contingent Reimbursement Model Code

Lack of resources at a PISP will be an issue should the authorities attempt to pursue the option of having PISPs join the Contingent Reimbursement Model Code (or 'CRM') for victims of APPF. This was suggested by the Payment Systems Regulator's 'Digital Payments Initiative' committee. Please refer to pp. 39-40 of the same paper in the section 'Authorised Push Payment Fraud through Open Banking is acknowledged – but not solved':

QUOTE

The report [of the Digital Payments Initiative] proposes, on p. 7, that Open Banking intermediaries should join the CRM, when the problem occurs that we mentioned earlier. At least we should be grateful that the problem is acknowledged, namely that thanks to PISPs (Payment Initiation Service Providers), fraudsters need only obtain one set of the customer's eBanking credentials in order to clear out all their accounts. However, since PISPs are by their nature thinly capitalized, it is a question of pure conjecture whether the PISP will have the resources to reimburse the entirety of a customer's money back even if they are bound by the CRM.

The proposal will only work if the risk can be covered under the PISP's professional liability insurance, and for a sum that will be radically in excess of the PISP's own resources: the maximum possible loss is the entire amount in all the accounts registered at the PISP for all its customers.

How will the PSP even know what that is at any one time? How can that be translated into a maximum amount insured such that the premium can be calculated and paid, and the cover put on-risk? How can it be ensured that the PISP abides by the policy conditions and that the premia continue to be paid, so that any claim is paid out and not refused by the underwriter? How is it ensured that a pay-out from the policy goes to the victims of fraud in the case that the PISP is itself insolvent?

UNQUOTE

Customer detriments at AISPs

A further two detriments have emerged at the other type of 'Third-Party Provider' – an 'AISP' or Account Information Service Provider.

Firstly it 'handles sensitive customer data and there must be a question as to whether the size of investment deployed enables an IT architecture commensurate with properly discharging the AISP's duty to safeguard this data.'

Secondly, AISPs are selling on data to third parties, without it necessarily being aggregated or anonymized. While the direct buyer from the AISP may not be a scammer, the data can fall into the hands of a scammer along the way, in which case the scammer can all the more easily groom the scam victim into believing the scammer is either the AISP or the victim's Account Servicing PSP, because the scammer has the victim's account information in front of them.

The propensity of AISPs to sell customer data is caused by the absence of other revenue streams. This means that there are no profits being added to the initial, very low amount of capital – even lower than that required to establish a PISP, which is lower than is needed for a Payment Institution or eMoney Institution.

Lack of adequate resources within the Fintech sector overall

The Fintech sector in all its guises lacks capital and profitability, and that means that the sector has inadequate resources.

Lack of resources exists in part because the barrier for the capitalization of eMoney Institutions (eMIs) and Payment Institutions (PIs) is set too low, and at an unrealistically low level for them to both operate safely for their customers and compliantly for AML/CFT, and to convince credit institutions to open accounts for them (safeguarding accounts and operational bank accounts).

An inadequate IT infrastructure has recently been blamed by Revolut for problems with its audited accounts.[1]

[1] https://www.reuters.com/business/finance/revoluts-2022-revenues-grew-by-33-despite-crypto-winter-2023-03-01/ accessed on 2 March 2023

Safeguarding arrangements likely to be tested and found wanting

The general undercapitalization of the eMIs and PIs means that the arrangements for protecting customer funds are commensurately more likely to be tested. PSUs will in that eventuality be completely reliant on safeguarding for getting their money back.

The chance of PSUs not getting all of their money back is high, because arrangements to protect customer funds are inadequate:

1. The money that PSUs hold at eMIs/PIs is not in the UK, neither funds held in 'safeguarding' or in operational accounts, with the accompanying uncertainty as to whether funds can be reclaimed and how quickly, and whether a foreign court would treat the PSP's failure in the same way as the UK's regulations governing the PSP expects and so on. Article 105 of the 2017 PSRs was meant to ensure that eMIs and PIs could get safeguarding accounts and operational bank accounts from credit institutions in the UK, but this has not occurred for a number of reasons such as:
    a. The final guidance contained in the 'FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011' of September 2017 in relation to this issue stating that credit institutions were not absolutely compelled to offer services: they could decline them if the returns did not justify the risks;
    b. Credit institutions have used this formulation verbatim when denying or withdrawing services;
    c. Another reason given has been that, in the opinion of the credit institution, the eMI or PI did not have the resources to maintain an adequate AML/CFT environment;
2. The legal situation even in the UK regarding Safeguarding being opaque as demonstrated by the iPagoo case, and the accounting of safeguarded money being inconsistent between one eMI/PI and another;[2]
3. Safeguarded money being in banks of low credit quality, and in financial markets with low standards.[3]

On the other hand the FCA has inadvertently restricted payment volumes by eMIs/PIs

The FCA's implementation of a part of the safeguarding regime – on when funds must go into safeguarding and when they can be released – effectively means that an eMI/PI can only release funds in safeguarding AFTER they have discharged their liability to the payee. This means that the eMI/PI has to discharge the liability with its own money, and then reimburse itself on the safeguarding pool. The results of this are:

- The payment volume that the eMI/PI can be handling at any one time is limited to the amount of its own funds;
- If the eMI/PI has to have its own funds in the amount of each payment, it may as well discharge each payment liability straight away from those funds, after which the money that the payer tendered for the making of the payment belongs to the eMI/PI. Those are not customer funds any longer so they do not need to be safeguarded;
- The situation is aggravated by the 2-3 business day delay between the transaction date and the settlement date for any funds tendered by a payer using a debit card: the eMI/PI is obligated by the Payment Services Regulations to discharge their payment liability to the payee sooner than they get settlement of the funds the payee tendered;

[2] http://www.lyddonconsulting.com/failures-of-fintech-accounting-and-legal-basis-of-safeguarding/ accessed on 2 March 2023

[3] http://www.lyddonconsulting.com/failures-of-fintech-safety-of-safeguarding/ accessed on 2 March 2023

- The situation is further aggravated by the difficulties in accepting cash from payers:
    - Because of the reduced network of bank branches, assuming the eMI/PI can even get an account;
    - Because of the reduced number of security carriers willing to visit eMI/PI premises and collect and deposit the cash;
    - The longer settlement time from using a security carrier compared to directly depositing cash into a bank, assuming the eMI/PI can even find a security carrier.

These problems are the greater for PIs than for eMIs given the business they do. The combined effect has been to eliminate one form of competition – the Small Payment Institution. Many have converted to becoming agents of Authorized Payment Institutions. It will be interesting to see if those with greater knowledge of the eMoney sector make similar observations regarding Small eMoney Institutions.

C. Ensuring the resilience and integrity of the UK's payment market

Not enough is being done to eliminate bad actors. We recently brought three practices to the attention of the trade body that acts for Fintechs in the UK (The Payments Association). This was done via an open letter, the full text of which can be accessed through our website.[4] The three practices are:

1. Manipulation of the scope of the permissions within AML/CFT regulations to which an 'obliged entity' can 'place reliance on' another 'obliged entity', with the intention and effect of shortcutting the Customer Due Diligence process;
2. Usage of Virtual Accounts where banking details are generated (notably an International Bank Account Number) that are identifiable to one PSP but where that PSP has no Customer Due Diligence file on the entity that will be using the banking details;
3. Nesting – where one PSP uses another as its main payment channel, without the other PSP necessarily being visible in the payment message – a problem when measured against Funds Transfer Regulation (EU) 847 of 2015, which requires that payment messages show all intermediary PSPs, as well as the payer's and the payee's PSPs.

D. Fostering competition, in the interests of consumers

Open Banking has become a prime channel for the achievement of this objective, and its success has been vaunted in terms of claims of 7 million users. It is our view that the statistics issued by the OB ecosystem are neither meaningful nor reliable in terms of measuring OB's success so far and of its current supposed status forming a solid basis upon which to create a roadmap for its future.

We have issued an analysis of OB's statistics, the full text of which can be accessed through our website.[5]

We have called upon the Joint Regulatory Oversight Committee for Open Banking to carry out a validation of these statistics as their next step.[6]

[4] http://www.lyddonconsulting.com/open-letter-to-project-financial-crime-c-o-the-payments-association/ accessed on 2 March 2023

[5] http://www.lyddonconsulting.com/open-banking-past-and-present-is-it-a-sham%ef%bf%bc/ accessed on 2 March 2023

[6] https://www.psr.org.uk/our-work/joint-regulatory-oversight-committee/ accessed on 2 March 2023

It was noteworthy that Open Banking did not feature at all in the two surveys carried out YouGov at the behest of the Bank of England and HM Treasury for the purposes of the 'Britcoin' project. These surveys were issued with the consultation papers for the recently-launched public consultation on 'Britcoin'.[7] The results of the two surveys were issued as 'YouGov SMEs Survey data tables' and 'YouGov Consumer Survey data tables'. Neither mentioned Open Banking in any question or in any response option.

2. To what extent would you support rationalising and/or removing the distinctions in regulation between payment institutions and electronic money institutions – in effect, combining the two sets of legislation? Would this be easier for the sector to navigate and/or lead to better outcomes?

We would support this and also cause all eMIs/PIs to be subjected to oversight for AML/CFT by a single body, and not have oversight split between the FCA and HMRC.

In the process several practices as referred to in our open letter to The Payments Association need to be brought to an end, such as Simplified Due Diligence being available on services to which there can be immediate or later add-ons – like the service's being issued with an IBAN – that serve to circumvent the service limitations that are the justification for the Due Diligence being Simplified.

Scope and definitions

3. Are (a) the definitions and (b) the scope of the regulated activities in the payments services and e-money framework clear and do they capture the right actors and activities within regulation?

The definition of an International Bank Account Number needs to be specific:

1. It must pertain to a bank account, not an eMoney account or a payment account at a non-bank;
2. Simplified Due Diligence must not be available for any payment service on which an IBAN is available;
3. An IBAN implies that normal Customer Due Diligence was carried out by the bank to which the IBAN, thanks to its composition, is identifiable, or Enhanced Due Diligence as the specific case requires;
4. There can be no difference between (i) the bank to which an IBAN is identifiable; and (ii) the bank acting as the Account Servicing PSP (or ASPSP) for whichever entity owns the account and uses the related IBAN.

4. Do the exclusions under the PSRs and the EMRs continue to be appropriate (includes limited network, electronic communication, commercial agent etc)?

No, they are not. They have been abused to create bank account functionality by the issuance of banking details (such as the IBAN) on a service that qualified for Simplified Due Diligence.

[7] https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper accessed on 26 February 2023

The regulatory treatment of payment services and eMoney

Considered against the government's objectives for payments regulation (paragraph 14), and referring to paragraph 20 in the government's accompanying review document:

5. How, if at all, might the framework for the authorisation of payment institutions and electronic money institutions be reformed?

These applicants should be required to line up an onshore safeguarding arrangement and operational accounts before authorization. There are two sets of operational accounts, one for the income and expense of the applicant itself, and one for the transit of customer funds, and these will need to be replicated for each currency.

6. How, if at all, might the framework for the registration of small payment institutions and small electronic money institutions be reformed?

There seems to be little point in persisting with the Small Payment Institutions regime, because they lack the resources to operate successfully, cannot get onshore banking arrangements and have a very limited potential for business volume given their need to pre-fund (as a result of FCA guidance on safeguarding). We cannot speak for Small eMIs.

7. How, if at all, might the registration requirements for account information service providers be reformed?

There needs to be an explicit and absolute ban on AISPs selling on customer statement data – whoever it is sold to, in aggregated or anonymized form or both or neither, and whatever safeguards supposedly exist. Customer statement data is circulating in a form that is plan, and neither aggregated nor anonymized. Once an AISP has sold customer data on once, they have no control over who it subsequently gets sold on to. Scammers, obtaining this information, can groom their victims, easily impersonating either the AISP or the ASPSPs. Consideration should be given to making it a criminal offence for all the directors of an AISP if it is found to have on-sold customer data.

8. Does the regulatory framework for payment initiation service providers (PISPs) and account information service providers (AISPs) sufficiently support the growth of this sector, and ensure a level playing field, and fair access to payment accounts, to support competition and growth?

It is already too generous, as explained above. PISPs and AISPs are thinly-capitalized, cannot reimburse customers from their own resources and fail to maintain an IT environment adequate to discharge their financial, legal and compliance obligations.

The contribution so far of the sector to competition and growth is suspect, hence our recent call to the Open Banking JROC to validate the OB statistics issued by the Open Banking ecosystem.

9. How, if at all, might the registration requirements or wider regime for agents be reformed?

Not answered.

Information requirements for payment services

Considered against the government's objectives for payments regulation:
10. Is the current framework for the provision of information to payment service users effective? If not, how should its scope change?

Not answered.

11. Are there particular changes that you would advocate to the Cross-border Payments Regulation in relation to the transparency of currency conversion, and what would these entail?

It was a mistake to abandon the parity of charges provisions in this Regulation, if the trouble was taken to keep the UK in the SEPA Area despite Brexit. This parity-of-charges is the main benefit for people and business in the UK from SEPA Area membership.

Rights and obligations in relation to the provision of payment services

Considered against the government's objectives for payments regulation:
12. What has been the experience of a) providers and b) users/customers in relation to the termination of payment services contracts? Does the existing framework strike an appropriate balance of rights and obligations between payment service users and payment service providers, including but not limited to a notice period applying in such cases?

Not answered.

13. With reference to paragraph 31 of the accompanying review, do stakeholders have any feedback on the government's view:

• that, as a general principle, a notice period and fair and open communication with a customer must apply before payment services are terminated?

Not answered.

• that the regulations and wider law operate here as set out under paragraph 29?

Not answered.

14. How and when do providers cease to do business with a user, and in what circumstances is a notice period not applied?

Not answered.

15. How effective are the current requirements in the Payment Services Regulations, notably under Regulations 51 and 71 – are these sufficiently clear or would they benefit from greater clarity, in particular to ensure that notice-periods are given and customer communication is clear and fair?

Not answered.

16. Should there be additional protections for payment service users against the termination of contracts? Should anything be specific to protect their freedom of expression – e.g. to ensure that adequate (or longer) notice is given in such cases, and what communication requirements should apply?

Not answered.

Wider considerations in relation to the provision of payment services

17. What provision, if any, should the regulatory framework make regarding charges for payment services?

Not answered.

18. Does the existing framework strike an appropriate balance of rights and obligations between:

• Sending and receiving payment service providers?

Not in the case of APPF. The receiving PSP is the one that has failed in its AML/CFT obligations by opening the payee account for the fraudster. The PSRs need to be altered – as per our response at 1B above – so as to make the payee name part of the payer's payment contract. This would have the knock-on effect of laying an obligation on the payee's PSP to check that the account identifiable through the Sort Code and Account Number (the 'Unique Identifier') carries the same naming as the payee contained in the payment.

The payee's PSP can then return the payment if the names do not match, or credit the payment if it believes they do or if it decides not to check at all. If the payee's PSP then makes a mistake and the funds go to a fraudster, the payee's PSP must reimburse the payer's PSP in full for its mistake, and the payer's PSP must reimburse the payer on the ground of 'defective execution': the payment as contracted was not executed correctly.

Of course there will need to be an agreement between payers' and payees' PSPs on the reimbursement – but the PSPs will be acting as often in one role as in the other, and it is all happening through a payment system of their own design anyway.

The major IT and operational change will be that the payee name will need to be processed and checked by the payee PSP in every case, with an option to return a mismatch, or to put it into a review queue and have an operator decide whether to credit it or return it.

UK credit transfer payment systems will then need also to implement the requisite messaging, the absence of which is a loophole in both RTGS Renewal and New Payments Architecture.

It is simply not fair on the PSU, though, that this major loophole should be allowed to persist, despite the investments going into the UK's credit transfer payment systems. The PSU's protection needs to be brought onto the same level as exists for cheques: if the payee's PSP allows a cheque to be paid into an account named differently to what is written on the payee line of the cheque, the payee's PSP bears the risk. In the case of APPF the payee account will be in a name concocted by a fraudster.

The payee's PSP has enabled the fraud by opening the payee account. It is only fair that the payee's PSP makes good the PSU damaged by their mistake. This would be enabled by the payee name becoming part of the 'payment contract' and by the elimination of the dispensation in Funds Transfer Regulation that the payment can be processed based on the 'Unique Identifier' alone.

• Account servicing payment service providers and payment initiation service providers/account information service providers?

See our views on PISPs/AISPs and APPF at 1B above. They need to take much greater responsibility for the volume of APPF in which they are involved.

19. Are consumers adequately protected from evolving fraud threats under the existing legislation – is further policy needed to ensure this, and how should that policy be framed?

No, thanks to APPF. The changes given in 1B above and summarized against Question 18 need to be implemented.

20. In relation to payment transactions which payment service providers suspect could be the result of fraud, is there a case for amending the execution times for payments to enable enhanced customer engagement? What requirements should apply here to ensure the risk to legitimate payments is minimised and that such delays only apply to high-risk, complex-to-resolve cases?

The problems would be solved by the solutions outlined above.

21. In relation to fraud, whether unauthorised or authorised, is there a need to a) complement rules with data sharing requirements; and b) for further reforms be made to make Strong Customer Authentication work more effectively and proportionately?

The problems would be solved by the solutions outlined above.

Issuance and redeemability of eMoney

Considered against the government's objectives for payments regulation:

22. Are the requirements regarding issuance and redemption of electronic money still appropriate?

Not answered.

Miscellaneous

23. Noting the intention to commission an independent review in due course, do you have any immediate observations on the efficacy of the operation of the Payment and Electronic Money Institutions Insolvency Regulations to date?

We have set out our views on the shortcomings of the current regime in 1B above:

1. Legal uncertainties of safeguarding as illustrated by the iPagoo case;
2. Inconsistent accounting of safeguarded funds by eMIs/PIs;
3. Safeguarded funds being in questionable banks and in locations with weak AML/CFT regimes;
4. The options of an insurance policy and of maintaining a pool of High-Quality Liquid Assets have proven to be cumbersome.

24. Finally, do you have any other observations relating to the payments framework not encompassed above, and how this could be further improved, in line with the government's objectives?

We would re-emphasize the following as subjects for detailed study and for potential consequential change to the payments framework:

1. The detriments caused by digitization – diminished access to services PSUs want, APPF, deductions-from-face-value and their contribution to general price inflation - as laid out in our paper on the plans for a UK central bank digital currency.
2. The statistics on the take-up and success of Open Banking as issued from within the Open Banking ecosystem;
3. The practices within the eMI/PI sectors that enable financial crime and which were outlined in our recent open letter to The Payments Association.

We would also respectfully draw your attention to our analysis of the two YouGov surveys commissioned by the Bank of England and HM Treasury in relation to the 'Britcoin' project and mentioned earlier.

This is relevant because the surveys exemplify points we made in response to Question 1A above, namely that what has happened in the UK is the fostering of digital means of payment at the expense of non-digital ones (cash, bank drafts and cheques) in a zero-sum game in terms of volumes of payments and in a questionable manner in terms of the distribution – between PSU and PSP – of the rewards, costs and risks:

- Lower costs for PSPs through the fostering of instant credit transfers via Faster Payments but a higher risk of fraud for PSUs (Authorized Push Payment Fraud or APPF);
- Higher revenues for PSPs in terms of deductions-from-face-value on card payments, which have achieved much higher market penetration, but with consequential increases in prices on all goods and services for people and businesses, a contributor to inflation.

The 'Britcoin' surveys for YouGov exaggerate the current take-up of digital/card/online/mobile means of payment, and customer satisfaction with them. The surveys suppress the detriments, or channel the discussion of the detriments so that they come over as less severe than they really are.

Our full analysis can be found at http://www.lyddonconsulting.com/analysis-of-the-yougov-surveys-commissioned-in-relation-to-the-britcoin-digital-pound-project/ and we have copied the overall summary below.

QUOTE

Both surveys are susceptible to the interpretation that UK SMEs and consumers are more open to and enthusiastic about digitization than is the case. There is a persistent tilting in favour of card payment methods and online/mobile payment methods, and against BACS, cheques and physical cash. This derives, inter alia, from the way the questions are structured, to terminology, to the way neutral and 'don't know' answers are treated, and to the absence of benchmarks for comparison where comparative questions are asked.

The detriments involved in online/mobile payments and card payments do not emerge clearly. The drafting of the questions and response options serve to suppress them.

Card payments nevertheless do not emerge favourably: they are convenient for consumers but their usage is not dominant across SMEs and consumers. They are not a preferred payment method for SMEs, either for paying away or receiving, although the reasons for this are not explored, and cannot be, given the questions and response options. There is a response option for SMEs about the cost of a card terminal, but there is no response option about the cost in the form of deductions-from-face-value. SMEs express a desire for payments to be cheaper and quicker, but this is an area where there is no 'compared to what?'.

Payment fraud is given intermittent attention, but its correlation to 'Online bank transfers' is not identified. SMEs appear barely concerned about it regarding payments in general, whilst it is a top concern when SMEs are making purchases online. Consumers are very concerned about it.

Cash, cheques and BACS – three payment methods that do not count as online/mobile/digital – are written out of the narrative as far as possible, for example by BACS not even being mentioned as a way in which SMEs make payments other than to staff.

By the same token Open Banking is not mentioned in either survey in any category, which is surprising if it has 7 million users as the Open Banking Implementation Entity recently claimed, albeit that the survey was carried out in February 2022.

It is also worth mentioning that the survey was carried out while UK interest rates were still very low, and before the crash in the prices of bitcoin, non-fungible tokens and other crypto assets. It would be interesting to see if the responses were the same now, as well as what results would emerge if (i) the response options were placed in a different order; and (ii) the drafting of both surveys were to be improved and expanded.

It will be vital also to see how the survey results are interpreted into the project for which the survey was commissioned: the Bank of England's 'Britcoin' Central Bank Digital Currency project, on which there is now a public consultation. This examination of the survey results was carried out before any study of the consultation documents: we prefer the bottom-up approach rather than just reading a high-level summary followed by intermediate summaries, in case the intermediate summaries are not supported by the base data, meaning that the high-level summary will not be supported either.

Our interpretation is that the results are in many ways irrelevant to the 'Britcoin' project and certainly do not make a compelling case for it.

UNQUOTE

R.J.Lyddon
9.3.23