Lyddon
CONSULTING

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

25th August 2023

Future of Payments Review,
Financial Services Group,
1st Floor,
HM Treasury,
1 Horse Guards Road,
SW1A 2HQ

Future of Payments Review – Response to Call for Input

Introduction

We note that the review has been asked to report on how payments are likely to be made in the future and the steps needed to successfully deliver world leading retail payments.

The payments industry has been trying answer these two questions without success for at least nine years, starting with the 'World Class Payments' project arranged by The Payments Council in 2014/5.

We attribute the failure of them and their successors – Pay.UK and UK Finance – and of authority bodies – the Bank of England, the Financial Conduct Authority, and the Payment Systems Regulator – to their attempting to answer two separate questions in reverse.

The above bodies, aided and abetted by self-interested organizations acting either through trade bodies or panels or advisory boards or subject-specific action groups, have answered the second question first, concentrating on the steps needed to deliver their own vision of 'world-leading retail payments' in which there are hundreds of digital payments companies on their journey from start-up to IPO and beyond, all gaining market share and revenues, and becoming an attractive investment for venture capitalists, share investors, pension funds and so on.

This has led to a payments eco-system that determines – in its own interests - how payments will be made as an outcome of its own economic interests. This outcome is now divorced from the wishes and needs of customers, and instead resides in the grip of vested interests pushing for the adoption of payment services on which they make money, and/or reduce their risks, or and/or reduce their costs.

This grip has been exercised through the multi-year pursuit of the same initiatives, as evidenced by this comparison table of World Class Payments, against Payment Strategy Forum, and against UK Finance's 'Future-ready payments 2030':[1]

- UK Finance's "Future-ready payments 2030: a dynamic, purposeful and united agenda for the UK", of February 2021;
- The Payment Strategy Forum's "A Payments Strategy for the 21st century: putting the needs of users first", of November 2016;
- Payments UK's "World Class Payments in the UK: enhancing the payments experience", of August 2105

How are payments likely to be made in future? In exactly the way that suits the payments industry, increasing its revenues, reducing its risks and diminishing its costs. The outcome counts as world-leading for the industry itself, but as costly, risky, and of low quality for customers.

[1] http://www.lyddonconsulting.com/comparison-table-of-uk-finance-report-future-ready-payments-2030-a-dynamic-purposeful-and-united-agenda-for-the-uk-february-2021/

Outcomes and detriments

The result has been the elbowing-out firstly of cheques and secondly of physical cash, to the benefit of 'digital' payment means. That has come with many detriments, which we will lay out, but its main outcome has been a major disconnect with the answer to the first question: what payment means would citizens and businesses choose to use if the choice was free, if many service options were available, and if the choice had not become weighted in favour of digital payment means thanks to the machinations and ministrations of the digital payments industry itself, and its control over all of the mechanisms and channels within which the future of payments is decided?

HM Treasury's own statement that this is all about 'boosting UK fintech competitiveness' is at the same time correct and a testament to the degree to which retail payments have left behind any pretence to serve customers as customers wish to be served, and have adopted a direction-of-travel in which the customer is disenfranchised.

Perhaps this review will be an opportunity to change and turn this direction-of-travel but the inclusion of a reference to fintech infers the opposite, and that this is an exercise to identify the measures needed to intensify and complete the damaging disenfranchisement of customers.

Who is fintech competing against actually?

HM Treasury's own statement 'boosting UK fintech competitiveness' raises the question of who UK fintech is meant to be competing against.

Are fintech companies meant to be competing against one another? If they are, why do they cooperate so closely with one another through trade bodies like Innovate Finance and The Payments Association? The scope and depth of that cooperation indicates a need for a Competition and Markets Authority investigation.

Are fintechs by definition not credit institutions (better known as banks), such that they are meant to be competing against banks? If that is the intention, how can it be the case when licences to act as an eMoney Institution, Payment Institution, Payment Initiation Payment Service Provider or Account Information Payment Service Provider preclude a vast majority of the activities that banks carry out?

Are UK fintechs meant to be competing against fintechs from other countries? How can that be, if the applicable licences preclude UK fintechs from serving customers in other countries and vice versa? Or is the form of competition some kind of meaningless beauty parade whereby the UK can claim to have more users of Open Banking than Germany has of Access2Accounts?

Or is it really that fintechs compete with the customer for control over the customer's well-being – their funds, the revenue potential of those funds, data on the customer's financial activities and data on the customer's wider life? Under this interpretation fintech is a parasite on UK citizens and businesses, adding no value to them and exploiting access to their money and data for their own benefit.

Which of these readings for fintech competitiveness is the one that HM Treasury wishes to boost?

Spurious legitimization for what has occurred

The issues, outcomes and detriments reflect a highly interwoven, self-referencing, and incestuous ecosystem. No one element is completely divorced from another. Shot through them is a line of spurious legitimization in the form of backing from policies, directives, frameworks, regulations or whatever handed down by global and EU bodies.

The EU regulations and directives are adhered to in spite of Brexit, with the notable exception of the Interchange Fee Regulations whose correct implementation would have cost the digital payments industry a lot of money, and which has thus had to be circumvented, at a huge cost to customers. The major elements are:

1. 4th AML Directive
2. Payment Services Directive 2
3. Funds Transfer Regulation
4. Interchange Fee Regulation
5. eMoney Directive

Further initiatives and practices derive from the outputs of global bodies:

1. The Financial Stability Board
2. The Bank for International Settlements
3. International Standards Organization, particularly ISO20022
4. The G-20 project on cross-border payments
5. The UN Sustainability Goals and definition of a Global Citizen

Thanks to Brexit and to the fact that the recommendations of global bodies are not mandatory, all this can be rowed back on.

Structure of our input

The structure of our input is aimed at demonstrating in detail what has gone wrong.

To that end we have reinterpreted the request for enlightenment on the most important consumer retail payment journeys both today and in the next 5 years into six figurative 'journeys' to a utility room in which the outcomes of the machinations and ministrations of the digital payments industry can be rinsed and cleansed from the current retail payment landscape, so that we can return to the status quo ante.

From that point the UK can begin again and with the needs and desires of the customer at the centre, not the needs and desires of the industry itself, and particularly not the fintech portion of the industry.

The Payment Systems Regulator was established to put the customer at the centre, but it has become an example of the most egregious 'regulatory capture' and may as well be closed down. All it seems to have achieved is to give the fintech industry a too-loud voice through the composition of the PSR Panel and then in the creation of the PSR's own Digital Payments Initiative. How much time, by contrast, has the PSR spent on considering the functioning of the Cheque&Credit Clearing System, which it is also charged with regulating?

Anyway, here are the six journeys to the utility room and the initiatives/issues to be cleansed by each one. You will find, if you compare these different streams, a significant crossover with our response to the Call for Evidence on the review of the 2017 Payment Services Regulations.[2]

There are also several references to a major paper we published in 2022 about the Bank of England's 'Britcoin' project, entitled 'Capture: Bigtech and Digital Payment Giants dominate the committees evaluating the replacement of physical cash with 'Britcoin' – a UK Central Bank Digital Currency'.[3] The paper is referred to in the footnotes as Lyddon, 'Capture'.

The footnotes contain links to articles in which I have explored in greater detail the particular issue that is referenced.

[2] http://www.lyddonconsulting.com/review-of-the-2017-payment-services-regulations-our-response-to-the-call-for-evidence/
[3] http://www.lyddonconsulting.com/capture-a-major-new-paper-on-the-committees-considering-a-uk-central-bank-digital-currency/

Question 1: What are the most important consumer retail payment journeys both today and in the next 5 years? For example, paying a friend, paying a bill, paying businesses for goods and services, in the UK or internationally etc.

First 'payment journey' to the utility room – reversing the attack on face-to-face banking

Attack on cash and burial of cheques

The attack on physical cash and the burial of cheques are well-known themes in UK retail payments.

Less known is the failure of alternative, digital payment means. These were examined in detail in Lyddon, 'Capture'.[4]

Attempts to protect access to cash have been arranged and mediated by the very people and organizations bent on its destruction, and the supposed protection afforded by the new Financial Services and Markets Act is disingenuous to say the least.[5]

Payment card issuers and payment card brands are the vanguard in the attack on cash.[6]

Then we have the 'frontrunners', the fellow travellers and the 'useful idiots.[7] 'Frontrunning' is a term for an organization that speciously attacks an existing service whilst pretending to be neutral and disinterested, whilst at the same time creating a marketplace for its own, substitute service.

National and international 'authorities' number amongst the fellow travellers.[8]

A supposedly humanitarian aim of increasing the flow of migrant remittances has been a favoured hobby horse of the anti-cash lobby, not that they have succeeded in delivering superior services.[9] At the same time it has been possible to build the perception of a strong connection between using cash and financial crime – all part of the strategy of dissing cash.

In that same direction we had the ultimate 'canard', that physical cash was responsible for the spread of COVID-19.[10] This was an unscrupulous rumour that the anti-cash lobby put about, but then, in their fervour of eliminate non-digital payment services, it is all grist to the mill.

Closure of branches and ATMs

There is a night-and-day contrast between:

- Expressed desires to protect access to cash and to face-to-face banking; and
- The actual rundown of access to such services.

We can quote a LinkedIn blog by Ron Delnevo, Chair of the Payment Choice Alliance:[11]

QUOTE

"Independent Access to Cash Review

In July 2018 LINK commissioned Natalie Ceeney CBE to chair a new, independent Review to look at the impact of the shift from cash to digital payments…"

---

[4] http://www.lyddonconsulting.com/digital-payment-failures-we-need-a-viable-face-to-face-banking-model/
[5] http://www.lyddonconsulting.com/digital-payment-failures-failed-access-to-cash/
[6] http://www.lyddonconsulting.com/the-anti-cash-lobby-principals/
[7] http://www.lyddonconsulting.com/the-anti-cash-lobby-frontrunners-fellow-travellers-or-useful-idiots-2/
[8] http://www.lyddonconsulting.com/the-anti-cash-lobby-national-or-international-authorities-as-fellow-travellers/
[9] http://www.lyddonconsulting.com/the-anti-cash-lobby-migrant-remittances/
[10] http://www.lyddonconsulting.com/the-anti-cash-lobby-migrant-remittances-and-covid-19/
[11] https://www.linkedin.com/feed/update/urn:li:activity:7099944497244971008/?commentUrn=urn%3Ali%3Acomment%3A(activity%3A7099944497244971008%2C7100041742921388032)&dashCommentUrn=urn%3Ali%3Afsd_comment%3A(7100041742921388032%2Curn%3Ali%3Aactivity%3A7099944497244971008)&dashReplyUrn=urn%3Ali%3Afsd_comment%3A(7100322936791674880%2Curn%3Ali%3Aactivity%3A7099944497244971008)&replyUrn=urn%3Ali%3Acomment%3A(activity%3A7099944497244971008%2C7100322936791674880) accessed on 24 August 2023

THAT WAS 5 YEARS AGO.

So what positive news have we had since then for the 90% plus of UK adults (YouGov June 2023) who continue to use cash?

Well, at the start of 2018, the year Nat began her work, the UK had more free-to-use ATMs than ever. 54,599 free-to-use ATMs, to be precise.

Five years later, at the start of 2023, there were only 39,429 free-to-use ATMs left in the UK. That's a fall of 28%.

NOT exactly positive news then for the 90% plus of adults - that's over 50 million, by the way - who continue to use cash

In the same period, the UK lost well over 4000 bank branches, meaning that nearly 50% were closed in 5 years. The vast majority of those branches provided over-the-counter cash withdrawal and deposit facilities.

NOT exactly positive news then for the 90% plus of adults - that's over 50 million, by the way - who continue to use cash.

Last week, HM Treasury announced that "the vast majority" of the British public would have some access to cash, within a mile in urban areas or three miles in rural areas.

Not to a free-to-use 24-hour ATM though - there is no mention at all of ATMs in the HM Treasury statement.

The access to cash "promised" can be over a limited-hours post office counter or via cash-back at a shop, though of course there is no guarantee that the shop will actually have cash to give you, even if it is open when you get there. You certainly will NOT get the £250 you could have taken from one of those fast-disappearing ATMs.

NOT exactly positive news then for the 90% plus of adults - that's over 50 million, by the way - who continue to use cash.

What else? Oh, yes. "Bank Hubs". Not Community Banks, which they were meant to be, but at least "something"… So to offset a loss of 4000 plus bank branches with counter cash services, how many "Bank Hubs" are now open, well over two years since the first one appeared in Rochford in Essex? SEVEN.

NOT exactly positive news then for the 90% plus of adults – that's over 50 million, by the way - who continue to use cash.

So after 5 long years, what IS the positive news then for EVERYONE who wants to continue to use cash - that's over 50 million people, by the way?

UNQUOTE

Hobbling of cheques by withdrawal of facilities for using them

These measures have made the usage of cheques inconvenient and impractical – all part of the digitization agenda. The two detriments aggravated by this are:

- Payees receive the full amount of a cheque, unlike a card payment, on which they receive the amount less the deductions-from-face value; and
- The payer is protected from 'conversion' – if the bank permits the cheque to be credited to a different party than the one named on the payee line, the bank is liable, unlike Authorized Push Payment Fraud, where the payee name is not part of the payment contract.

The measures to hobble cheques include:

- Withdrawal of the cheque guarantee card;
- Cancellation of the automatic re-issuance of cheque books;
- Difficulty in obtaining a paying-in book;
- No bank service to pick up cheques in bulk from a payee's premises;
- Closure of bulk deposit facilities in banking centres;
- Cheque image deposit services that allow only one cheque to be deposited at a time.

Undermining of LINK/poor scope and service of Banking Hubs

LINK has been undermined by its owners and is no longer a viable part of any solution for access to cash.[12] Knowing this, the banks position LINK as a major component of Banking Hubs, ensuring their eventual failure.

The service scope and level of Banking Hubs has been specified by the banks themselves, without a benchmarking against either:

- What service scope and level would have been supported by the branch of a major bank 10 years ago, before the erosion began; or
- What service scope and level meets the wishes and needs of the community in which the Banking Hub is to be established.

Instead it is left to the banks, along with LINK and possibly the Post Office, to specify the service scope and level, and of course these are specified not only without reference to the wishes and needs of the community, but also on a deliberately *de minimis* level. The service is therefore unattractive, does not entice customers to it, and can, in a year or two with much feigned sorrow and regret, be concluded to have failed and be closed down. It is farcical that those institutions determined to kill off face-to-face banking have been allowed to play such a large role in determining the shape of face-to-face banking over the next two or three years, up to the point where they can conclude that it can be killed off completely.

Loopholes left in latest Financial Services & Markets Act

The protection for cash in the latest legislation is so low that its effect will be to accelerate its killing-off.[13]

Access to Cash – Quick-Fix Solution

There is a way of protecting Access to Cash in the short term, and here it is:[14]

QUOTE

Appendix 6 - Access to Cash – Quick-Fix Solution

Background

Access to Cash is threatened by banks' closure of branches and consequent closure of their ATMs. The Payment Systems Regulator has undertaken 'work' in this area, there has been an 'Access to Cash' report, and the solution has been deemed to be within so-called 'banking hubs', physical locations run by The Post Office in which customers can undertake cash transactions with any one of the ten main UK financials services groups. According to an article in The Daily Telegraph, too few of these hubs have been established, and there is a long lead-time and many obstacles.[15] One could add that there has been no benchmarking of a 'banking hub' to the service range and service level of a physical location that supports the usage of cash to a viable level, and to the transacting of other services – like cheques – that are not on the agenda at all. This is important, especially for merchants, in that cash and cheque are two payment means under which the merchant receives the full face value of the sales they make.

[12] Lyddon, 'Capture', pp. 101-4 'Appendix 8 - how LINK has become unviable'
[13] http://www.lyddonconsulting.com/promised-legal-protection-for-cash-is-a-further-nail-in-its-coffin/
[14] Lyddon, 'Capture', p. 99
[15] 'How the botched banking hub rollout left people struggling for cash', published on 12th September 2022 by Patrick Mulholland

Now LINK – the payment scheme for the withdrawal of cash through ATMs – and the chair of the PSR's Access to Cash work[16] are saying that more needs to be done, although it is only months since the Access to Cash work was completed.

There has been no recognition that the major banks have been allowed to have their cake and eat it: they are the major issuers of the cards that are used in ATMs, they have reduced their own numbers of ATMs, so they now are more in the position of seeing their customers use cards in the ATMs of others. This leads the bank to have to pay the LINK interchange fee, which remunerates the operator of the ATM from which the withdrawal was made. At the same time the same banks have used their dominance in the ownership of LINK to reduce that interchange fee. On 4th September The Daily Telegraph reported that the fee is 26.5p for ATMs in a location where there is another free-to-use ATM less than 1km away, and 29.3p where the ATM is 'protected', meaning there is no other free-to-use ATM within 1km. Only 6.3% of UK ATMS are 'protected'.

Solution

The current interchange fees need to be scrapped and a banding arrangement applied. The banding will result in a variation of the interchange fee – higher or lower – around a base of 30p per transaction based on the card issuer: the issuer will fall into one of nine bands, and the appropriate interchange fee will be charged to that issuer for all instances where a card issued by them has been used to make an ATM withdrawal at an ATM not operated by the card issuer. The Payment Systems Regulator, as an economic regulator, should be capable of working out the detail, and of imposing it, since LINK is one of the payment systems it regulates. Nevertheless, key factors that will go into the banding will be:

Number of ATM-eligible cards in issuance	Trend over 10 years	Number of LINK-connected ATMs operated	Trend over 10 years	Number of branches operated	Trend over 10 years

An example outcome would be:

Band	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Variation	-70%	-35%	-15%	-5%	0%	+5%	+15%	+35%	+70%
Fee	9.0p	19.5p	25.5p	28.5p	30.0p	31.5p	34.5p	40.5p	51.0p

Outcome

The major banks will pay more to take account of their dominant market share of cards in issuance. A particular surcharge will fall on those banks who have closed branches and ATMs over the last 10 years: they have had their cake and eaten it. The new arrangement will result in more interchange fees being paid into LINK than now, because the bigger banks have both more cards in issuance and will be subject to a surcharge. This money can be passed to independent ATM operators, and all ATMs can be free-to-use.

UNQUOTE

Access to Cash – Long-Term Solution

The pathway to protecting Access to Cash and indeed full-service, face-to-face banking is this one:[17]

QUOTE

Appendix 7 - Access to Cash – Long-Term Solution

Background

The Quick-Fix to Access to Cash – the change in the interchange fee to a banded one – should ensure the continuation of the UK's network of free-to-use ATMs for a reasonable period so as to enable a new blueprint for banking provision to be designed and implemented. The first step in that is not a piecemeal focus on just one payment means, but (i) on the series of payment means that used to be transacted in bank branches in the normal course of business; and (ii) other services that were offered in bank branches in the normal course of business. It will be necessary to draw up a specification of the scope of the service to be offered, the level of service to be offered, the timings and the price.
The benchmark will be a full-service branch in 2012, before the major banks embarked on their campaign of reductions in service scope, service level and performance that has undermined the branch concept and enabled the banks to push

[16] Natalie Keeney CBE
[17] Lyddon, 'Capture', p. 100

customers onto their range of more lucrative services (lower costs, higher income, lower risk – all seen from the banks' point of view). The success of the banks' campaigns of undermining the in-branch offering is played back by the banks as the banks responding to customer demand. This is disingenuous and needs to be called out: customer behaviour has altered thanks to banks' policies, which are determined by considerations of returns, risks and costs. No survey was ever taken with open questions about customer desires and requirements.

Solution

The solutions proposed for Quick-Fix to Access to Cash, for Authorised Push Payment Fraud, and for Deductions-from-face-value on card transactions will, in sum, substantially alter the returns, risks and costs for banks in UK retail banking. Banks will take the 'payee name' risk that they ought to take as a matter of principle and did take when cheques were involved. Banks will suffer costs from branch and ATM closures where they continue to issue large numbers of cards but have reduced the estate of their ATMs out of which their customers can draw cash with their cards. Banks will give up the false subsidy they enjoy where, together with their allies the major card brands, they impose deductions on merchants which are passed on in the form of higher prices for goods and services and which are inflationary.

Those solutions will take some time to implement and to filter through. While that is occurring – and it could be 2-3 years – the solution to in-person banking can be worked out. It may include banking hubs, or it may not. But for sure it will be designed (i) with the needs of wider society at the forefront; and (ii) against a backdrop where banks' business cases for the one or other development are not distorted as they are now by their being able to palm off risk onto their customer, by the large income streams available from the cards business which are little more than an unfettered ability to draw money out of wider society, and/or by their ability to cut costs whatever the impact on wider society.

The Payment Systems Regulator (PSR)

It is worth noting that the PSR was established around 2014 to represent the wants and needs of wider society against entrenched vested interests in the payments industry. It is a measure of the PSR's failure that we have arrived where we are now, eight years on, with vested interests as much in control as ever. Indeed one might argue that the major liberalization of the payments business overseen by the PSR – easier access to payment systems – has resulted in a huge expansion of the number of actors in the Visa and Mastercard ecosystems and a consequent increase in the market power of the cards duopoly. The PSR recently, in its response to the report of the Digital Payments Initiative, declared that it viewed the adoption of digital payment means as part of its own remit. To that extent it appears to have become completely captured by the Visa and Mastercard agenda.

UNQUOTE

Second 'payment journey' to the utility room – reversing and rebalancing the favouritism in favour of digital payment means extended by authorities who ought to be impartial

Bias of the FCA/Payment Systems Regulator (PSR) in favour of digital

The FCA has permitted numerous non-compliant practices to persist in the digital payments world – these have a 'payment journey' of their own and include Virtual IBANs and 'nesting'.

The PSR has permitted the Cheque&Credit Clearing System to wither on the vine, focusing its attention instead on BACS and Faster Payments. It has at the same time permitted Visa and Mastercard not to split their scheme management from their infrastructure, a form of built-in subsidy for these two payment systems, alleviating them of a source of extra administration and cost.

The PSR permitted Mastercard to acquire Vocalink, which provides the infrastructure for three of Mastercard's competitor systems – BACS, Faster Payments and LINK.

The PSR appoints its PSR Panel to advise it from the digital world.[18] It sets up its Digital Payments Initiative as a supposed sub-committee of the PSR Panel, but then co-opts onto it further representatives of the digital world.[19]

The PSR issued a response to its own creature's report – the initial report of the Digital Payments Initiative - perpetuating the illusion that the creature has a life of its own: the PSR Panel and the Digital Payments Initiative are marionettes of the PSR.

In point 1.5 of the Executive Summary on p. 3 of the response, the PSR made an extraordinary statement:[20] 'Removing barriers to new digital payment services, to better meet people's needs, is part of our remit.' The PSR is an **economic** regulator of payment **systems**: it has no brief to steer what payment **services** end-users decide to use or not use.

It is supposed to act impartially towards the payment systems that fall within its remit. It is supposed to represent the voice of end-users, which entails standing up for end-users' right to have a choice of payment means. It has failed and is instead a mouthpiece for the digital payments world.

Britcoin will be distributed using the Visa/Mastercard market model

'Britcoin' – the digital pound – will not give retail access to central bank money if there are either deductions-from-face-value or a settlement delay.[21] Both those detriments are part-and-parcel of card payments now.

It is obvious that the Bank of England envisages a distribution model for the digital pound that is identical to the Visa/Mastercard model, and which by implication will involve deductions-from-face-value by financial intermediaries in a way that does not occur with payments made by means of physical cash.[22]

The 'Technology Working Paper' that accompanied consultation on the digital pound contained very little about technology.[23]

The consultation itself overlooked the results of the project's own YouGov survey, which showed very little appetite for digital payments beyond what has been in use for some years, and a reluctance amongst businesses to use card payments (due to deductions-from-face-value).[24]

[18] Lyddon, 'Capture', pp. 31-3
[19] Lyddon, 'Capture', pp. 34-5
[20] psr-response-to-digital-payments-initiative.pdf available through www.psr.org.uk
[21] http://www.lyddonconsulting.com/digital-pound-will-not-be-central-bank-money-if-there-are-deductions-or-a-settlement-delay/
[22] http://www.lyddonconsulting.com/bank-of-england-consultation-on-the-digital-pound/
[23] http://www.lyddonconsulting.com/technology-working-paper-accompanying-the-bank-of-england-consultation-paper-on-the-digital-pound/
[24] http://www.lyddonconsulting.com/analysis-of-yougov-surveys-commissioned-by-the-bank-of-england-in-connection-with-its-digital-pound-project/

The level of support for the digital pound that can be garnered from the parallel investigations by other central and by the central banks' own bank (The Bank for International Settlements) has fallen.[25]

Undismayed the Bank of England and HM Treasury proceed into the next phase of their 'work' on the digital pound, now saying it is needed for the purposes of innovation.[26] This smacks of desperation, casting around for a new excuse to go ahead with what you wanted to pursue anyway, which is to eliminate physical cash and have all payments made by digital means.

High deductions-from-face-value on card payments in defiance of the Interchange Fee Regulation – an unfair leg-up for digital payment means

Merchants who make sales of goods and services where payment is by card (including contactless and cardholder-not-present) suffer a deduction of fees from their sales proceeds that is commonly estimated at 3%.[27]

Based on our knowledge it ranges from 1%-8%, depending upon the market power of the merchant (who can negotiate a large fee rebate) and the type of card (8% would apply to a Premium card accepted by a merchant with too little market power to negotiate a rebate).

With the major recent moves in payment means from cash to card, from cheques to card, and from in-person to online shopping, the volume and value of payments subject to deductions-from-face-value has risen inexorably, and so have the deductions: the fees swallowed by the payments industry from undertaking a simple process.

The digital payments industry has become a parasite on the UK economy, swallowing 3% x (portion of GDP transacted by card payment/GDP), in exchange for a core and basic service, and one little changed over the last 40 years. This is a cash cow for the UK financial services industry, and such a large one that it has resulted in the industry de-banking all types of geographies in the UKs and all types of supposedly 'higher-risk' customers, and in the industry failing to deliver genuine innovation: it is surprising how many Fintech businesses come down to the issuance of a Visa- or Mastercard-branded payment card.

The PSR – supposedly an economic regulator – has presided over a colossal economic dislocation in the industry it is meant to be regulating.

Here is our solution to this problem, and it is not original. It is the proper implementation of the Interchange Fee Regulation:[28]

QUOTE

Appendix 5 – solution to Deductions-from-face-value on card transactions (Deductions)

Background

Merchants do not receive the full face value of the sales they make when payment is by card. They receive, through their merchant acquirer and some days later, an amount that is the sale value diminished by several lines of fees. The fees are not limited to the 'interchange fee', an element whose size is capped by the EU Interchange Fee Regulation 2015/751 of 29th April 2015 (the IFR). The IFR caps the interchange fee at 0.2% for debit card transactions and 0.3% for credit card transactions. The deductions experienced by merchants are normally in a range between 3-8% with a minimum deduction in a range of £0.35-0.70. The aim of the IFR was to avoid (i) the false subsidy enjoyed by card payment actors due to their fees not being transparent and negotiable; and (ii) the inflationary effect of the deductions whereby merchants increase the price of goods and services to all buyers in order to recoup the fees the merchants suffer when some of their buyers pay by card; and (iii) benefits being made available to cardholders by their card issuers that are paid for by merchants and higher prices for all.

[25] http://www.lyddonconsulting.com/central-banks-should-be-wobbling-in-their-drive-towards-central-bank-digital-currencies/
[26] https://www.bankofengland.co.uk/quarterly-bulletin/2023/2023/enabling-innovation-through-a-digital-pound
[27] http://www.lyddonconsulting.com/digital-payment-failures-fraud-and-card-deductions/
[28] Lyddon, 'Capture', p. 98

Solution

The UK should re-issue the IFR in line with the intentions of the original, namely that the merchant's acquirer must receive – and must pay on to the merchant - 99.8% of the sale value when a debit card is accepted, and 99.7% when a credit card is accepted. No other fees or deductions will be routed through the merchant acquirer by any other market actors like card issuers or card schemes. The merchant acquirer will be allowed to charge service fees to the merchant, the costs of which will solely be a matter between the merchant and the acquirer and not involving the card schemes or card issuers. The deduction of 0.2/0.3% and these service fees will be the total cost for merchants of accepting payment by card.

The further benefits for merchants promised by the IFR need also to be realised: (i) granular presentation of fee levels on different categories and brands of card (Article 9); (ii) ability not accept particular cards at a granular level (Article 10); (iii) receipt of comprehensive information on each transaction in a timely manner so as to enable internal financial processes (Article 12).

The PSR must (i) undertake the annual process to ensure compliance with the interchange fee caps (Article 3.5); (ii) compel Mastercard and Visa to separate their scheme management from their infrastructure, in the way LINK, BACS and Faster Payments have had to (Article 7).

Outcome
The false subsidy enjoyed by card payments will cease. Card payments will have to compete on a level playing field with cash, cheques, direct debits and credit transfers. Merchants will be able to reduce prices for goods and services as they will no longer have to factor in the large deductions on card payments. Benefits made available by card issuers to holders of their cards will have to be funded by the card issuer itself and not by wider society.

UNQUOTE

PSR focus on any aspect of the payment cards market except deductions-from-face-value

It is noteworthy that the PSR has conducted several streams of 'work' connected to payment cards and the costs for merchants of accepting them.[29] These include the clarity of pricelists for payment terminals, and the comparability of pricing of payment terminal services proposed by different vendors.

There has been no workstream on deductions-from-face-value, the biggest and most onerous component of cost for a merchant in accepting payment cards.

For a supposed 'economic regulator' to turn a blind eye to this issue is bizarre to say the least, but then the digital payments industry must be protected and encouraged, even at the price of a major detriment to merchants, which is passed on to consumers in the form of higher prices and inflation.

Authorised Push Payment Fraud – unfairly transfers 'conversion risk' to the customer, making credit transfers both cheaper and less risky for banks

Authorised Push Payment Fraud is another gift of the digital payments industry to UK individuals and businesses.[30] Where one pays by cheque, the bank must cause the cheque to be deposited into an account named as per what is in the payee line of the cheque, whilst with a credit transfer the bank can credit based on the Sort Code and Account Number alone, and ignore the payee name.

We have written at length about it and into various public processes, for example our response to the PSR's consultation 21/10.[31]

[29] http://www.lyddonconsulting.com/the-payment-systems-regulators-ps22-2-card-acquiring-market-remedies-final-decision-surrender/
[30] http://www.lyddonconsulting.com/digital-payment-failures-fraud-and-card-deductions/
[31] http://www.lyddonconsulting.com/our-response-to-the-psr-consultation-cp21-10-on-app-scams/

In this area the PSR has demonstrated favouritism to one segment of the digital payments industry – card payments – to the detriment of another – credit transfers, albeit that the loser is always the customer. The elevated risk of using credit transfers dissuades customers from migrating to them, keeps the volumes of card payments high, protects the fees taken by the card payments segment in the form of deductions-from-face-value, and insulates the card payments segment from a give-up of revenues if volumes migrated to card payments.

The UK payments market model that delivers such high revenues on card payments is protected by the PSR's both accepting the mantle of the organization that will solve Authorised Push Payment Fraud and then failing to do so, over a 7-8 year period.

The exasperating thing is that there are two simple legal changes that could be made which would make the payee name part of the payment contract and compel checking of the payee name. Whilst this might not completely eliminate payment scams, it would mean that an overwhelming proportion of cases that now count as 'Authorised Push Payment Fraud' would become 'Unauthorized', because the banks will have contrived to pay a payee different from the one named in the payment contract. In consequence the customer would have the automatic protection under the 2017 Payment Services Regulations for an unauthorized payment.

So simple, yet the PSR has repeatedly turned its face against resolving Authorised Push Payment Fraud at its root, and chosen instead firstly a Fintech solution to try and resolve a problem caused by Fintech, and then a leaky reimbursement scheme.

Here is the outline of the solution to Authorised Push Payment Fraud that we have proposed multiple times:[32]

QUOTE

Appendix 4 – solution to Authorised Push Payment Fraud (APPF)

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.

[32] Lyddon, 'Capture', p. 97

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

CoP- Confirmation of Payee

Instead of solving Authorised Push Payment Fraud at its root, the PSR has chosen a Fintech solution to try and resolve a problem caused by Fintech. This is called Confirmation of Payee or CoP and already featured in the World Class Payments Report in 2015.[33]

It is accepted seemingly as normal business for payers to have to confirm their payment orders to their payment service providers, rather than for payment service providers – who construct and choose the payment systems through which customers' payments are made – to make sure they pay the correct payee or return the money.

Instead the customer has to undertake extra work, and in doing so to accept extra responsibilities.[34] This is unfair and an unwarranted transfer of banking work onto customers, reducing the workload and the costs of the payments industry, and its risks, and lumping them both onto the customer.

CoP is not even properly supported in the payment system (Faster Payments) through which most fraud is transacted.[35]

Two major defects in CoP remain:

1. The customer's degree of protection when CoP returns an approximate match, neither a 'Thumbs-Up' nor a 'Thumbs-Down';
2. The customer's lack of legal records of when they applied for a CoP against a particular name, Sort Code and Account Number, and what the outcome was: only the payment service provider has those records.

The CReM – Contingent Reimbursement Model

The PSR also arranged for a reimbursement scheme for customers who have become victims of Authorised Push Payment Fraud, but it was contingent on the customer having used CoP and obtaining a 'Thumbs-Up' result. This is why it is called the Contingent Reimbursement Model or CReM.

Needless to say the CReM has not led to the full reimbursement of all claims for Authorised Push Payment Fraud. The PSR's response has been to extend the number of payment service providers that are part of it, to the extent that they now intend to make CoP and CReM mandatory.

[33] http://www.lyddonconsulting.com/what-we-learned-about-pay-uks-confirmation-of-payee-service/
[34] http://www.lyddonconsulting.com/lyddon-consulting-submissions-to-the-treasury-select-commitee-on-confirmation-of-payee-and-app-fraud/
[35] http://www.lyddonconsulting.com/the-uks-new-payment-system-operator-makes-a-world-class-cop-out-on-confirmation-of-payee/

We recently had the opportunity of commenting on a letter sent by The Payments Association to a member of the House of Lords criticising the extension of the membership of the CReM.[36]

We responded to the PSR's consultation on the CReM.[37]

We made a presentation on the CReM to a trade body called Vendorcom.[38]

We responded to a Treasury Select Committee consultation.[39]

We published a series of blogs when the CReM was first unveiled, showing up its shortcomings:

- The CReM excludes half of victims, ameliorates the financial firms' position vis a vis the rest, does not cause financial firms to make legally binding contractual commitments, throws sand in the eyes of customers regarding their baseline rights in law, limits firms' financial commitment to only 7 months' of claims, and then allows firms to place the entire financial burden onto all their customers;[40]
- No coverage under the CReM for where the fraudsters gull a person's eBanking credentials from them and use the credentials to make push payments from the victim's account to their own;[41]
- Fails to address the root of the problem;[42]
- Allows the payee payment service provider to persist with not checking that the payee name in the payment is consistent with the name on the account associated with the Sort Code and Account Number in the payment;[43]
- Limited number of payment service providers covered by the CReM initially and the dependency upon customers having used CoP and got a 'Thumbs-Up';[44]
- Customers' baseline rights are overridden;[45]
- Customers are expected to do bank-like work and to do it instead of payment service providers doing it;[46]
- Low standards required of payment service providers.[47]

The PSR lamentably failed to press a simple point: if payment service providers can operate CoP, why cannot they do the same on every payment? That, in essence, is our solution and it is a core and basic validation step in payment processing. Unfortunately the model on which all of the UK's credit transfers operate misses out this core and basic step, and the customer is the loser.

The CReM, and CoP have not solved Authorised Push Payment Fraud and will never do so at its root. That is why our proposal is inherently superior.

The question remains why the PSR has for 7-8 years espoused the Fintech world's preferred solution to a problem of the Fintech world's creation, and why the PSR has espoused a 'chocolate fireguard' scheme like the CReM…and all the time the deductions-from-face-value on card payments keep rolling in.

---

[36] http://www.lyddonconsulting.com/commentary-on-the-payments-associations-letter-to-lord-johnson-about-the-proposed-widening-of-the-coverage-for-victims-of-authorised-push-payment-fraud-appf/
[37] http://www.lyddonconsulting.com/our-response-to-the-psr-consultation-on-their-contingent-reimbursement-model-draft-code-aimed-at-authorised-push-payments-fraud/
[38] http://www.lyddonconsulting.com/presentation-to-vendorcom-special-interest-group-on-faster-payments-about-authorised-push-payments-fraud/
[39] http://www.lyddonconsulting.com/lyddon-consulting-submissions-to-the-treasury-select-commitee-on-confirmation-of-payee-and-app-fraud/
[40] http://www.lyddonconsulting.com/crummy-crm-code-offers-no-comfort-to-uk-payment-fraud-victims-part-1/
[41] http://www.lyddonconsulting.com/crummy-crem-code-part-ii-bizarre-choice-of-types-of-fraud-it-covers/
[42] http://www.lyddonconsulting.com/crummy-crem-code-part-iii-root-cause-of-wrong-name-appf-and-customers-current-legal-protection/
[43] http://www.lyddonconsulting.com/crummy-crem-code-part-iv-ensuring-that-the-mandatory-data-is-validated-at-the-beneficiary-firm/
[44] http://www.lyddonconsulting.com/crummy-crem-code-part-v-types-of-customer-covered-firms-offering-cover-and-dependency-upon-confirmation-of-payee/
[45] http://www.lyddonconsulting.com/crummy-crem-code-part-vi-as-customers-baseline-rights-are-overridden/
[46] http://www.lyddonconsulting.com/crummy-crem-code-part-vii-and-customers-added-responsibilities/
[47] http://www.lyddonconsulting.com/crummy-crem-code-part-viii-and-the-low-standards-for-firms-to-meet/

Third 'payment journey' to the utility room – collapsing detrimental projects

Bank of England's new CHAPS system after the fallover in 2014 – 9-year project called 'RTGS Renewal' – uses the EU's ISO20022 XML data format – fell over on 14th August 2023 a few weeks after go-live[48]

It is a disgrace that this system fell over again only a few weeks after the switchover to ISO20022 XML in June this year.[49] This is after a 9-year project misdiagnosed the cause of the 2014 fallover, permitting the adherents of ISO20022 XML to position it as a solution. It clearly was not, so the project now needs to be frozen with no new steps taken. Yet another review needs to take place, of the new architecture of CHAPS and its components after 'RTGS Renewal', and a new pathway forward plotted, without ISO20022 XML.

'Trusted KYC Data Sharing' – financial institutions sharing the black marks they have put against individuals and businesses with every other financial institution, to ensure systemic de-banking

This PSR project needs to be abandoned. Banks and payment service providers are not up to being entrusted with this level of power and the ability to transmit a system-wide black mark that was originally put incompetently against a legitimate market actor.[50]

New Payments Architecture – will combine BACS and Faster Payments using the EU's ISO20022 XML data format – but it won't solve Authorised Push Payment Fraud

The Pay.UK New Payments Architecture project – derivative of the PSR's Payment Strategy Forum – will achieve little more than move Faster Payments and BACS onto ISO20022 XML, a move bringing no immediate business benefits to customers.[51] Indeed it may not even be this good because the major beneficiary will be Mastercard, by dint of its being the infrastructure provider through its Vocalink subsidiary. It is a national scandal that Mastercard has managed to retain its position as a regulated payment scheme – and one exempted for some reason from divorcing its scheme management from its infrastructure – at the same time as having and consolidating a lock over the infrastructure provision to three competitors of the Mastercard scheme – Faster Payments, BACS and – ludicrously of all – LINK. Mastercard has a strong vested interest in the decline of LINK and the increased usage of payment cards instead of cash, so it is major regulatory failure that it continues to be permitted to supply the infrastructure for LINK.

Pay.UK is charged with delivering NPA, but this organization has had the NPA blueprints since 2017 and still nothing has been delivered.[52] Pay.UK has a big hand in anything to do with ISO20022 XML but even that degree of influence has not resulted in new messages to be used in NPA that are better than the old ones. The new messages are like-for-like with the old ones and will exchanged under the existing scheme rules. This means that the payee bank will still not check that the payee name is coherent with the name on the account identified by the Sort Code and Account Number in the payment. In other words NPA will do nothing to solve Authorised Push Payment Fraud.

This is also a national scandal – that the payment system through which this fraud occurs is subjected to a multi-year and multi-multi-million-pound renewal but the possibility of fraud is not eliminated as a Day 1 deliverable.

Open Banking – derivative of EU Payment Services Directive - who is using it? HMRC, and ???

Open Banking claims to have over 7 million 'active users' or 7 million users 'benefitting' from it. This might be different from individuals and businesses who have knowingly subscribed to a service based on Open Banking and are fully aware of what happens behind the scenes. The most convincing case of Open Banking is Intuit QuickBooks: a business appoints Intuit to access statements from its banks so that Intuit can carry out such tasks as accounting, reporting, cash application and so on.

---

[48] https://globalbritain.co.uk/the-illusion-of-uk-financial-stability-why-the-new-bank-of-england-payment-system-fell-over-just-like-the-old-one/ accessed on 22 August 2023
[49] https://globalbritain.co.uk/the-illusion-of-uk-financial-stability-why-the-new-bank-of-england-payment-system-fell-over-just-like-the-old-one/ accessed on 22 August 2023
[50] http://www.lyddonconsulting.com/faragegate-shows-the-trusted-kyc-data-sharing-project-must-be-stopped/
[51] http://www.lyddonconsulting.com/uks-new-payments-architecture-now-to-be-a-bungalow/
[52] http://www.lyddonconsulting.com/what-we-learned-about-the-uks-new-payments-architecture/

At the other end of the spectrum is HMRC adding credit transfers as a payment option for the tax obligations of individuals and businesses. In order to enable that the individual or business is caused to sign up with an Open Banking provider, without knowing that Open Banking is behind it and without using that provider for any other service than its (at most) twice-a-year payments to HMRC. Given that there are upwards of 100 million entities of all types that are liable for tax, 4% of them signing up for the HMRC service would contribute over half of the total of 7 million that Open Banking claims are 'active users' and/or 'benefitting' from Open Banking.

Open Banking – permitted to mark its own homework, big up its statistics, and be falsely endorsed by the PSR and the PSR's Digital Payments Initiative

Open Banking's statistics about its own success are flawed and in need of a diligent sanity check.[53]

Open Banking was falsely endorsed by the PSR's Digital Payments Initiative as the channel through which its own work should be taken forward.[54] The PSR permitted itself to establish the Digital Payments Initiative, ludicrously, as part of its workstream on Access to Cash. Rather than concentrate on protecting and enhancing Access to Cash, it once more demonstrated its partiality against cash payments and in favour of digital payments by appointing a panel of digital payment specialists under a mandate to highlight digital services that could substitute for cash in cases where is used now. It failed. It came up with absolutely nothing. Instead of admitting to this explicitly, its recommendation was that Open Banking be appointed as the future conduit for seeking these missing services. It was no coincidence that the Digital Payments Initiative's sponsor, the PSR, was about to take a higher profile in the governance of Open Banking. This is a good example of the incestuousness of this 'industry' and of the egregious 'regulatory capture' of the PSR by the digital payments industry.

Open Banking/Fintech – unauthorised on-sale of customer data

Open Banking providers have few sources of revenue. They are permitted to on-sell customer data as long as it is anonymised. In that case it ceases to be of any great value. The FCA should conduct a detailed investigation into all Open Banking providers (acting as Account Information Service Providers), who on-sell customer data to ensure that it really is anonymised and to conduct a sanity test: what revenues did the Open Banking provider receive from on-selling customer data and is it plausible that the purchaser-in-question would spend that amount of money for data that they could not exploit?

Open Banking/Authorised Push Payment Fraud

There is an overlap between Open Banking and Authorised Push Payment Fraud in the sense that Open Banking providers can be the conduit through which payment instructions are delivered via which an Authorised Push Payment Fraud is effected. In fact, if a fraudster obtains the log-in credentials for a customer's Open Banking providers and all of their accounts are accessible through that Open Banking provider (acting as a Payment Initiation Service Provider), the fraudster can clear out all the accounts. Open Banking providers claim that this would not work, because each Account Servicing Payment Service Provider would have a process in place to verify the payment order before executing it. The FCA should conduct a detailed investigation into all Open Banking Payment Initiation Service Providers to make sure that every single Account Servicing Payment Service Provider does have a process in place to verify a payment order, relayed to them by the Payment Initiation Service Provider, before executing it.[55]

Fintech – clientele of Silicon Valley Bank UK bailed out by the government bending the ringfencing rules and allowing HSBC to buy it…but with what allocation of capital, and with what risks to other customers of HSBC UK Bank plc now that VC funding for Fintech has dried up?

The government relaxed ring-fencing rules to permit HSBC to acquire Silicon Valley Bank UK within its ring-fenced bank.[56] This placed high-risk business inside a bank that was meant to be low risk, increased the likelihood of loss for other depositors, and increased the amount of the bank's capital that should have been earmarked to support mortgages and credit to UK individuals and businesses to instead be tied up behind loans to the Fintech clientele. As Fintech is high-risk, the amount of capital so tied up will be elevated.

[53] http://www.lyddonconsulting.com/open-banking-past-and-present-is-it-a-sham%ef%bf%bc/
[54] Lyddon, 'Capture', pp. 34-6
[55] http://www.lyddonconsulting.com/failures-of-fintech-open-banking-and-authorised-push-payment-fraud/
[56] http://www.lyddonconsulting.com/hsbc-rescue-of-silicon-valley-banks-uk-arm-did-have-taxpayer-support/

Fintech pays off its loans from the next ‘funding round’ subscribed by venture capitalists, or from the proceeds of an initial Public Offering. Both sources have dried up. How is the knock-on risk to other customers of HSBC’s ring-fenced bank being monitored and managed by the UK financial authorities?

This bending-of-the-rules to the benefit of Fintech counts as another example of the playing field not being level but being tilted in Fintech’s favour.

Fourth 'payment journey' to the utility room – eradicating the damaging legacy of EU membership

The decision by Pay.UK that the UK would remain a member of the Single Euro Payments Area (SEPA)

The decision for the UK to remain as a member of the Single Euro Payments Area was a political decision that should have been made by government. Instead Pay.UK appear to have made that decision autonomously. The main benefit for consumers of SEPA membership has been discontinued – moderation of charges for using payment cards in other member states. Similarly to the situation with deductions-from-face-value on card payments within the UK, the industry appears to block, pass up or otherwise undermine benefits for customers. This being the case there is no point in continued SEPA membership and it should be stopped since the UK is no longer and member of the EU and does not use the euro.

The adoption by UK payment systems of the SEPA data format - ISO20022 XML – how much easier to adopt the euro if we are already using the euro payment data format

The decision to adopt ISO20022 XML is similarly flawed. At the time the Bank of England and Pay.UK decided it would be used, the UK was an EU member state. Now it isn't. The decision should have been reversed at that time. In fact ISO20022 XML was not a global standard when a decision was made for the UK to use it. Its first deployment was for SEPA and even then its usage had eventually to be compelled, through EU Regulation 260 of 2012, known as the 'SEPA Migration End Date Regulation'. Its adoption by the UK was decided upon false pretences and it is not too late to reverse it. The suspicion remains that the adoption of ISO20022 XML is favoured by Remainers within the payments industry because its usage in the UK would facilitate the eventual adoption of the euro. Given that the country voted to leave the EU and will not adopt the euro, the UK ought to adopt a data format that meets the UK's needs, and not make the usage by others of ISO20022 XML as reason for the UK to use it.[57]

ISO20022 XML conveying more so-called 'financial crime data' – same problem as 'Trusted KYC Data Sharing'

ISO20022 XML certainly has the capacity to carry more data than its predecessors – SWIFT MT (for CHAPS), Standard18 (BACS) and ISO8583 (Faster Payments). ISO20022 XML is a bloated data format as well as a dated one. The concerns in adopting such a format are firstly efficiency: the entire bloated XML schema is transmitted every time, even if most of the fields are blank. This requires greater computer and communications capacity, even if no more operative data is transmitted than where a 'shorthand' like Standard18 is used.

Nevertheless the repeated contention of the Bank of England, Pay.UK and other ISO20022 supporters is that UK payment messages will transport more data and this data will be such as to facilitate the detection of financial crime. There has not been a deeper case put than that so far. A deeper case would lay out what the extra, mandatory data would be (it will be no use if it is optional), how it will be filtered and examined, and in what way that will lead to higher detection of financial crime.

If one accepts that there will be more data and that it will be filtered and examined, other outcomes are equally plausible:

1. More payments being blocked because systems detect a 'false positive', leading to greater payment delays;
2. Suspicious Activity Reports being wrongly generated which put an unwarranted black mark against legitimate payment actors;
3. Such black marks being shared around the payment industry under initiatives like 'Trusted KYC Data Sharing'.

The upshot would be that ISO20022 XML would act as a facilitator of systemic transmission of incompetence, and cause significant detriments to legitimate payment actors.

[57] http://www.lyddonconsulting.com/iso20022-the-great-leap-sideways/

But actually ISO20022 XML may contain even less scannable data for detecting financial crime

On the other hand it is equally likely that ISO20022 XML in the UK will for many years contain the exact same data as the respective legacy payment data formats: SWIFT MT if the ISO20022 UK credit transfer is being used for a CHAPS payment, Standard18 if the ISO20022 UK credit transfer is being used for a batch payments under the BACS process, and ISO8583 if the ISO20022 UK credit transfer is being used for an individual payments up to £1 million within the Faster Payments process. This would be the upshot of the first deployment of ISO20022 XML being 'like-for-like', a decision already made by Pay.UK.[58]

It may appear absurd that no new functionality is to be achieved as a result of a project (New Payments Architecture) that will have been well over a decade in the making once it has come out of its post-conversion support.

Not only has this project blocked any other developments within its scope for its duration, it may still be a few years after the project has exited post-conversion support that new functionality is added. By that time – possibly as late as 2030 – no new functionality will have added to the UK's electronic retail payment systems for 15 years.

As for the longer-term likelihood that ISO20022 XML payments will contain more scannable data and thus make a contribution to combatting financial crime, the experience in SEPA has been the opposite. A payment with both endpoints in the SEPA Area can be completed with just the IBANs of the payer and payee: no names, no addresses, no payment reason.[59] In this case the dozens of available data fields in the ISO20022 XML will be transported as the schema but with all but seven or eight of them being empty.

UK consumers' money can be 'safeguarded' (ha ha!) in any Hicksville Bank anywhere, thanks to the EU's Payment Services Directive and eMoney Directive[60]

The 'safeguarding' regime for customer monies held by eMoney Institutions/Fintechs is a legacy of the EU one. It allows UK customer monies to be lodged in virtually any bank anywhere.[61] The EU presumption was that such a bank, if in the EEA, will have been under the supervision of EU-equivalent regulators and regulatory regimes and will thus be solid. Because UK banks have turned away smaller payment service providers (Payment Institutions and smaller eMoney Institutions), 'safeguarding' accounts could only be obtained in such paragons of solidity and probity as Estonia, Latvia, Malta, Lithuania and Cyprus.

UK customer monies are at risk. The FCA and PSR seem to be unaware of this risk when the deposit institution is foreign. They have paid some attention to where the deposit institution is in the UK, and to have customer monies covered by the Financial Services Compensation Scheme where both the eMoney Institution/Fintech and the deposit institution come under the supervision of UK regulators, but not if there are foreign elements. It is therefore certain that the deposits of UK Payment Institutions/eMoney Institutions/Fintechs in a foreign deposit institution will be treated as an ordinary, unsecured liability of that deposit institution, if it goes into resolution or liquidation.

In the case of a resolution, the Payment Institution/eMoney Institution/Fintech will not even be protected up to EUR100,000 under the local counterpart of the Financial Services Compensation Scheme because it is an ineligible depositor. Instead the entire deposited amount will be 'bailed-in': converted into capital-like instruments in the new bank that is launched out of the resolution, which will be unquoted, illiquid and initially valueless.[62]

In case of liquidation, the Payment Institution/eMoney Institution/Fintech will receive the same premium as any other ordinary, unsecured creditor, and probably some time later.

Either way the UK customer will not be able to access their money for a long while, and they will for sure lose a portion of it completely.

[58] http://www.lyddonconsulting.com/pay-uk-board-ditches-main-benefit-of-iso20022-adoption/
[59] http://www.lyddonconsulting.com/payment-technocrats-have-crippled-eus-ability-to-impose-biting-sanctions-on-russia/
[60] https://globalbritain.co.uk/jeremy-hunt-should-be-aware-the-financial-conduct-authority-has-form-in-supporting-de-banking/ accessed on 17 August 2023
[61] http://www.lyddonconsulting.com/failures-of-fintech-safety-of-safeguarding/
[62] http://www.lyddonconsulting.com/emoney-safeguarding-regime-in-doubt/

Accounting and legal basis of 'safeguarding'

The FCA has recognised some of the issues around separating customer monies from the funds of the Payment Institution/eMoney Institution/Fintech, and making sure that no other creditors of the Payment Institution/eMoney Institution/Fintech should be able to make a claim on the customers' money.[63]

Having that as an objective is one thing but the reality is that creditors of iPagoo will have the funds returned to them diminished because other creditors have been able to attach some of them.[64] The FCA/PSR had to join the iPagoo legal action to find out what the legal treatment was – an absurdity.

The conclusion to be drawn from the iPagoo case is that customers' money is not genuinely 'safeguarded' under the application of English law if the firm goes under.

Digital currency: how much easier to adopt the euro if there is no physical cash to replace

This is an aside for the current process but an important point for Remainers: it is easier to adopt the euro if there is no cash and coin to replace. The legacy national currencies of the initial Euro joiners disappeared in scriptural form on 1st January 1999. For an initial period the legacy currency amount of a euro payment or bill had to be shown as 'Euro-Related Information' or 'ERI', but the legacy currency in scriptural form had effectively ceased to exist at the end of 1998.

Not so the legacy currency note and coin.

While euro note and coin came into circulation on 1st January 1999, there was a six-month dual circulation period until the legacy currency note and coin ceased to circulate. This was a colossal and costly logistical exercise. How much easier if there had been no legacy currency note and coin at all!

[63] http://www.lyddonconsulting.com/failures-of-fintech-accounting-and-legal-basis-of-safeguarding/
[64] http://www.lyddonconsulting.com/ipagoos-insolvency-puts-question-mark-against-npa/

Fifth 'payment journey' to the utility room – FCA failure to close loopholes in AML/CFT regime invented and exploited by participants in detrimental projects, resulting in a further, hidden subsidy for fintech

eMoney Institutions/Fintech – placing unauthorised reliance on the AML/CFT work of others in order to shortcut their own homework

eMoney Institutions/Fintech place reliance on the AML/CFT due diligence work of other 'obliged institutions', without the knowledge and consent of the other 'obliged institution', so as to save themselves the trouble of doing the work themselves. This was the first subject addressed in our Open Letter to the Project Financial Crime set up by the sector trade body The Payments Association to supposedly solve the major financial crime issues of the sector.[65] The failure of the FCA to make sure that reliance is placed only with the knowledge and consent of the party being relied upon and for permitted tasks acts as a lowering of the bar in favour of Fintech. It permits them to carry out less work and incur less cost.

eMoney/Fintech – setting up an account based on Simplified Due Diligence, then immediately offering add-ons which, had they been part of the initial service package, would have required ordinary Customer Due Diligence and Enhanced Due Diligence as appropriate

This was also addressed in our Open Letter. It is the technique whereby a very simple service package is offered to the customer at set-up, basic enough to qualify for Simplified Due Diligence. Additions are quickly made to the service package once established – and it could be minutes later- such as the issuance of an IBAN. Had the additions been part of the initial service package, Simplified Due Diligence would not have been sufficient and the payment service provider would have had to carry out ordinary Customer Due Diligence and, if the case warranted it, Enhanced Due Diligence.[66] The outcome is a far too low level of due diligence effort given the service package, a form of disguised subsidy in the form of work not being carried out.

eMoney/Fintech – usage of Virtual Accounts, bypassing any due diligence

eMoney Institutions/Fintechs arrange for the issuance of an International Bank Account Number, firstly without the account being a bank account, and secondly with the composition of the IBAN being such as to identify a different payment service provider.[67] No account belonging to the respective account owner exists at this second payment service provider: despite issuing an IBAN identifiable to itself, this payment service provider has no Customer Due Diligence file on the entity that uses the IBAN, a breach of the 2017 Money Laundering Regulations. Being able to arrange IBANs for their customers improves the customer service proposition of the eMoney Institutions/Fintechs, but they do not have to make the arrangements to issue their own IBANs, saving them money, another disguised subsidy. Their identities are also absent from the payment messages as payer/payee payment service provider, a breach of Funds Transfer Regulation.

eMoney/Fintech – 'nesting': disguising intermediary payment service providers in the payment chain in defiance of Funds Transfer Regulation

eMoney Institutions/Fintechs use other eMoney Institutions/Fintechs as their payment service provider. The intermediary payment service providers – since there may be more than one – are not identified in the payment messages, a breach of Funds Transfer Regulation.[68]

FCA view

The Financial Conduct Authority sent a scathing letter to the sector about certain of its business practices, but has not so far followed through with specific action to combat the shortcutting of AML/CFT procedures listed above.[69] This approach both perpetuates the hidden subsidy afforded to the sector, and lays it open to financial crime. The eMoney/Fintech sector will counter that the above problems can be laid at the door of the FCA and the PSR for their failure to ensure access to accounts and payment services as required by Article 105 of the 2017 Payment Services Regulations.

---

[65] http://www.lyddonconsulting.com/open-letter-to-project-financial-crime-c-o-the-payments-association/ p. 2
[66] Open letter as above pp. 2-3
[67] Open letter as above pp. 2-3
[68] Open letter as above pp. 3-4
[69] http://www.lyddonconsulting.com/financial-conducts-authority-letter-on-failings-in-the-non-bank-payment-service-provider-sector/

There is some merit in this argument, insofar as it affected smaller firms, and this problem is outlined below under the heading '*De-banking of smaller cross-border payment firms'*. However it did not affect eMoney Institutions as much as Payment Institutions because the former tend to be larger and to generate more revenue for banks, in which case the banks are willing to adjudge that the returns of banking them do justify the risks.

Sixth 'payment journey' to the utility room – unravelling the causes of de-banking

Globalist 'Financial Action Taskforce' as the source of the problems

The global regime for combatting money laundering and the financing of terrorism pre-dated the Global Financial Crisis but its manifestation has interacted with the cures for the ills diagnosed as causing the Global Financial Crisis to create a banking market in which some types of customer are in high demand and others are frozen out.

The recommendations and special recommendations of the Financial Action Taskforce do seem to have restricted the financing of terrorism, but they have had little impact on money laundering and on financial crime generally. Fraud is widespread and, in the UK, untackled by law enforcement.

Stigmatization of all forms of international business and connections > De-internationalization

The Global Financial Crisis was misdiagnosed in the UK to focus attention on cases like Lehman Brothers and Royal Bank of Scotland, and away from Northern Rock, Bradford & Bingley, Alliance & Leicester, Britannia, and Halifax/Bank of Scotland.[70]

The main resulting action – ring-fencing at the major banks – bundled international business with investment business and designated both as high risk, even though it was in mortgage lending that the UK suffered the most casualties.

Supposedly low-risk business – including mortgages – was segregated inside the ring-fence. Political pressure was brought to bear to divert resources to this area rather than to investment/international business, and to set suitably narrow criteria for what type of business this bank could take on.

Anything foreign has become a no-no: non-resident accounts, businesses with foreign ownership, businesses with foreign directors, principals or signatories, individuals or businesses with foreign connections.

Individuals or businesses engaged in a lengthy list of supposedly higher-risk businesses have become a no-no: the list is too long to reproduce here but it is based on original FATF lists of industries (each with its own SIC code) that FATF believe to show a raised incidence of financial crime.

On the other hand the bank outside the ring-fence usually sets a minimum revenue per customer of US$250,000 per annum. It has a permission to deal with higher-risk business if it will deliver that amount of revenue, because the supposed costs of mitigating the risks can be met from that size of revenue.

This leaves a very considerable number of individuals and businesses whose characteristics rule them out of being banked within the ring-fence, but whose transactions will not deliver an annual revenue of US$250,000. They will therefore be turned away by both sides of the bank, the ring-fenced one and the non-ring-fenced one.

The ring-fenced bank becomes narrow and parochial; the non-ring-fenced bank becomes global and institutional, dealing with multinational corporates, government entities, other banks, and the large non-bank financial institutions.

The other negative outcome of this is the narrow scope and low service level of international services available to customers of the ring-fenced bank. The ring-fenced bank is not permitted to enter into a service level agreement with the non-ring-fenced bank to buy higher-quality international services for its customers, and it is precluded from entering into direct relationships with correspondent banks. The outcome is that the ring-fenced bank cannot adequately service domestic customers with international needs, and these customers are inconvenienced by being compelled to obtain those services from other suppliers, often from eMoney Institutions, which may not be their preferred choice.

[70] http://www.lyddonconsulting.com/the-great-game-of-basel-rules-its-worse-than-we-thought-and-how-new-labour-loved-it/

De-banking of smaller cross-border payment firms[71]

Smaller payment firms and in particular Small Payment Institutions have been particularly badly affected by de-banking. Serving other financial institutions is the province of the non-ring-fenced bank, whose target market is other banks and the larger non-bank financial institutions.

The ring-fenced bank may only take on a financial institution as a policy exception. The process gone through by NatWest in the timeframe 2018/9 is notable: it transferred all financial institution relationships into NatWest Markets, or rather it transferred all the relationships that met the criteria of NatWest Markets. The other relationships were terminated.

Small Payment Institutions do not present a revenue potential of US$250,000, and so would not be of interest to a non-ring-fenced bank. On the other hand a non-ring-fenced bank is of no interest to a Small Payment Institution because the services it requires are supported in the ring-fenced bank.

The services include cash and cheque pick-up by security courier and debit card acceptance the latter requiring a physical service via a branch or regional operations centre. In fact the banks have discontinued security courier pick-up, as well as hobbling step-by-step the usage of cash.

Neo-banks (like Starling, Monzo and ClearBank) do not offer those services, nor do foreign banks or building societies. The Post Office, Santander (the former Girobank) and Co-Operative Bank – three traditional supporters of physical services – retain some degree of capability, but the trend is towards degradation and withdrawal.

The responses of Small Payment Institutions have been various, as laid out in the footnoted blog, but none of them involve using the banking services they want and in the way they want them supported. The base has been withdrawn, and the Small Payment Institution has to adapt to substantive or actual de-banking. The commonest responses have been re-positioning themselves as an agent of a larger actor – reducing competition – and nesting – retaining their own identity but using either an Authorised Payment Institution or an eMoney Institution as their main payment connection, and at the same time reducing their payment volume so as to avoid the need to 'safeguard' customer monies.

Banks' and Payment Service Providers' narrow and copy-cat Target Market Definition and Risk Acceptance Criteria

Banks and Payment Service Providers set their Target Market Definition and their Risk Acceptance Criteria, applicable to market segments such as 'UK personal banking', 'UK microenterprise banking', 'UK small and medium business banking', 'UK commercial banking', 'Corporate and institutional banking'.

In a bank subject to ring-fencing, the relationship management for 'Corporate and institutional banking' will be in the non-ring-fenced bank.

The market segments are then broken down into Customer-Facing Business Units operating under the Target Market Definition for their market segment e.g. 'UK personal banking – East of England' or 'UK commercial banking – transport and utilities'.

The Target Market Definition gives the general characteristics of the types of customer the bank or PSP wishes to serve, which services the customer is expected to use and in what volume/value, and the resulting revenue for the bank or PSP. A customer fitting the Target Market Definition and using an array of services would by definition generate the returns needed in order for fulfilment of the mantra 'the returns justify the risks'.

The Risk Acceptance Criteria go hand-in-hand with the Target Market Definition, specifying the risks arising from banking customers within the scope of the Target Market Definition, and the cost of mitigating those risks. The cost-of-mitigation of a particular risk will present itself as a cost levied by the internal Business Unit responsible for managing that risk on the respective Customer-Facing Business Unit.

[71] https://globalbritain.co.uk/jeremy-hunt-should-be-aware-the-financial-conduct-authority-has-form-in-supporting-de-banking/ accessed on 17 August 2023

This is the source of the other amount mentioned in the mantra 'the returns justify the risks': there is an accumulation of internal charges for risk management on the Profit & Loss account of the Customer-Facing Business Unit serving the client, set against the revenues. This accumulation of charges is added to a portion of the costs of the Customer-Facing Business Unit itself, as well the costs levied by operational business units for carrying out the customer's transactions, and for ancillary services like statement production and electronic banking. In this way the Customer-Facing Business Unit's Profit & Loss account can be broken down to a customer-by-customer level. If the revenues from that customer are below the aggregate of all of those lines of cost, then the 'returns do not justify the risks'.

In order to contain the incidence of risk within the customer base of each Customer-Facing Business Unit, limiting characteristics are applied at the level of individual customers or applicants by the Risk Acceptance Criteria, in the way insurance companies specify either types of policy they will not write or events the policy does not cover.

This is where the filtering is carried out, which leads to de-banking of customers or to the turning-away of applicants. There is no outcome in retail and business banking that is the equivalent of an insurance company writing a policy with special conditions or loading the premium. That outcome is reserved for customers within the Target Market Definition of 'Corporate and institutional banking', or of a unit for Wealth Management or Private Banking, if there is one. These units will be equipped firstly to undertake Enhanced Due Diligence as part of the initial AML/CFT due diligence on the customer, and then to run enhanced monitoring of the relationship once it has begun.

No such option is available to other market segments and the result is that the Risk Acceptance Criteria will disbar any customer or applicant that shows a characteristic which would cause Enhanced Due Diligence:

- Politically-Exposed Person;
- Connection to a high-risk jurisdiction;
- Connection to a high-risk industry or activity.

Notwithstanding that legislation does not dictate that customers/applicants requiring Enhanced Due Diligence should be de-banked or turned away, this is what is the reality in UK banks and PSPs.

High personal penalties for bank staff who take a risk and get it wrong (money/prison)

The AML/CFT regime involves high personal penalties for taking a risk and getting it wrong. This will include the loss of career as a starter, as well as financial penalties, but it could also include prison time.

Against that backdrop it is not feasible that individual staff members will deviate from the Target Market Definition and Risk Acceptance Criteria of the business unit in which they work.

Distortions caused by deductions-from-face-value on payment cards

This is a shared objective amongst banks and payment service providers going after the business of the customers who would fall within any of 'UK personal banking', 'UK microenterprise banking', 'UK small and medium business banking', and 'UK commercial banking': it is to get the payment card business.

It appears to be accepted that the bank or payment service provider issuing a card that is used by such a customer receives around 3% of the value of all purchases – instead of 0.2-0.3% as specified by the Interchange Fee Regulation.

It is hard to overstate the degree to which obtaining this high percentage of the turnover through an account (because such a small percentage of turnover is represented by cash, cheques and credit transfers) has become the entire focus of the industry.

The industry's 'in-flight plans' will result in more card payments at the expense of cash and cheque, with perhaps a modest share of the decline in cash and cheques being taken up by credit transfers.

Given the colossal revenues available from card payments from low-risk customers, there is no need to take risk in straying beyond narrow Risk Acceptance Criteria.

The deductions-from-face-value available on – primarily – Visa- and Mastercard branded cards have led to an overcrowding of banks and payment service providers all soliciting for the same business from the same customers.

The neglect of 'peripheral' customers and of non-digital services is a direct result of the way in which 'digital' has been permitted to unfold in the UK. There is very little genuine choice, although there is competition, if one understands competition as being many market actors trying to get exactly the same business. That is not competition, though, when a main element in the Price + Performance = Value equation is not negotiable (Price) and when the Price is forced not on the payer, as was the intention of the Interchange Fee Regulation, but on the payee.

It is hard to overstate the distortion of competition in the UK payments business and in the overall provision of banking services that has been brought about by deductions-from-face-value on card payments.

Fraudsters and money mules do not fall between the cracks, and carry out Authorised Push Payment Fraud

Notwithstanding the risk-aversion of payment service providers, their narrow Target Market Definitions and restrictive Risk Acceptance Criteria, it has proven perfectly easy for the perpetrators of Authorised Push Payment Fraud and their money mules to open payment accounts, receive the proceeds of their malefaction, and transmit them out of reach.

This subject features little in the PSR's deliberations about Authorised Push Payment Fraud. Without such ready access to payment accounts, the fraudsters could not engage in Authorised Push Payment Fraud. Looked at in this way, Authorised Push Payment Fraud is the fault of payee payment service providers, and they should reimburse all cases of Authorised Push Payment Fraud in full as punishment for their AML/CFT failings in:

a. opening a payment account for the fraudster or mule;
b. not checking the coherence of the named payee of a payment with the name on the account identified by the Sort Code and Account Number contained in the payment;
c. not installing a profile of the expected activity level on an account commensurate with the Know Your Customer and Know Your Customer's Business Due Diligence that they are required to carry out at the opening of the account;
d. failing to monitor actual activity against expected activity, a process that would have shown a major discrepancy and given rise to special monitoring of the account and Suspicious Activity Reports;
e. not maintaining adequate facilities to reclaim monies fraudulently obtained and then further transmitted onwards, once it had become clear that a fraud had been perpetrated.

These failings – which are industry-wide – have created the seedbed for Authorised Push Payment Fraud. They point to the payee bank being the one that should reimburse losses 100% in all cases. Of course, when it comes to the major banks, they will be acting as both payer and payee bank in many cases and can reimburse themselves. In all cases the reimbursement of losses on account of Authorised Push Payment Fraud can be construed as a fitting punishment for payment service providers for failures in AML/CFT due diligence.

Question 2: For these journeys today, how does the UK consumer experience for individuals and businesses compare versus other leading countries? For example, the quality of experience, security or cost.

The question is misplaced. Far too much attention has been paid to what goes on in other countries: this legitimizes the copying of approaches and the basing a business case – for example the adoption of ISO20022 XML – on its supposedly global adoption.

Question 3: Looking at the in-flight plans and initiatives across the payments landscape, how likely are they to deliver world leading payment journeys for UK consumers? For example, we welcome suggestions that you feel would support, or are essential to delivering, world leading payments for UK consumers.

The in-flight plans are certain not to deliver 'world leading payment journeys for UK consumers' or for businesses. They are already leading to the opposite.

I would confirm my suggestion: first eradicate all the issues, detriments, costs and risks that have been created for UK consumers and for businesses, and which are enumerated under my answer to Question 1, and then we can take stock with a view to plotting out a completely new roadmap.

Yours faithfully,

R.J.Lyddon