



## **THE EVIL PAYMENTS TRILOGY: PUSH PAYMENT FRAUD; ABOLITION OF CASH AND DEDUCTIONS FROM FACE VALUE WHEN PAYMENT IS MADE BY CARDS**

*Gordon Kerr<sup>1</sup>*

**Abstract:** *Initiatives in accounting, central banking supervision of banks, bank stability and payments which incept in the UK are generally copied throughout the EU. The Bank of England are, it is believed, determined to abolish cash and replace it with a CBDC (central bank digital currency) already trendily named “Bitcoin”. Riding the general wave of enthusiasm for tech and “digitisation”, rapid changes are planned late 2022 early 2023 to the UK payments system. All of these changes, proposed by regulators as ‘modernisation’ to be embraced and worshipped on the altar of tech, tech and more tech, should be paused. The real agenda of the Bank of England (and ECB) is to abolish cash to enable deeply negative interest rates despite rising inflation. This will be retrograde for UK and European societies; will lead to mass poverty and will reduce democratic accountability of governments. Moreover, the desire to abolish cash has incentivised the Bank of England via its subsidiary regulator, the Payment Services Regulator, to do nothing to address rising frauds and charges for card use, since they will claim that this Bitcoin replacement of cash will be easier to use and cheaper than cards and less exposed to fraud. The present payments landscape in the UK is dystopian, marred by three easily fixable problems causing massive consumer harm. They are each presented here and collectively termed the ‘evil payments trilogy’.*

**Keywords:** *Cash, payments, cards, payment fraud, CBDC, central banks, Bank of England, Payment Services Regulator, Visa Mastercard, stress tests, IFRS accounting rules, zombie banks*

**JEL:** *G18, G21*

---

<sup>1</sup> Founder of Gobden Partners, UK



*Objective. A public call for all UK and EU new digital initiatives in payments to be suspended pending the establishment of a genuine, independent committee of experts to evaluate the costs and benefits of the preservation or abolition of cash*

## **1. Executive Summary**

Simply because all citizens of UK and Europe are using less cash – physical shops, bars sports venues and marketplaces are increasingly refusing cash and demanding card payments – it is vital to the preservation of democratic societies that citizens’ rights to withdraw all their funds from banks in cash are preserved. It is syllogistic to suggest, as proponents of cash abolition always do, that because we all use less cash then it logically follows that central banks should feel able to abolish cash and replace it with central bank digital currencies (CBDCs). There is not one iota of any logic linking this premise with the conclusion. If CBDCs are designed to replace cash, and if we don’t need cash, then CBDCs are not needed either. But as set out herein, we do need the power to withdraw our funds from banks, and the power not to deposit our funds in banks; and these powers are impossible to preserve unless we preserve also cash.

There has been much research on the topic, some of this with different simulation models of impacts of CBDC (Leonov, 2022), (Ozturkcan , et. el 2022) whose findings suggest there are benefits of CBDC. For example, the study of Leonov (2022) concludes that CBDC impacts the economy beneficially through changes in the monetary base, strengthening the structural liquidity deficit, banking disintermediation, and increasing fiscal policy capabilities.

Most of this research concentrates on the technical issues of CBDC. They neglect to analyse the core issue problems of the dramatic change to people’s control over their lives and spending.

The media in the UK and the general public have been fooled into believing that, after the spectacular GFC banking collapse of 2007-09 our banks have been recapitalised. The UK is dominated by 5 large banks who control 96% of all UK banking business including all account holders: retail, business, NGOs municipal, government, education, utilities and charities. This is false, all SIFI banks remain zombified and on central bank life support. There is no functioning interbank market for funding and the Bank of England operates as the lender of first resort (not last resort) and at ultra-low interest rates (not at penalty rates) on a permanent basis (not for the provision of temporary liquidity). Late in September when the Bank of England announced it was planning to reduce quantitative easing to banks, the market reaction was sufficiently strong to result in the resignation of the then new Prime Minister Truss. Since then the B of E has openly acknowledged its subordination to ‘the markets’ and its fragile attempts to compel banks to stand on their own two feet have been quickly abandoned.



Consequently, the context to each limb of the ‘evil payments trilogy’ as set out below, is a concerted effort by the UK government, central banks and the Visa/ Mastercard duopoly to abolish cash. This trend is spreading to Europe where the payment landscape is notably different but not so different as to fail to be exposed to the same three problems. These are powerful forces, and sadly the public and elected politicians understand few of these points.

The context of this paper is the UK (and European, but the paper is short and focuses on the UK) reduction in the availability of cash.

## 2. The Colossal Problems Caused by ‘Digitised payments’ in the UK

The common thread behind the three problems which will be summarised in this section is the remarkable weakness of the specific regulator, The Payment Services Regulator, which was set up as a limb of the Bank of England as recently as 2014. At every juncture it has acquiesced to the wishes of Visa and Mastercard, ignored EU laws limiting deductions from payments (such laws being enshrined automatically pre-Brexit in the UK legal code), and sat idly by as the banking industry has succeeded in leaving liability for weaknesses in banking technology with their customers. This latter point has been a massive encouragement to fraudsters who prey on everyone with access to online banking and of course in particular on the vulnerable and elderly. As a child of the 60s I have now lost both my parents, but nearly all my friends, lucky enough to still have living parents, have removed their parents’ access to online banking and to the internet itself. Removal of the internet, owing to email pressure, obviously increases the sense of loneliness and reduces quality of life, and inability to use online banking is a particular inconvenience to elderly UK citizens given the substantial reduction in physical bank branches. There is simply no alternative course of action for these middle-aged children since their parents would otherwise be scammed multiple times each week. Almost all of this would have been avoided had the regulator been willing to regulate, as opposed to cheering on Visa and Mastercard from the side-lines.

It is precisely this relaxed, casual regulatory approach that has inspired banks and the Visa Mastercard duopoly to ignore laws and nakedly promote their own interests at the expense of their customers (basically all of us, we all need to make payments all the time) in defiance of the rules. This has resulted in a relentless reduction in the quality of service by banks, the closure of swathes of physical branches, and the promulgation of dishonest banking spin to justify this; banking PR teams claim that these closures reflect the wishes of their customers: “our customers prefer to do banking on their phones than in branches”. Nonsense.



### 3. Each Leg of the Trilogy; Problem and Obvious Solution

#### a) **Failing Access to Cash**

Not only are bank branches being closed, but the banking industry has rejected entirely sensible proposals from the ATM industry, who obviously are synonymous with the pro cash lobby, for ATMs to be rolled out which not only dispense cash but also enable merchants to deposit cash. No UK ATMs allow this; the regulators in typically supine fashion have acceded to the specious argument by the anti-cash lobby that to allow deposits of cash via ATMs would somehow facilitate fraud and money laundering. Clearly the deposit instruction would be to pay the cash to an account which has already passed all the KYC and anti-money laundering checks else it would not exist as a bank account in the first place.

Before setting out the perfectly sensible proposal to solve this problem, a few words about the pending financial collapse of the cross-bank UK ATM system called LINK. I quote the ultimate expert on whose work this entire paper is based, Bob Lyddon (see References):

*“LINK is the payment scheme, regulated by the PSR, under which cardholders can withdraw cash from ATMs where the ATM operator is not their card issuer. Before LINK NatWest cardholders could only draw cash from NatWest branches for example”.*

In August 2022, Lyddon continues, the CEO of LINK predicted cash will end within five years because this infrastructure is collapsing. The fixed costs of LINK are £5 billion each year. No data is available for the number of bank branches in the UK (this data exists but is not revealed to the public by the banking industry); but as a reasonably sharp observer of our high streets the author estimates that 60 – 70 per cent of bank branches have closed since the Great Financial Crisis (GFC). This underlines the point in the Executive Summary, that the claims of the Bank of England that banks are ‘fixed’ or ‘recapitalised’ are false.

#### Solution

The solution to this ‘Access to Cash’ problem is to change the rules regarding the fees that banks pay to this LINK system called the “interchange fee”. This should be banded. This could ensure the continuation of a network of free to use cross bank ATMs.

The solution is set out in the paper but, put simply, involves amending the present interchange fees which banks pay for each cash withdrawal at a different bank’s ATM. Presently this is a fixed GBP 0.30 pence. Merely by increasing this pro rata to branch closures and reducing it for branch openings, the problem can be solved.

#### b) **Authorised Push Payment (APP) Fraud.**

In the UK all bank accounts are identified by two numbers; one is a six-digit bank branch identifier called the “Sort Code”, common to thousands of customers of that branch, and the



second is an eight-digit account number which no other customer *of the same branch* will have, but which customers of other branches and of other banks will have. As readers will know, given that all credit card numbers have been sixteen digits for decades, eight digits is exponentially much smaller. For this reason, in the UK it is false to assert that there is any such thing as a “unique customer identifier”. The shocking problem set out below has happened because of the general move to digitisation, which the Payment Services Regulator (PSR) has blithely nodded through.

Data published by two trade associations UK Finance, and Financial Fraud Action UK, showed that APP fraud in H1 2018 was £145 million, up 44% on H12017<sup>2</sup>. Although these gross numbers are small, the average loss per customer (GBP 4,000) is much larger than for card fraud (GBP 300). Estimates for 2022 are that customers will be defrauded of £2 billion.

There are many APP variants. A common example is where the criminal induces the bank customer to send a typically quite large payment- for example a deposit to purchase an apartment – to a bank account controlled by the criminal. Property purchase deposits are a typical use case. The customer is excited about buying his home, there is time pressure, he has not previously made an online payment to his solicitor (many solicitors are today provided “free” by mortgage lenders) so when he receives an email purporting to emanate from the lawyer in identical font and format to what he is used to, correctly identifying the apartment, the date the payment is due and stating the correct amount he is easily persuaded to press the button on a transfer of say GBP 25,000.

Consumer groups are worried, particularly because unlike card fraud, where the loss is usually borne by the bank, the significance of this rapidly growing APP fraud is that the loss is typically borne by the customer. This is different from the established practice for card payments. When a customer disclaims liability for a card transaction in the UK, the bank must demonstrate on the balance of probabilities that the customer has been reckless with his PIN number and stewardship of the card. If it cannot, the bank should bear the loss. However, the cybersecurity measures and rules which banks have established regarding online payments concentrate on the physical hardware. As a result, if a device (laptop/ phone) which has been accredited by the customer as his own is used during an APP scam or spoof, the customer will usually bear the loss.

### *Solution – Confirmation of Payee*

The central flaw in the present online payment system is the lack of a name check in the messaging system which is at the heart of the UK’s online payments system known as “Faster

---

<sup>2</sup> <http://www.ukfinance.org.uk/criminals-steal-500m-through-fraud-and-scams-in-the-first-half-of-2018/>



Payments”<sup>3</sup>. How was this allowed to happen? This absence can be viewed as a side door to the system which was opened when the present Europewide Point of Sale (PoS) payments architecture was established some 20 years ago. For PoS to work, the payments system had to generate a fast and accurate response from the purchasing customer’s bank as to whether a) she had enough funds in her account to pay for the item; b) whether the debit / credit card was valid and not reported lost or stolen. Authentication was initially based on a visual check of the signature strip which later was replaced by Personal Identification Numbers. So these card based PoS purchases were the first payment processes requiring the payer’s bank to receive a message and respond to it within a few seconds. The payee’s identification information was never required to be captured by such a messaging system since that information was contained in the PoS device which initiated the message/ payment request.

As each new iteration of payments technology was adopted, the payments architecture was further constructed, but around this side door flaw. Today the Faster Payments architecture uses the ISO8583 data protocol, the same as for card payments, throughout Europe. In Europe, and a few countries beyond Europe’s borders, a similar fast payments architecture is in place, known as SEPA INST. This is an instant credit transfer system, in any major currency, which can be conducted using just an IBAN number, so again the payee’s name is not required and the side door to APP fraud is wide open.

The obvious solution to APP fraud is for the system not to make the payment unless the payee’s account details match the payee’s name which the customer types into her tablet or other device. The payments industry has been talking about implementing such “Confirmation of Payee” (CoP) protection for years. The PSR constantly assures the Government’s Treasury scrutiny committee that CoP will soon be in ‘in place’ but there is little chance of a working CoP protocol being established before 2023 -5, if at all, because the UK is at the start of a project to completely overhaul the non-card payments infrastructure. The project is labelled the New Payments Architecture (NPA) and aims to rip out and replace this infrastructure. The new architecture will facilitate the replacement of the old, slow, costly (to banks) payment methods such as cheques and encourage retail customers to make greater use of irreversible online payment tools which are beloved of APP fraudsters.

---

<sup>3</sup> APP fraud can also occur in one of the UK’s other main payments system called BACS. This supports cheque clearing and customer initiated payments over the slower, paper form based system called CHAPS. For brevity we will consider only Faster Payments here.



### c) Deductions from Face – Card Payments

A perfectly sensible piece of EU legislation was enacted in 2015, the Interchange Fee Regulation (EU 2015/751). Pre Brexit it automatically became UK primary law, and this law has survived Brexit. The law specifies the maximum deductions from the ‘Face Value’ of the transaction:

- i) Debit Cards – 0.2%
- ii) Credit Cards – 0.3%

So if a lady buys a pair of shoes costing £100 the shoe shop is legally entitled to receive no less than £99.80 if she pays by debit card or £99.70 if she pays by credit card.

But once again the sleepy PSR regulator has proved spineless, and this law is ignored by the entire card industry. Obviously, giants such as Amazon can negotiate Visa and Mastercard down to relatively small deductions, but small merchants are today facing deductions of 3% to 8%. This is scandalous.

Moreover, there is always a minimum deduction of £0.30, which of course equates to 30% if the item costs £1. To be clear, this interchange fee deduction is only the fee allowed to the hierarchy of actors in the card business. Another level of deductions is permitted to merchant sources such as Elavon, Sumup and Barclaycard.

### Solution – Enforce the Law

Interchange Fee Regulation (EU 2015/751) should be enforced and the deductions limited to 0.2% and 0.3% as set out above.

### 4. Conclusion

The author has assisted the payments expert Bob Lyddon prepare a 100-page paper on this subject which he has sent to the Treasury, to the PSR, to the Bank of England, and to several members of Parliament. The short form of the message is that the Bank of England should ice its two major pro digitisation projects until the colossal problems caused by each of the three legs of the ‘evil trilogy’ set out above are solved. The two projects are:

- a) The “New Payments Architecture” project, intended to transpose SEPA euro data payment standards (ISO20022XML) into UK retail payments.
- b) Open Banking: the legislation allowing new fintech startups to demand via API links all bank customers’ data in order to pitch to them. This was supposed to engender competition and encourage the big 5 banks to sharpen up their act. But this aim has already failed. Instead, the data is purely being used by sloppy payments actors and finding its way into the hands of fraudsters.



The urgency from the Bank of England is to protect its own reputation by abolishing cash so that as the true dire financial condition of the big 5 becomes apparent to the public, they will be unable to withdraw their funds and cause bank runs. All present CBDC design work is being done by the same digital industry actors responsible for the ‘evil trilogy’ and therefore these companies have a vested interest in not fixing these colossal problems.

On top of these problems, as set out in the ‘Deductions from Face’ section, the Visa/ Mastercard duopoly sense that now is the time to seize the opportunity to push hard for cash abolition which will push so much more business their way. They have succeeded in swamping the two relevant Bank of England ‘committees of experts’ with their own people. These committees are supposedly ‘evaluating’ the pros and cons of keeping cash versus abolishing cash, but the decision to abolish cash has already been doubtless taken by these conflicted placemen of Visa/Mastercard. This is unacceptable and these committees should be re-established with unconflicted experts.

## References

Leonov, M., 2022, MONETARY POLICY AND BANKING INTERMEDIATION IN CBDC ECONOMY, INDEPENDENT JOURNAL OF MANAGEMENT & PRODUCTION (IJM&P )<http://www.ijmp.jor.br>. 13, n. 4, Special Edition CIMEE -June2022  
<http://www.ijmp.jor.br/index.php/ijmp/article/view/1928/2157>

Lyddon, R 2022 Capture – A New Major Paper on the Committees Considering a UK Central Bank Digital Currency:  
<http://www.lyddonconsulting.com/capture-a-major-new-paper-on-the-committees-considering-a-uk-central-bank-digital-currency/>

Ozturkcan S., Senel K., OzdincM., 2022, Framing the Central Bank Digital Currency (CBDC) revolution,  
<http://nu.diva-portal.org/smash/get/diva2:1684261/FULLTEXT01>