Written evidence for the Treasury Select Committee Inquiry into the Payment Systems Regulator regarding the proposed "Confirmation of Payee" service and Authorised Push Payments Fraud

Submitted by: Bob Lyddon, Director of Lyddon Consulting Services Ltd
(www.lyddonconsulting.com)

Date: 17th September 2018

Introduction

What is Lyddon Consulting?
A specialist consultancy in payments and electronic banking. We have recently acted as advisor regarding the UK payments landscape to a trade body representing UK Payment Institutions and to a major payments communications cooperative reviewing their UK market positioning.

Why this evidence is being submitted:
We have consistently pointed out the divergence between the PSR's plans and actions, and the actual problems besetting the UK payments landscape. We believe that the action plan and proposed solutions to Authorised Push Payments Fraud ("APP Fraud") as presented by PSR in oral evidence to the Treasury Select Committee in early 2018 will either not be solutions, or will arrive far later than the PSR has represented.

In particular "Confirmation of Payee" is unlikely to be available in proper production before 2025: all UK Payment Service Providers need to be reachable through it for it to have any value.

APP Fraud is one of the problems that falls within the scope of Project Carlton, a research project on which we are lead consultant. The initial phase of Project Carlton provides an overview of the multiple failures and mistakes made in UK payments landscape since 2014. This overview is being socialised in the payments marketplace now with a view to creating an interest group and a business case for a change in direction. What we have set out below is substantially drawn from the Project Carlton research.

Opinions
Where we express an opinion, we believe we can bear it out with reference to the full Project Carlton research.

Contact details
Lyddon Consulting Services Ltd
14 Portsmouth Avenue
Thames Ditton KT7 0RT

07939 – 132341

bob@lyddonconsulting.com

Submission

Executive Summary:

- Confirmation of Payee will not exist in 2018: it is on the drawing board.
- Indeed it is dependent upon the existence of New Payments Architecture ("NPA"), which is unlikely to exist in stable form until 2025, notwithstanding what the PSR has told the committee.
- NPSO, not the PSR, is responsible for delivering NPA and CoP, and their actions indicate a very large project.
- CoP is not definitely feasible from a legal & regulatory point of view and it does not resolve the central flaw that has opened the door to APP Fraud: the lack of a name-check in the Faster Payments processing at beneficiary banks.
- NPA does not address this flaw either, but it does elevate Faster Payments to being the main retail payment system and also the settlement mechanism for the other retail payment types: this threatens to exacerbate the APP Fraud problem, not resolve it.
- NPA envisages retail payments principally being initiated in an eBanking channel and completed via a Faster Payment: this is the exact model within which APP Fraud arises.
- The PSR's supposed remedies to APP Fraud are non-specific, and lacking in certainty as to their timing and their effectiveness.
- Most were already underway before Which? lodged its supercomplaint.
- The PSR presents volume of work, number of workstreams, and progress against the workplan as proof of success, as against going to the heart of the matter, identifying important correlations, and crafting specific responses to the core problem.
- The PSR has failed to identify the correlation between fraud using eBanking channels and APP Fraud: we have demonstrated that they are closely correlated.
- Open Banking is yet another eBanking channel, out of which the available payment type is a Faster Payment.
- The direction of the industry, fostered by the PSR, is towards the model of eBanking channel + Faster Payment, even though the average eBanking/APP Fraud is over £4,000 when the average Card fraud loss is £302.
- In addition the 2017 Payment Services Regulations make the PSP responsible for Card fraud losses, unless the PSP can prove gross negligence on the part of the cardholder.
- Under APP Fraud, though, it is the payer who takes the majority of the loss.
- The direction of the industry - as presided over by the PSR and their creatures the Payment Strategy Forum and New Payment System Operator - needs to change dramatically.

1. Confirmation of Payee or "CoP" and its dependency on New Payments Architecture

1.1. The PSR led the TSC to believe, in the January hearing, that the CoP service would exist for sure this year and make a major contribution to solving the APP Fraud problem.

1.2. CoP will not exist this year as a service, widely available, and in stable production. CoP is an "overlay service" that will sit on top of the New Payments Architecture ("NPA") which is being designed by New Payment System Operator ("NPSO"). Appendix 1 confirms this: it is drawn from the NPA Blueprint document of July 2018.

1.3. CoP cannot come into being before NPA. NPA is in the quite early stages of design at NPSO. The PSR knows this: its Open Letter to NPSO of 18th January 2018 confirms the understanding that NPSO is in charge of developing and delivering NPA.

2. NPA timeline and the timeline of the most comparable project

2.1. NPSO sent a response dated 28th March 2018 to the PSR's Open Letter referred to in 1.3 above. The response listed a large number of pieces of work to be carried out but gave no estimated live date for NPA.

2.2. The PSR, in their oral evidence to the TSC in January 2018 against question 33, first stated that CoP "will definitely be part of the new payments architecture that will be in from 2020 (2)". The (2) refers to a "Clarification from witness: The new payments architecture will be in place from 2021". We regard that timeline as very optimistic and NPSO has not committed to it.

2.3. NPA involves a transition to a new data format called ISO20022 XML. The main implementation of ISO20022 XML is for the Single Euro Payments Project, or "SEPA".

2.4. The equivalent body to NPSO for SEPA – the European Payments Council - was established in 2004. The first SEPA product went live in 2008, and the migration was completed in 2016 – with the force of a 2012 EU regulation behind it (the SEPA Migration End Date Regulation No 260/2012). There were migration projects at the levels of the Clearing & Settlement systems, at the Payment Service Providers ("PSPs") and at major business and public authority users, which were extensive and requiring of intricate coordination.

2.5. NPSO was founded a year ago. If NPSO can work to the same timescale as the European Payments Council, we could expect to see the infrastructure level of NPA established with a basic product (i.e. a Faster Payment) available on it between major banks in 2021, after which the remaining PSPs can be brought on, after which the end users can be migrated. That takes us to 2025 in a likely scenario and NPA can then be said to exist. After that, new "overlay services" – like CoP – can be contemplated.

3. Scale and timing of NPA project as indicated by NPSO actions

3.1. The scale of the project is indicated by the number of advisory groups that NPSO is setting up to help it define NPA – nine: https://www.newpso.uk/advisory-groups-for-new-payments-architecture-start-recruitment/

3.2. We can also appreciate the timescale on the basis of the delays requested by NPSO's subsidiaries to the dates for the implementation of the remedies that the PSR set in its Market Review on Infrastructure Provision behind BACS, Faster Payments and LINK.

3.3. These payment systems should put their provision out to competitive tender and the new solution should use ISO20022 XML. BACS has sought a delay of 3 years, with an option to roll its contract with Vocalink beyond the contract's current end date.

3.4. Faster Payments has sought a delay of 2 years with an option to extend that by six or twelve months. (See Appendix 2 for an extract from the NPSO Board Minutes attesting this).

4. Status of development of CoP itself

4.1. NPSO put out a "call for industry views" on 23rd July 2018 regarding the initial CoP logical Application Programming Interface specification: https://www.newpso.uk/npso-calls-for-industry-views-on-initial-confirmation-of-payee-api-specification/

4.2. The methodology being used to develop new services on NPA is the same as that which was used to develop the SEPA services, and it starts with a specification of the business model using Universal Modelling Language: this is a logical specification.

4.3. In brief this sets out who the "actors" are in the service, what task each one does at each stage in the business process, what input data they need to carry out the task and who from, and what data they output from the task and who to.

4.4. Once all these data flows have been mapped out and agreed, the actual messages in the ISO20022 XML data format can be specified and agreed. The final outputs are a service rulebook and a message usage guidelines ("MUG") document. CoP is at the very start of that process. The ISO20022 XML messages needed to support it may not yet exist, in which case they will have to be submitted into the ISO20022 XML registration process.

4.5. Once the rulebook and MUG are complete, they have to go through development, testing, implementation, conversion, roll-out and post-conversion support at many market actors individually and in multi-actor testing phases, before the new service can be rolled out and then said to exist "in stable production".

4.6. There will also be legal agreements to complete. The European Payments Council now has a comprehensive "Adherence Pack" for new participants in SEPA, and all of that will have to be produced for CoP:
https://www.europeanpaymentscouncil.eu/what-we-do/participating-schemes/toolkit-new-scheme-participants

5. CoP is not definitely feasible from a legal and regulatory perspective

5.1. CoP also stands some way from certainty that the service is even feasible from a legal and regulatory point of view.

5.2. The NPSO Board Minutes of 2nd May 2018 against point 97 contained a significant list of issues of a legal/regulatory nature that stand in the way of CoP: "disclosure of personal data, fraud, PSD2, privacy and consumer protection" (see Appendix 3).

6. CoP does not resolve the key flaw that has opened the door to APP fraud

6.1. A flaw in the original design of the Faster Payments system is the door that has admitted APP fraud.

6.2. Faster Payments was built around the process for debit card payments at Point-of-Sale because, at the time, this was the only process at the major banks for receiving a message, processing it and sending a response in real time.

6.3. Faster Payments uses the ISO8583 data standard – the same one as is used for Card payments.

6.4. In a card transaction at Point-of-Sale the payer's name is not captured because the transaction is processed through to the cardholder's bank on the card number and other digital details captured by the terminal, and authenticated by PIN.

6.5. Nor is there a need to capture the beneficiary name in the terminal: the merchant and their acquirer ensure the money goes into the merchant's account.

6.6. In Faster Payments there is a need to capture the beneficiary name, and indeed the payer does complete their payment order in an eBanking channel, inserting the beneficiary's name to the extent possible when the field length is limited to 18 characters.

6.7. But this name is not processed at the beneficiary bank: there is no check on the coherence of the beneficiary 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.

6.8. The processing at the beneficiary bank is on the Sort Code and Account Number alone, just as the processing at the cardholder's bank in a PoS transaction is done on the card number and digital details captured in the terminal.

6.9. This enables fraudsters to send invoices and payment requests quoting a legitimate name, but their own account details to which a Faster Payment can be directed.
6.10. Since a Faster Payment is instant and irretrievable, the fraudsters receive the fraud proceeds into the beneficiary account straight away, and clear it out straight away.
6.11. CoP does not resolve this flaw; indeed it accommodates to it by adding a process in which the payer is asked to repeat what they already put in their payment order – the name of the intended beneficiary.
6.12. The NPA Blueprint does not contain a provision to eliminate this flaw.

7. Under NPA, Faster Payments becomes the main retail payment system and the settlement system for the others

7.1. Under NPA, the core method of making a payment would be by the payer using an eBanking channel (PC, tablet, mobile phone, Open Banking) and initiating an instant "Push Payment", namely a Faster Payment
7.2. The channel of initiation and the method of completion are tightly coupled in the NPA conceptual model.
7.3. Faster Payments is thereby elevated to being the main retail payment system (see NPA Blueprint of July 2018), as it completes the payments initiated in an eBanking channel.
7.4. NPA foresees payers progressively migrating to using eBanking channel + Faster Payment.
7.5. NPA does not contain a plan to retire the other retail payment types (Direct Debits, BACS Credits, cheques and bank giro credits) but it does envisage Faster Payments acting as the settlement system for them.
7.6. These other services become "overlay services" on top of Faster Payments, in just the same way as CoP is proposed to be.
7.7. Migrating more payments to Faster Payments both directly and indirectly makes it unlikely that Authorised Push Payments Fraud will fall, unless the core flaw at the centre of Faster Payments is eliminated.
7.8. Reversing the direction-of-travel would be contrary to what the PSR has worked towards since it was established, and it would cancel the outcome of the Payment Strategy Forum, which the PSR established to plot out the future direction. That outcome is NPA with its array of "overlay services".

8. **CoP will only be effective when all PSPs and customers are reachable**

8.1. CoP must be adopted by all PSPs in the UK in order to be effective at any.
8.2. There can be no opt-out at the customer level: every bank account in the UK must be reachable or else fraudsters will simply opt out. The legal and regulatory obstacles to CoP no doubt include overcoming the customer's privacy and data protection rights.
8.3. Every PSP must be able to act as confirmer on behalf of its payer customers, to confirm payee details at a different PSP.
8.4. And every PSP must be able to act as confirmee, confirming the details of their payee customers back to the PSP of the payer customer.
8.5. Assuring universal reachability is the same difficult task as occurred in SEPA. It required European legislation to compel PSPs to become reachable (EU Regulation 924/2009).
8.6. In the case of a service like CoP and in the absence of complete reachability, fraudsters would target the PSPs that were unable to support CoP, up until the final PSP was able to.
8.7. If CoP cannot even begin roll-out until NPA is in stable production, and if that only occurs in 2025, then the SEPA experience would indicate a multi-year timeline from then.

9. **The PSR's output on APP Fraud lists many streams of supposedly relevant work**
   9.1. The PSR has held out CoP as one of the Prevention measures and "Starting 2018" in its document dated 21st June 2018 "PSR work on authorised push payment scams".
   9.2. This is consistent with the report they issued under a press release dated 7th November 2017 (see Appendix 4).
   9.3. The graphic on page 5 of that report (see Appendix 5) shows 4 measures under "Prevention", 4 under "Response" and 3 under "Outcome and follow-up" – 11 streams in all and, on the face of it, an impressive package of work.
   9.4. In common with most PSR outputs, progress is measured against the completion of the work set by the PSR for itself, not against progress in resolving the underlying problem.
   9.5. There is no proof that these workstreams will definitely resolve the problem, how and by when. Instead they promise to eat at the edges, and they may have some mitigating impact at some future point. The sheer volume of work that the PSR sets for itself replaces specificity and certainty. The work fails to address the root cause of the problem.
   9.6. The PSR's initial December 2016 response to the Which? authorised push payments super-complaint did explain in point 8.5 that "As set out in Chapter 7, there is a significant programme of work already under way that has the potential to reduce consumer harm caused by APP scams" and went on in point 8.6 to say that "In developing our proposals, we have been mindful of not taking action that either duplicates existing work or that could have the effect of frustrating this work. That said, there are clear interactions between the actions we propose below and some of the initiatives already under way. In implementing our proposals, we will ensure any interactions are managed effectively".
   9.7. This is hardly the same as admitting, though, that 6 of the 11 streams had already been underway within the PSR's "Payment Strategy Forum" or "PSF" and for over a year, and indeed that CoP had been underway since 2014 in the "World Class Payments Project" (see Appendix 6 for the respective graphic from the interim project report "A report on how customers around the world make payments").
   9.8. Two more streams have significant question marks against them, as explained in Appendices 7 and 8.
   9.9. Finally, it is not just CoP that is dependent upon NPA – Transaction Data Analytics is also.
   9.10. Here is the full list of the PSF's action streams towards APP Fraud:

Stream Name	Derivation
Customer Education & Awareness	PSF – Financial Crime stream
Guidelines for identity verification, authentication and risk assessment	PSF – Financial Crime stream
Trusted KYC Data Sharing	PSF – Financial Crime stream
Confirmation of Payee	PSF – Meeting End User Needs Stream
UK Finance's best practice standards	New
Information sharing in response to scams	See Appendix 6
Financial crime data and information sharing	PSF – Financial Crime stream
Transaction Data Analytics	PSF – Financial Crime stream
Joint Fraud Taskforce's recovery of funds	See Appendix 7
Contingent reimbursement	New
Collection and publication of APP scam statistics	New

10. **Scale of APP Fraud**
    10.1. All figures used in this submission are based on the data in the "2017 annual fraud update" published jointly in March 2018 by Financial Fraud Action UK and UK Finance.
    10.2. Figures on APP Fraud were given in that update without comparison to previous years and without extrapolating the loss to victims (i.e. the total of APP fraud less the amounts returned).
    10.3. We have given – in Appendix 9 – both the version in the report and our extrapolation.
    10.4. £175.2 million was not returned to victims.
    10.5. The average victim's loss was £4,090.
    10.6. That is potentially life-changing.

11. **Amount that can be lost**
    11.1. The amount that a payer can lose is limited only by the lower of (i) the ceiling on the size of payment that the payer's PSP imposes on the eBanking channel through which the payer is initiating the payment, and (ii) the Faster Payments system limit - the maximum size of payment that can pass through the Faster Payments system itself.
    11.2. The Faster Payments system limit was £25,000 at launch.
    11.3. A PSP might typically have set its ceilings as (a) £10,000 for their Personal Internet Banking system and (b) £15,000 for their Business Internet Banking system.
    11.4. The fact that ceilings were set by PSPs in eBanking channels that related to the Faster Payment system limit proves how correlated eBanking channels are with the completion of a payment via Faster Payments.
    11.5. The Faster Payments system limit – and the ceilings in eBanking channels – have risen in line with the Bank of England's policy to remove from the CHAPS system those payments that it does not view as systemically important.
    11.6. This has had the effect of increasing the amount that can be taken in an APP Fraud.
    11.7. This policy at the Bank of England should be reviewed.

12. **Trajectory of fraud on Cards**
    12.1. The NPA vision is that payments are increasingly made via credit transfers i.e. authorised push payments initiated in eBanking channels.
    12.2. This will be at the expense, inter alia, of payments by Card.
    12.3. However Cards fraud is falling – see Appendix 10 for detail.
    12.4. There were 1,874,002 cases in 2017 (i.e. more or less meaning the number of victims).
    12.5. The loss was £302 per case.
    12.6. The Prevented Value of card fraud was £985 million.
    12.7. Since a card counts as a "payment instrument" under 2017 Payment Services Regulations (the UK transposition of the EU's 2nd Payment Services Directive), it is the PSP that takes the loss, unless the PSP can prove gross negligence on the part of the payer.

13. **Trajectory of fraud through eBanking channels**
    13.1. Financial Fraud Action UK and UK Finance track fraud through various eBanking channels.
    13.2. This type of fraud is rising sharply.
    13.3. The loss on remote banking fraud rose by 14% in 2017.
    13.4. The loss value on internet banking fraud rose by 19%.
    13.5. The loss value on telephone banking fraud fell by 4% (but possibly because of the falling usage of this channel).
    13.6. Mobile banking fraud rose by 10%.

13.7. The full picture can be ascertained from this compilation of the figures:

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

14. **Failure to identify correlation of APP Fraud with fraud through eBanking channels**
    14.1. The PSR has failed to take account of the fact that a significant portion of fraud through eBanking channels is completed by the fraudster procuring that a Faster Payment is made in their favour.
    14.2. The initiation channel for an APP Fraud and the method of its completion are strongly correlated, with the loss per case being something over £4,000 in both instances:

Channel	Prevented value	Total losses	Cases	Loss per case
Total eBanking channels	£261 mil	£311 mil	69,486	£4,475
APP Fraud	£61 mi (returned)	£175 mil	42,837	£4,090
"New methods" totals	£322 mil	£486 mil	112,323	£4,327

15. **Addition of eBanking channel – Open Banking**
    15.1. Open Banking is a new eBanking channel.
    15.2. The payment option available under Open Banking is a Faster Payment, as per the standards https://www.openbanking.org.uk/providers/standards/
    15.3. Open Banking can only add to APP Fraud.

16. **Who bears the loss?**
    16.1. The PSR has failed to adequately distinguish between Cards fraud and APP Fraud on the issue of who ultimately bears the loss.
    16.2. As Cards are a "payment instrument", it is the PSP who takes the loss unless they can prove gross negligence on the part of the payer.
    16.3. The average loss per case on Cards is £302, which is unpleasant but – for most – not life-changing.
    16.4. The losses on APP Fraud/eBanking fraud are potentially life-changing and it is currently the payer that bears most of the losses.
    16.5. One would be forgiven, we believe, for being sceptical about the proposed Contingent Reimbursement Scheme, simply because it is contingent.
    16.6. Equally the controls that banks have implemented so far have ensured that the victim of an APP Fraud will have used their "payment instrument" (a card, a terminal etc.) to authorise the payment and then to confirm authorisation, thus disabling any legal protection they have under 2017 Payment Services Regulations.

Recommendations

1. New Payments Architecture to be coolboxed and replaced with a project to eliminate the flaw at the heart of the Faster Payments system: the beneficiary bank must check the payee name in the payment they received, against the name of the account associated with the sort code and account number in the payment.
2. The Faster Payments limit could theoretically be cut to £300 until the central flaw was eliminated. The maximum customer loss on APP Fraud would then be the same as on Card fraud. However, this would be a revolutionary step and throw into reverse gear the direction of the UK payments landscape bus ever since Faster Payments was conceived.
3. Fraud tracking must include Open Banking as an eBanking channel and recognise the correlation between eBanking fraud and APP Fraud.
4. A legal change should be considered to apply the same legal protection to the payer using as eBanking channel as they have when they use a card: the PSP is responsible unless the PSP can prove gross negligence.
5. If payer has a claim on their PSP when it is the beneficiary PSP that is at fault (for opening account for a fraudster), the payer's PSP would have to be indemnified by the payee's PSP.
6. In the meantime the FCA should take a much firmer line with the PSPs who have opened accounts for fraudsters. This is a failure of their Customer Due Diligence processes under Anti-Money Laundering regulations. The PSPs are handling the proceeds of a crime when an account in their books is used for an APP Fraud. This is a predicate offence for money laundering so the PSP that has opened the account for the fraudster should have Money Laundering sanctions imposed upon them, and the FCA should lead the way on that.
7. Lastly, the Bank of England should be lobbied to reverse its policy of pushing systemically-important payments off CHAPS and to re-scope its own "RTGS Renewal" project accordingly.

BL/17.9.18

Appendices

Appendix 1 – extract from page 5 of the New Payments Architecture Blueprint document put out to consultation in July 2018 positioning Confirmation of Payee as an "overlay service" in the final bullet point

The key features of the NPA are:

- A layered approach, with a 'thin' collaborative infrastructure to enable competition and innovation.
- A single set of standards and rules with strong central governance.
- Adoption of the common, international messaging standard, ISO 20022, to enable access, innovation and interoperability, both in the UK and potentially for international connectivity.
- Security and resilience, with financial stability a key principle.
- The use of 'push payments' to enable simplicity and increase customer control.
- Flexibility built into the design to support a range of new end-user overlay services such as Request to Pay and Assurance Data (including Confirmation of Payee).

Appendix 2 – extract from NPSO Board Minutes of 4th April 2018 **attesting to delays in adoption of ISO20022 XML requested by NPSO subsidiaries**

82. IMR Competitive Procurement Remedy - Extensions

The paper was taken as read. DM said the PSR sought implementation of a remedy for Bacs and FPS, to ensure that competitive procurement takes place. Bacs and FPS intend to seek extensions to the remedy by mid-April 2018. Bacs is seeking a three year extension and

6

PUBLIC CIRCULATION

Bacs have the option to roll the contract beyond its end date. FPS is seeking a two year extension, with an option to extend by six or twelve months.

The Board was comfortable with the position regarding the extensions.

Appendix 3 - NPSO Board Minutes of 2nd May 2018 point 97 - legal/regulatory obstacles that stand in the way of CoP

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.

Appendix 4 – PSR's announcement of their report on reducing APP Fraud

Payment Systems Regulator sets out progress on work to tackle payment scams

Published | 07 11 2017

- PSR reports progress on key industry initiatives it has led that should boost consumer protection and reduce harm from APP scams
- PSR is now consulting on how to deliver a scheme that would see victims of scams reimbursed
- Vital that regulators, industry, and consumers work together to make a difference

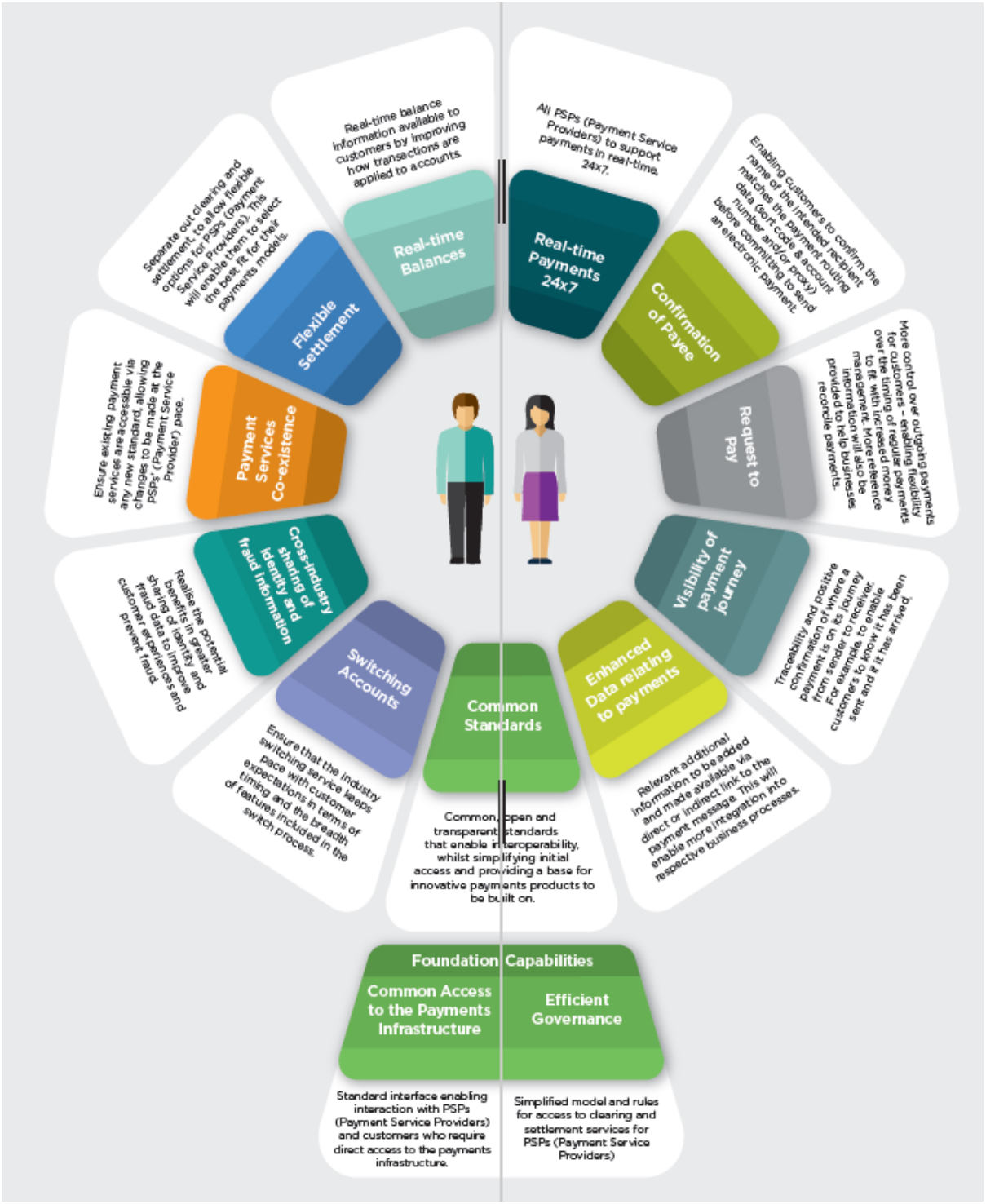
The Payment Systems Regulator (PSR), the economic regulator for the £75 trillion UK payment systems industry, has today published a report on its work to protect consumers from authorised push payment (APP) scams – where people are tricked into sending money to a fraudster. The report shows that good progress is being made across a wide range of initiatives and areas.

The report explains the work the PSR has led, working with the Financial Conduct Authority (FCA) and industry over the past year to reduce the harm from these scams. It highlights the range of industry measures it has overseen – some in place now, others to follow – which will deliver benefits to consumers. The PSR is also today launching a consultation on a 'contingent reimbursement model' it believes should be introduced to compensate victims in certain circumstances. All this work should, together, lead to better protection from scams and better support for victims.

Appendix 5 – graphic from page 5 of the PSR's November 2017 report on reducing APP Fraud

Figure 1: Measures to assist with APP scam prevention and response

Appendix 6 - graphic from the interim project report "A report on how customers around the world make payments showing "Confirmation of Payee"



Appendix 7 – PSR Response "Information sharing in response to scams"

Page 15 of the PSR's report gives more detail against "Information sharing in response to scams" and states:

> **Improved information sharing**
>
> **3.19** The industry has made good progress in developing a common understanding of what information can be shared between PSPs under the current law, for the purposes of processing APP scam claims. This is on the basis of the provisions of the Data Protection Act 1998. This common understanding on information sharing underpins the best practice standards.
>
> **3.20** However, there is still work to be done on other aspects of information sharing and in relation to the recovery of victim's funds. Addressing these issues may require legislative change or developments.
>
> **3.21** UK Finance is seeking to ensure that PSPs can continue sharing relevant information under the best practice standards when the new Data Protection Bill becomes law. The new provisions are due to come into force by May 2018 and will replace the Data Protection Act 1998.
>
> **3.22** UK Finance has stated that, in the immediate future, it will be seeking to agree a privacy impact assessment and put in place a data-sharing agreement between its member PSPs (with the involvement of the Information Commissioner's Office (ICO) as appropriate). The data sharing agreement is intended to set out the basis upon which the PSPs will share information and the processes they will follow when doing so. UK Finance has also agreed to explore and progress any legal changes or developments that they believe are needed to continue to share relevant information when the Data Protection Bill becomes law.

In other words:

- This is still a work-in-progress;
- Progress could be reversed by GDPR;
- Legislative change may be needed;
- No certainty that this will materialise or when;
- No certainty that this will have an impact on APP Fraud when it was conceived with different objects in mind.

Appendix 8 – PSR Response "Joint Fraud Taskforce's recovery of funds"

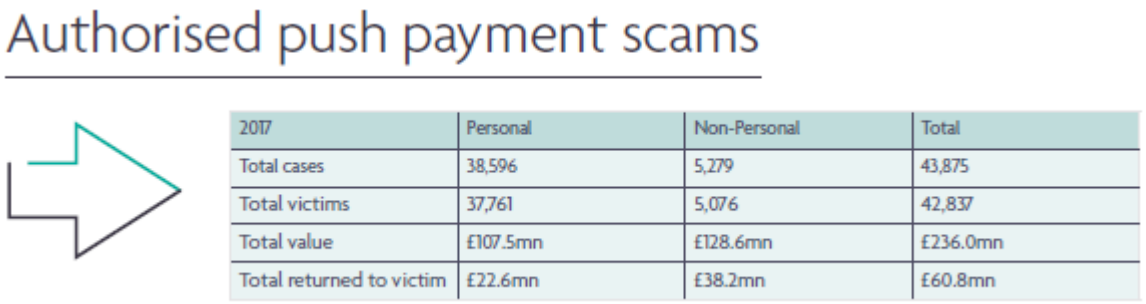
Page 15 of the PSR's report also gives more detail against "Joint Fraud Taskforce's recovery of funds", and states: "In relation to the recovery of victim's funds, the Joint Fraud Taskforce, and UK Finance as part of it, is developing a framework for a funds repatriation scheme – so that stolen money can be tracked across payment systems, frozen, then returned to the victim of the crime (see the box on page 25 regarding the recovery of victim's funds). This may require legislative change."

In other words:

- It is not the PSR doing this;
- It is at the development stage;
- It may require legal change;
- There can be no certainty that it will occur or when.

Appendix 9 – APP Fraud figures of Financial Fraud Action UK and UK Finance and our extrapolation

Financial Fraud Action UK and UK Finance rendition:



2017	Personal	Non-Personal	Total
Total cases	38,596	5,279	43,875
Total victims	37,761	5,076	42,837
Total value	£107.5mn	£128.6mn	£236.0mn
Total returned to victim	£22.6mn	£38.2mn	£60.8mn

Our extrapolation:

	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

Appendix 10 – Cards fraud commentary

Fraud losses on cards totalled £566.0 million in 2017, a decrease of 8 per cent on 2016.

There were 1,874,002 cases (i.e. more or less meaning the number of victims) of card fraud so the loss was £302 per case. The Prevented Value of card fraud was an impressive £985 million.

Within the overall figure for Cards…

- Losses due to remote purchase fraud fell by 5 per cent to £409.4 million in 2017;
- Losses due to lost and stolen fraud fell by 4 per cent in 2017 to £92.5 million, though the number of incidents increased by 51 per cent;
- Card not received fraud losses fell by 19 per cent to £10.1 million;
- Counterfeit card fraud losses fell by 35 per cent to £24.2 million;
- The loss value on Card ID theft fell by 25%;
- UK face-to-face card fraud fell by 2%;
- UK cash machine fraud fell by 14%;
- Losses on domestic and international card fraud fell by 2% in the UK (frauds in the UK using overseas cards) and by 21% overseas (frauds outside the UK using UK cards).