Flaws in the UK Faster Payments ecosystem that have led to the sharp rise in Authorised Push Payments Fraud

Bob Lyddon – Project Carlton Lead Consultant

Vendorcom Faster Payments Special Interest Group Event

London 8 November 2018

Lyddon
CONSULTING SERVICES LTD

Introduction

What is the problem?

- Faster Payments is the main completion channel for Authorised Push Payments Fraud
- New Payments Architecture elevates Faster Payments and makes it the universal retail settlement system

Who I am

- Management consultant in banking and payments of 23 years' standing
- Former General Secretary of the IBOS Association banking club

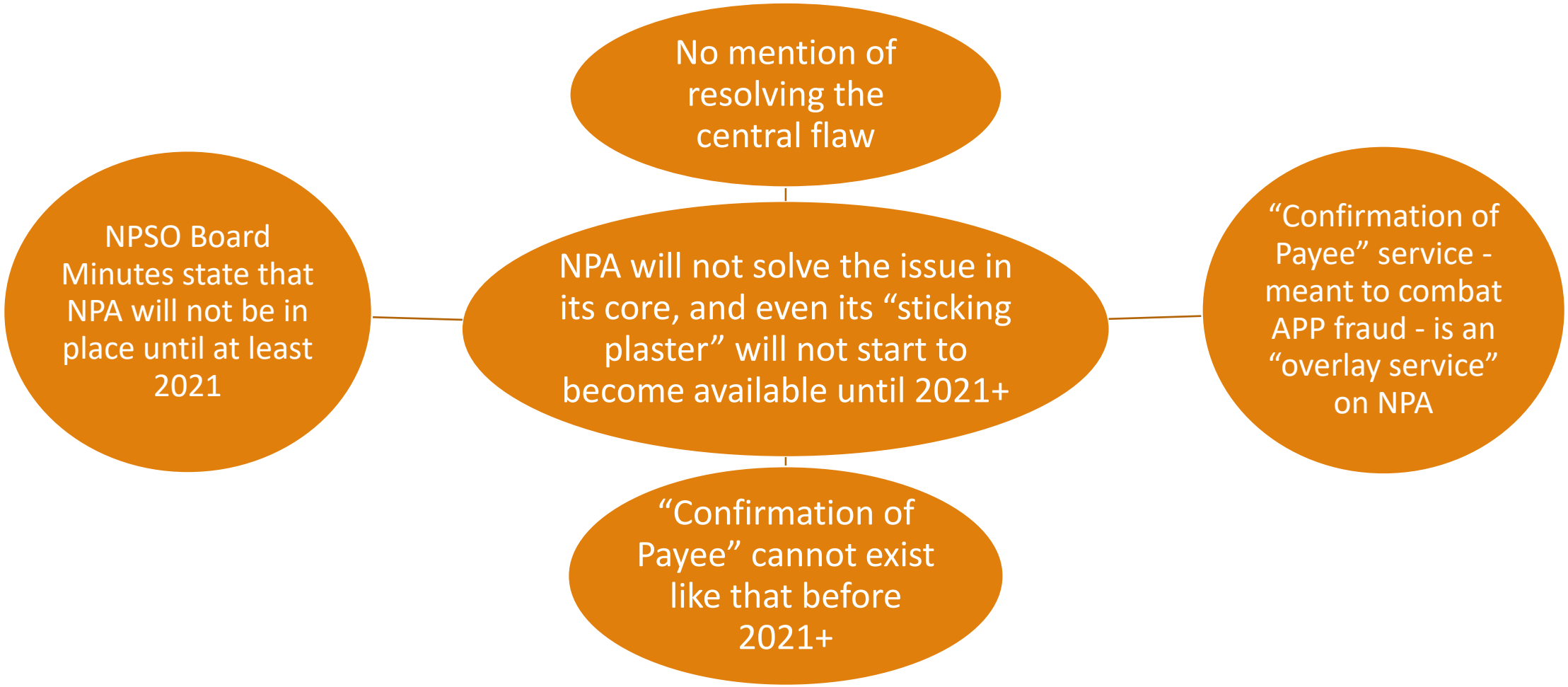
What is Project Carlton?

- Research project to initially provide an overview of the multiple failures and mistakes made in UK payments landscape since 2014
- This should lead to a business case for a change in direction

Problem exacerbators

- Fraud statistics list “Authorised Push Payments Fraud” separately from fraud using eBanking channels (like mobile, PC, telephone)
- Yet the outcome of a fraud through an eBanking channel is normally a Faster Payment to a fraudster’s account with a reachable PSP
- Open Banking is a new eBanking channel and its only payment outcome is a Faster Payment
- The proposed “Request to Pay” service is an open invitation to invoice fraud, and its outcome is a Faster Payment
- The Bank of England’s policy to push payments they regard as not systemically important off CHAPS has led to a much higher Faster Payments system limit and in its train to frauds of much larger size

New Payments Architecture ("NPA") RfP process through New Payment System Operator ("NPSO") will not solve this



Lyddon
CONSULTING SERVICES LTD

Faster Payments central flaw

- **No name-check at the beneficiary bank on the coherence of the payee name as stated in the payer's payment order, with the name on the account associated with the Sort Code and Account Number that the payer gave in their payment order**
- **The processing at the beneficiary bank is on the Sort Code and Account Number alone**
- **Enables fraudsters to send invoices and payment requests quoting a legitimate name, but their own account details**
- **Since a Faster Payment is instant and irretrievable, the fraudsters clear out the beneficiary account straight away – without recourse!**

The circumstances around FPS' build led to this flaw

The business process is based on the one for card payments at Point-of-Sale

The PoS process was the only one that existed in all of the main banks for receiving, acting on and responding to a message in near real time

FPS was built at short notice to a fixed deadline – it used shreds and snatches of existing payment services

Field length for beneficiary name is limited to 18 characters (as is the reference field) – Standard-18

FPS uses the BACS Sort Code tables to identify reachable institutions

Key differences between PoS and FPS

Point-of-Sale	Faster Payments
Payer gets an immediate proof of discharge of their payment obligation	The payer gets no proof of discharge of their underlying obligation
Beneficiary can be relied upon to pay the money into their own account, and the set-up with their acquirer has this as an objective	Recourse on the payer exists right up to the point where the payee confirms receipt of good funds – which may be never
If it does not, it is acquirer error or merchant staff fraud	
Neither of these eventualities compromises the payer's discharge	

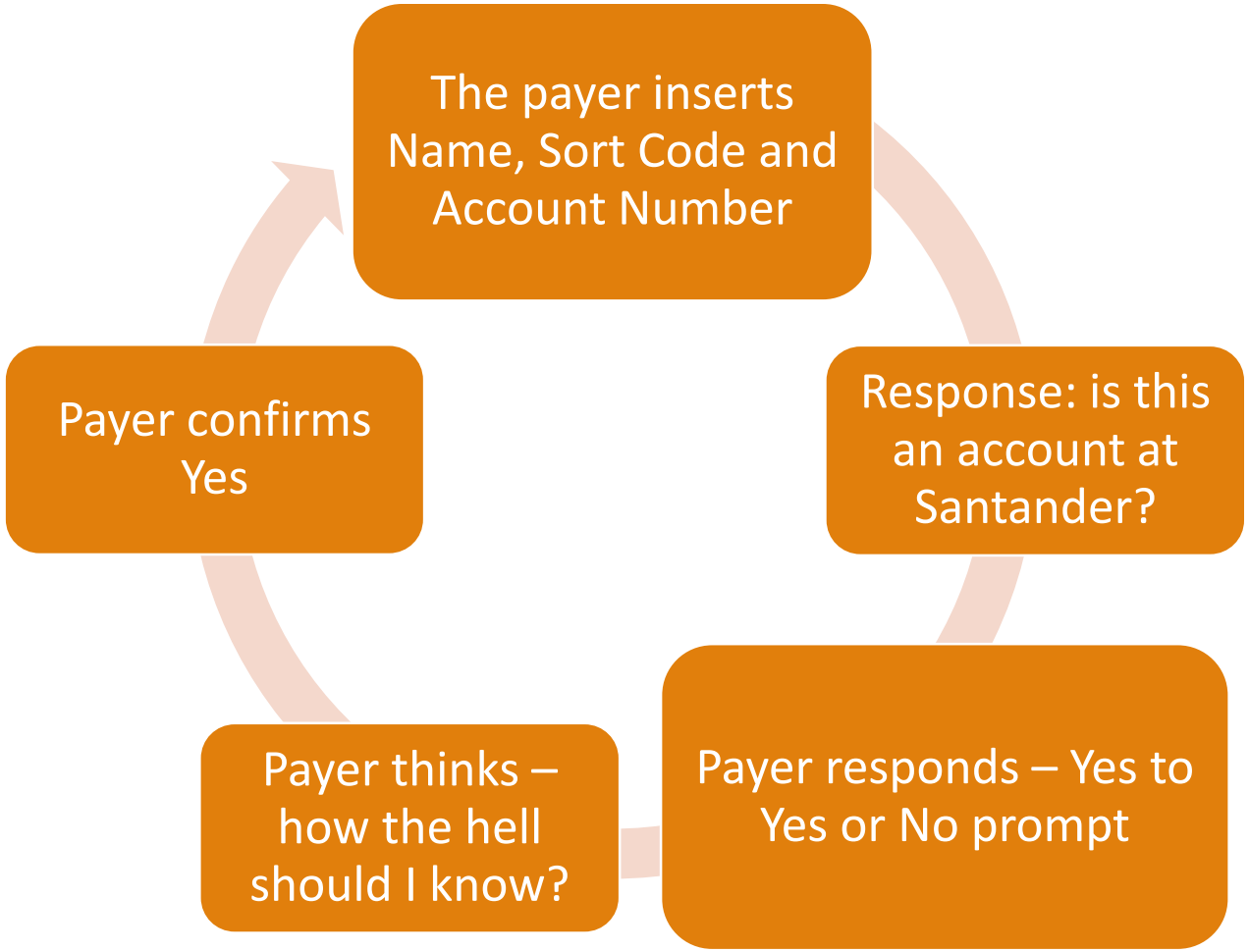
Comparison with a cheque and conclusions

Cheque
A cheque is crossed “Account Payee” so that it can only be paid into an account carrying the name the payer writes in the payee line
If the cheque is paid into a different account, the risk is on the payee and the banks – the payer is indemnified

Conclusions
The construction of FPS has left the payer wide open
The data that flows with the payment and the processing routines do not support adequate consumer protection

Flawed consumer protection measure #1 – when setting up a Lloyds payment template

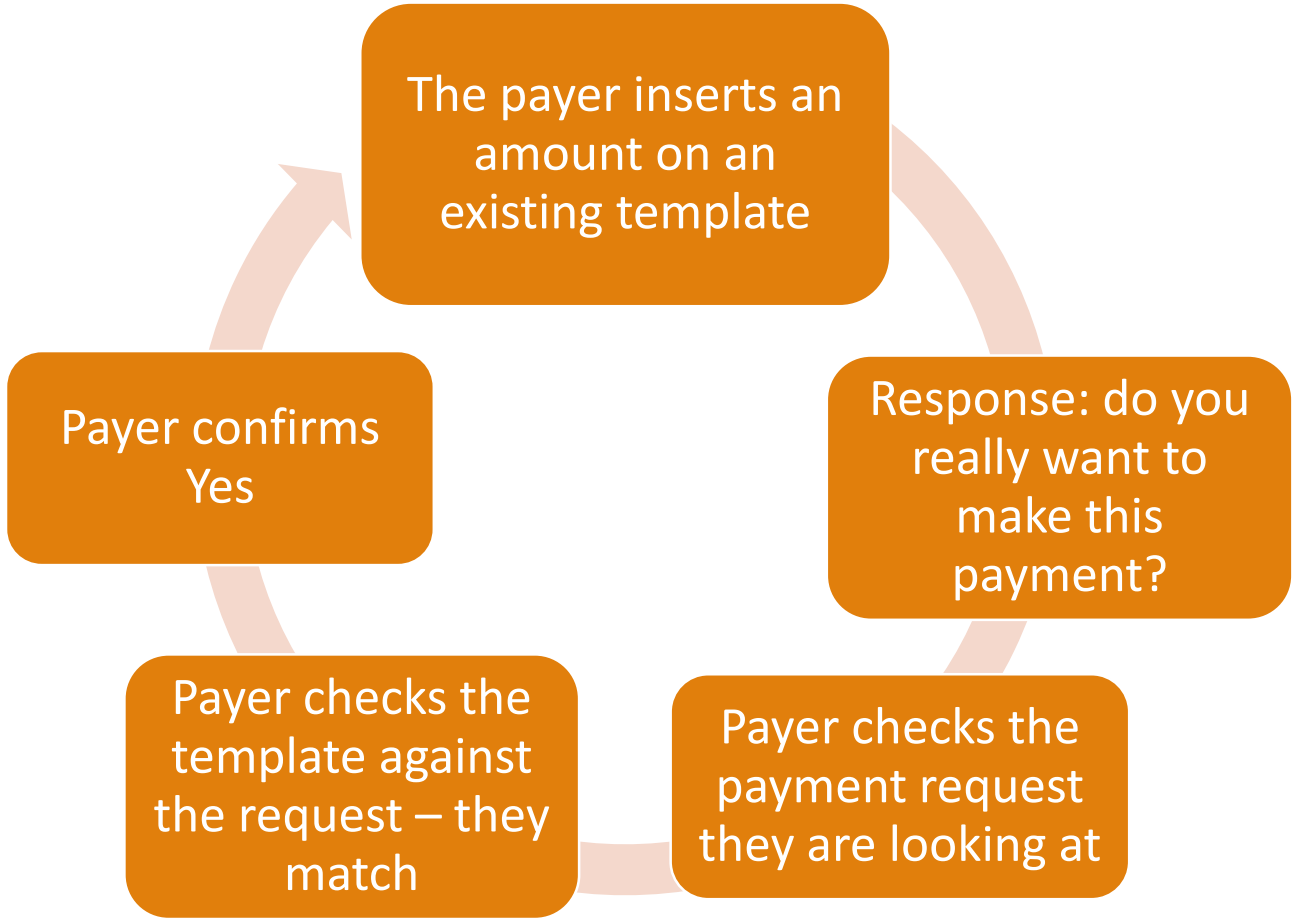
- The payer is invited to believe their bank made a check with the beneficiary bank
- Actually the check was with the BACS Sort Code table



Lyddon CONSULTING SERVICES LTD

Flawed consumer protection measure #2 – when confirming an individual payment by Lloyds

- The payer is looking at a fraudulent payment request
- The process disables the payer's legal protection that the payment was not authorised



Lyddon CONSULTING SERVICES LTD

PSD2 legal protections for the payer

- Blanket protection against unauthorized payments where:
  1. A “payment instrument” was used
  2. The payer’s Payment Service Provider cannot prove gross negligence on the part of the payer
- The interpretation of what a “payment instrument” is and what the security tokens and materials are that are used to authenticate payments initiated through eBanking channels currently deny this protection to push payments
- Indeed the usage of the materials (as per the preceding slide) is the proof that the payment was authorized, leaving the payer without legal protection

Current trajectory of UK fraud on Cards (which are “payment instruments”) sourced from Financial Fraud Action UK

- Fraud losses on cards totaled £566.0 million in 2017
- This was a year-on-year decrease of 8 per cent
- There were 1,874,002 cases (i.e. more or less meaning the number of victims) of card fraud
- The loss was £302 per case
- The Prevented Value of card fraud was an impressive £985 million

Breakdown of UK fraud on Cards sourced from Financial Fraud Action UK

Loss type	Amount of loss (£ millions)	Year-on-year change
Losses due to remote purchase fraud	409	-5%
Losses due to lost and stolen fraud	93	-4%
Card not received fraud	10	-19%
Counterfeit card fraud	24	-35%
Loss value on Card ID theft	N/A	-25%
UK face-to-face card fraud	N/A	-2%
UK cash machine fraud	N/A	-14%
Losses on domestic and international card fraud:		
• Frauds in the UK using overseas cards	N/A	-2%
• Frauds outside the UK using UK cards	N/A	-21%

Current trajectory of fraud on eBanking channels sourced from Financial Fraud Action UK

Channel	Prevented value	Total losses	Year-on-year change	Cases	Loss per case
Remote banking	£261 mil	£156 mil	+14%	34,743	£4,490
Internet banking	N/A	£121 mil	+19%	21,784	£5,554
Telephone banking	N/A	£28 mil	-4%	9,575	£2,924
Mobile banking	N/A	£6 mil	+10%	3,384	£1,773
Total	£261 mil	£311 mil		69,486	£4,475

- Fraud on eBanking Channels is rising sharply, except on Telephone banking – but that can be attributed to the fall in usage of that channel
- The payment system through which these frauds are completed is predominantly Faster Payments
- Open Banking is a new eBanking Channel that has been opened up in 2018

PSR 2017 Data on Authorised Push Payment Scams

	Personal	Non-Personal	Total
Total cases	38,596	5,279	43,875
Total victims	37,761	5,076	42,837
Total value	£107.5 million	£128.6 million	£236.0 million
Total returned to victim	£22.6 million	£38.2 million	£60.8 million
Total not returned to victim	£84.9 million	£90.4 million	£175.2 million

- £175.2 million was not returned to victims
- The average victim's loss was £4,090
- That is potentially life-changing
- The PSR's total did not have a line "Total not returned to victim": we had to extrapolate it

Lyddon CONSULTING SERVICES LTD

Summary of current payment fraud data sourced from Financial Fraud Action UK/PSR

Channel	Prevented value	Total losses	Cases	Loss per case
Total eBanking channels	£261 mil	£311 mil	69,486	£4,475
APP Fraud	£61 mil (returned)	£175 mil	42,837	£4,090
Card Fraud	£985	£566 mil	1,874,002	£302
Cheque Fraud	N/A	£10 mil	1,745	£5,616
Industry totals	£1,307 mil	£1,062 mil	1,988,070	£534

- The similarity of “Loss per case” under fraud on eBanking Channels and APP Fraud proves the correlation between the two
- The “Loss per case” for both types is very high, far higher than for Cards
- The “Prevented value” for APP Fraud is about 25% of the total fraud attempted of £236.0 million, whereas for Cards it is nearly 64%

Conclusions on current payments fraud

- On the basis of the data quoted the industry should not be pushing the uptake of eBanking channels to initiate Faster Payments, at the expense of Cash, and of Cards, Cheques, Direct Debits and all types of “pull payment” generally
- The amount limit for the Faster Payments system should be reduced, perhaps to £300 (the average loss on card fraud), and not increased
- But it isn’t even this good for the end user – these types of fraud are further distinguished by a simple question: **who eats the loss**?
    1. the Payment Service Providers in the case of Cards, absent proof of gross negligence by the cardholder
    2. the Payment Service Users in the case of eBanking channels initiating Faster Payments

Emerging “protections” for the Payment Service User against APP Fraud

Customer Awareness

- Generally has the effect of strengthening the PSP’s legal position against their customer

Contingent Reimbursement

- Much weaker than the PSD2 rights in the case of the usage of a “payment instrument”
- Contingencies can be expected to limit payouts to fraud victims in practice

Confirmation of Payee

- Originally an “overlay service” on top of New Payments Architecture
- Weak roll-out plan
- Uncertain reachability
- Will not be done on every payment

Confirmation of Payee

- Superficial solution, unless it is done on each and every payment
- Does not address the problem in the core – indeed it accommodates to it
- Why should the payer have to confirm the payee when they already stated it in their payment order?

97. Confirmation of Payee

CB stated that NPSO had put together a working group including representatives from all key stakeholders which had met to try to reach a consensus on legal issues including disclosure of personal data, fraud, PSD2, privacy and consumer protection. The next steps for the taskforce were as set out in the paper circulated ahead of the meeting.

Lyddon CONSULTING SERVICES LTD

Request to Pay ("RtP") – open goal for fraudsters

- Another "overlay service" on top of NPA that end users have apparently been keen to have since 2014
- End users receive a bill with a button on it that they can click, and that takes them into an eBanking Channel and they can settle the bill with a Faster Payment
- Where is the protection against spurious bills?
- No new service could have been conceived that plays so gloriously into the vulnerabilities of both Faster Payments and of the controls and policies at the Payment Service Providers that offer the Faster Payments service

NPA and Faster Payments within in it

Elevation

- Faster Payments becomes the main retail payment system for direct usage
- It will receive the investment; cheque, giro credit, BACS Credit and Direct Debit will wither on the vine

Single Settlement Layer

- Faster Payments becomes the universal settlement layer for itself and for cheque, giro credit, BACS Credit and Direct Debit
- This creates a single point of failure where none exists now

Non-systemically important payments

- Accommodates to the Bank of England's policy to move payments off CHAPS
- The Faster Payments system limit has been progressively raised to enable this…
- Much to the delight of APP fraudsters

NPA as a whole

- NPA is an unproven concept that greatly depends on questionable and unchallenged contentions made by the Horizon Scanning Working Group of the Payment Strategy Forum Phase 1
- This WG was meant to act as an advisory resource to the other three Working Groups, to whom the “detriments” had been allocated for examination and solution
- These detriments were the ones agreed upon in the Community Event in September 2015
- Horizon Scanning had no detriments allocated to it: its tasks were to look at technological, legal&regulatory and geographical developments across the entire field of the Forum’s work, and to advise the other Working Groups of their existence and significance

Failure of Horizon Scanning to scan the horizon

- Instead of discharging its Terms of Reference, the Horizon Scanning Working Group issued a triage document, shut up shop regarding leg&reg and geographical developments, and made its claims about its ability to solve everything through technology:

While the Geographic and Regulatory Horizon sub-groups are meant to bring to the attention of the Forum, the future developments and initiatives and business models in other countries so that this is taken into account in the UK, the Technology Horizon is focused in identifying what technologies could be adopted to address the detriments of the current payments systems and experienced by service users.

In this sense the Technology Horizon sub-group has found that an overwhelming high number of detriments could be solved with a mix of these technologies and concepts:

- Blockchain
- Distributed ledger
- APIs
- Layer Modelling
- Identity Management

Summary

- NPA should be coolboxed, and preferably very deeply
- Faster Payments has a central flaw which should be remedied as an absolute priority
- Confirmation of Payee is a distraction which serves only as a Confirmation of Vulnerability
- In the meanwhile Faster Payments should neither be:
    1. The receptacle of the payments that the Bank of England wants to move off CHAPS
    2. Elevated in importance above other payment systems
    3. The universal settlement layer for retail payments
    4. The basis for further new payment products like Request to Pay