

General directions for the  
implementation of  
Confirmation of Payee

Responses to consultation

May 2019

# Contents

Anonymous 1	4
Anonymous 2	8
Association of Independent Risk & Fraud Advisors (AIRFA)	14
The Association of Corporate Treasurers	31
Atom Bank	36
Bank of America Merrill Lynch	46
Barclays	48
British Retail Consortium (BRC)	61
Building Societies Association (BSA)	63
CashFlows	71
CBI	75
Clydesdale Bank PLC	79
Dudley Building Society	82
Electronic Money Association (EMA)	84
Emerging Payments Association (EPA)	95
Experian	100
HSBC Bank PLC	107
HSBC UK Bank PLC	112
Information Commissioner's Office	130
Industrial Bank of Korea	132
Link Asset Services	135
Lloyds Banking Group PLC	140
Member of the public	151
National Trading Standards (NTS)	153
National Westminster Bank PLC	157
Nationwide Building Society	168
Open Banking Implementation Entity	177
Ordo	184
Santander UK, plc	191

Secure Trust Bank	195
Societe Generale	201
SWIFT	207
Transpact	211
TSB Ltd	216
UK Finance	233
Ursa Finance	242
Virgin Money	246
Visa	250
Which?	257
WorldFirst	263
Worldpay	265
Yorkshire Building Society	267

Names of individuals and information that may indirectly identify individuals have been redacted.

# Anonymous 1

## PSR Questionnaire

**Question 1:** Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?

**Answer:** We agree that this is one approach but seems complex and difficult to implement in the time frame. Another way would be to implement a process whereby the receiving bank checks the name and the account number match prior to the credit being processed.

**Question 2:** Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?

**Answer:** Directions should be directed at the participants (member banks) of CHAPS & Faster Payments. Considering the proposed process covers 24/7, 365 days a year it would not be possible for an agency bank like us to implement in the time frame suggested. Currently our systems are open Monday to Friday between 8.00 & 18.00.

**Question3:** Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?

**Answer:** Yes the participants (member banks) should be subject to a requirement to respond to a CoP request as those that are required to send a request. A Partial solution should be designed for agency banks because of the different business hours they have.

**Question 4:** Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?

**Answer:** Makes sense to offer directions for both FPS and CHAPS, but in our view BACS should also be included.

**Question 5:** Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?

**Answer:** If CoP is implemented it makes sense to all payment channels but consideration should be made for agency banks.

**Question 6:** How should any directions deal with the potential for people to opt out of the CoP process?

**Answer:** The idea of CoP is to reduce the amount of fraud in the market why would you want anyone to opt out as long as confidentiality is guaranteed.

**Question 7:** Should any directions cover the sending of money from both individual and business accounts?

**Answer:** We believe it should. We only hold business accounts but this is definitely an issue which has affected our customers.

**Question 8:** Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding? Should directions cover both sending and responding?

**Answer A:** Yes, but different rules should apply to different types of PSP's

**Answer B:** Yes both sending and responding should be covered.

**Question 9:** Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.

**Answer:** Based on what we see the following conclusion/restrictions:

- Currently we see no obligation to offer the service by regulatory requirement. If a receiving bank does not offer Confirmation of Payee then the paying customer will be advised that the recipient (or payee's) account name is unable to be checked. However, we understand that the PSR might be considering regulatory intervention to ensure that PSPs implement CoP in a timely and coordinated way.
- Our payment infrastructure of foreign branches is not 24/7/365 ready, which means that implementation is very critical from IT architecture point of view.
- Implementation costs are not known but expected to be very high due to infrastructure dependencies.
- We do not have any technical specifications regarding the new service; a detailed assessment is therefore very difficult. Especially when it comes to the infrastructural topics, matching algorithms, connectivity and interfaces.
- Targeted start dates are totally unrealistic even if other restrictions would not apply.

As far as the consultation paper is concerned, we see difficulties in answering the questions correctly and effectively. It should be pointed out that the deadlines set (for consultation as well as for implementation) cannot be reached.

**Question 10:** Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?

**Answer A:** Validation of account name and number for incoming payments prior to the credit being booked.

**Answer B:** A centralised database could be created for all account number and sort codes for all PSPs.

**Question 11:** Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

**Answer:** Unable to assess without further analysis

**Question 12:** Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

**Answer:** Unable to assess without further analysis

**Question 13:** Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

**Answer:** Unable to assess without further analysis

**Question 14:** What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?

**Answer:** We only have corporate clients and further analysis would be needed regarding costs, benefits and deadline for the implementation.

**Question 15:** Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?

**Answer:** We do not deal with protected groups or vulnerable consumers as the bank only hold accounts for corporate clients.

# Anonymous 2



- We would like to see Pay.UK play a more prominent role in driving industry collaboration and implementation of CoP. We recommend to the PSR that CoP is set out as an Industry standard and managed by Pay.UK, who will then be responsible for setting out and managing the rules for implementation, and the BAU operation. This will support a consistent application across all the banks/PSPs, particularly in an environment where multiple technology providers (and solutions) may be supporting bank / PSPs in delivering the CoP service to consumers.

**Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

We would recommend direct and indirect participants of FPS and CHAPS are given the same direction, in order to drive consistency across the industry and to optimise consumer benefit.

**Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

We recommend banks/PSPs are subject to both 'respond' and 'send' requirements, to ensure consistency and standardisation across the industry.

**Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

We agree with the PSR around the need to provide directions to PSPs for both FPS and CHAPS payments.

**Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

We agree directions should apply to all payment channels that can initiate a FPS or CHAPS payment. The following payment channels should be in scope to protect consumers:

- Mobile Inc. Open Banking
- Internet Inc. Open Banking
- Contact centres - Branches

CoP requests should only apply to:

- New payment mandates
- Beneficiaries that have not been sent funds by the payer over a certain time period E.g. Over 6 months
- When a mandate is amended by the payer

**Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

Some consumers may want to opt out of CoP at the bank/PSP's discretion. However, there is a risk that if a bank/PSP doesn't have a robust opt out process in place (with strict due diligence), CoP may end up benefiting fraudsters. Further clarity is needed on liability within the CRM where consumers can opt out and the decision process that will sit behind it.

We believe there should be no opt out option for a bank/PSP to receive and respond to a CoP request.

**Question 7: Should any directions cover the sending of money from both individual and business accounts?**

We recommend the direction covers both individual and business accounts. The experience from our customers suggests this is a challenge for both consumers and businesses. However the voluntary CRM Code currently only applies to domestic payments affecting consumers, micro-enterprises and small charities. We believe consistency is key here in the way in which CoP interacts within the CRM.

**Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

We suggest directions for both responding and sending CoP requests. We feel there are merits in differing timeframes for respond and send capabilities.

**Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

The timelines currently set out by the PSR will not be achievable for [REDACTED] as things stand and we believe that delivery within these timeframes would place a more onerous burden on smaller banks / PSPs more generally. [REDACTED]

[REDACTED] This is consistent with the messages we have previously provided to Pay.uk.

We recommend H1 2020 as a more manageable timeframe to:

- enable a realistic timeframe for a successful and beneficial procurement activity for a CoP Vendor
- better plan for delivery against a backdrop of other regulatory/mandatory changes in and around the payments environment E.g. PSD2
- successfully implement and embed the contingent reimbursement model guidelines across the industry

If the Industry are directed to implement receive/respond capability by 1st April 2019, there is a risk PSPs/banks will choose a vendor solution because it is ready in time, rather than because it is the best solution for the Industry, or (above all) the best solution for the Consumer.

[REDACTED]

We would also recommend CoP solutions are implemented after the CRM Voluntary code is finalised and successfully embedded into the Industry.

**Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

We are in agreement and recommend that directions are needed for CoP to be successfully implemented. However [REDACTED] would like to see increased involvement from Pay.UK. We would encourage Pay.UK to take a leading

role for both CoP implementation and operation to ensure a high degree of consistency and standardisation throughout the industry particularly given the various technical solutions (and vendors) that may be in use at any given time.

**Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

The themes feel appropriate, but we cannot comment on the cost of implementation at industry level. We would like the PSR to consider the amount of time it could take for customers to adapt to this change. This period of time when CoP is introduced into the market, is likely to not only heighten consumer concern about fraud, but will also introduce friction to the payment process, which are both likely to increase customer queries and have a knock-on impact on wider business functions, such as call centres and branches. This impact will be hard to assess in terms of cost but must be considered. Introducing CoP around the same time as other industry changes, such as PSD2 and Open Banking, may cause further confusion amongst consumers, with the impact felt by various customer-facing departments across the banks/PSPs. We would also ask the PSR to consider the risk that CoP could drive changes in consumer behaviour. Having this new form of security check may lead some customers to stop completing some due diligence checks they perform today when sending a payment. The point here is that CoP may not deliver as much fraud reduction benefit as the PSR model suggests.

**Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

Cost estimates in section 7.13 do not align with our internal estimates of how much this will cost to implement. More information will be given in our information request under section 81 FSBRA response. We consider ourselves a small PSP in relation to CMA 9.

[REDACTED]

**Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

[REDACTED]

**Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits? Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

[REDACTED]

[Redacted]

We do recognise there will be the ongoing benefits once CoP has been implemented, however we have not included any of those benefits from CoP on our total cost of operation at this stage.

We propose the PSR extend the CoP timelines by at least 12 months, as this would enable us to deliver our mandatory and discretionary changes effectively, without creating any major risk to both Customer and Bank. It will also provide a more realistic timeframe for the industry to agree full operational standards and embed the broader CRM.

**Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

[Redacted]

[Redacted]

As previously mentioned, we would welcome direct discussion with the PSR on any of the points raised in this response.

Yours sincerely,

[Redacted]

[Redacted]

# Association of Independent Risk & Fraud Advisors (AIRFA)

# COP - consultation

4th January 2019

Name of the originator	The Association of Independent Risk and Fraud Advisors AIRFA (www.airfa.net)	
Contact Details		The directors Association of Independent Risk and Fraud Advisors (AIRFA)
	<a href="mailto:enquiries@AIRFA.net">enquiries@AIRFA.net</a>	
	[REDACTED]	
<input checked="" type="checkbox"/>	The comments provided can be provided to staff in PSR and into Pay.UK The document and comments cannot be published unless also provided in full to the working party members and to the WHICH? Super complainant representatives.	

## General Comments

The AIRFA members and its directors amongst them are former bankers, risk managers and payments specialists with careers spanning in payments for their entire careers – generally spanning 25+ years each. In particular its members have mostly worked in the areas of payments fraud, payments risks, disputes and compliance. They have additionally been involved in payment scheme issues of this nature across the UK, Europe, US and further-afield.

Members of AIRFA have also engaged the FCA / PSR to discuss the fundamentals of this issue and the potential solutions, sat on the Financial Crime and Fraud Working Party at the PSR amongst many other areas of involvement.

This response may also be read in conjunction with the AIRFA response to the APP Scam Consultation response dated 15<sup>th</sup> November 2018. Some content may overlap and has been repeated in places in this response, where relevant.

The following details, i.e. before responding to the specific questions, are provided to cover the broad principles that flavour the answers to the questions posed. The challenges are complex and consist of a need for a more comprehensive set of solutions. Unfortunately, the COP solution assumes a rather over-simplified view of the problem without addressing the needs for a solution.

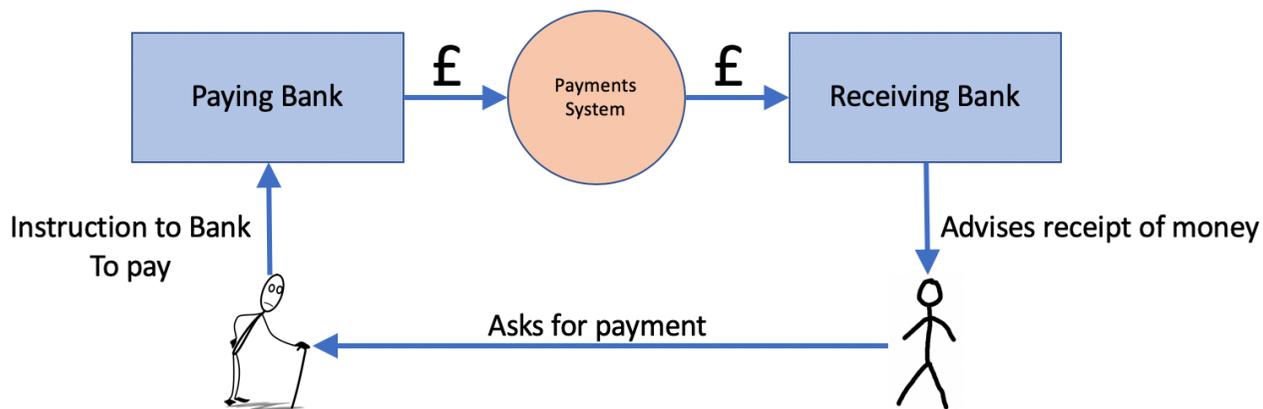
Above all, the COP consultation justifies itself as a solution to address a FRAUD problem supported by the industry. It should be noted that this is not a solution that was addressed by the PSR Fraud and Financial Crime Working Party, but as part of the customer working parties; proposed by receiving payment institutions with an interest in diverting attention towards the traditional paying banks, and NOT supported by the wider industry as claimed.

### Framing the wider Problem

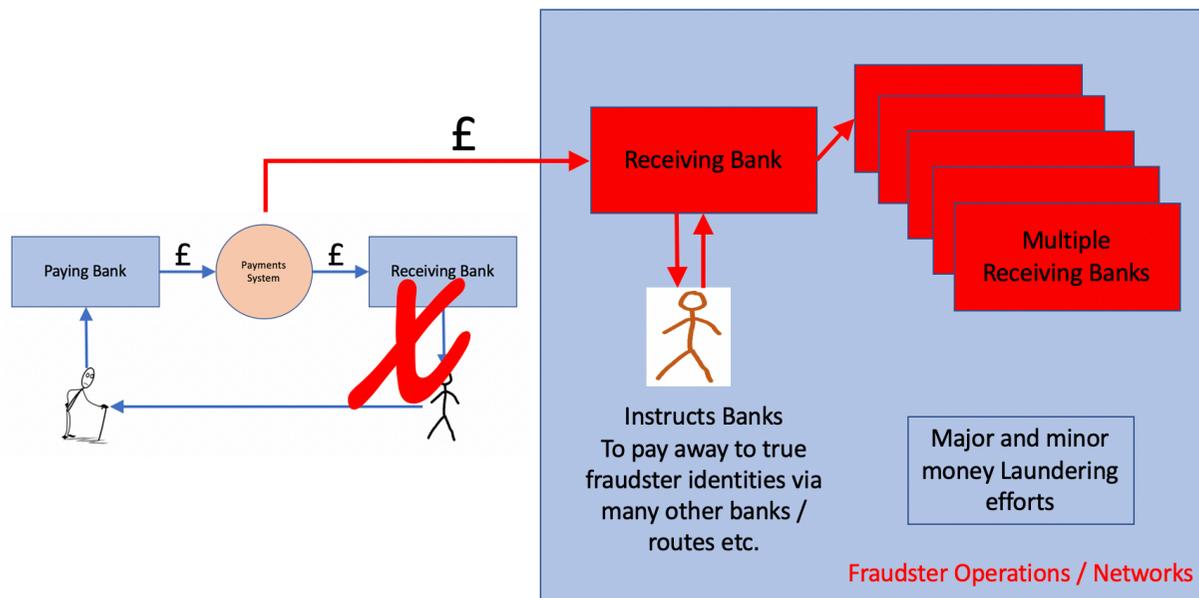
Key to addressing most fraud and scam activity is, and always has been to “follow the money”. A structured risk management approach should always be taken to deconstruct the processes and to stop the fraud. A good approach for any infrastructural analysis is to consider PREVENTION, DETECTION, INVESTIGATION and CORRECTION aspects of the problem and to address them all.

The following is presented to help the reader to understand the real problem and to support the comments given to the consultation comments and questions, and to aid the reader in understanding why the COP programme is NOT A SOLUTION to the fraud problem, is NOT something that is likely to realise any financial benefit or to address anything but a perceived customer issue.

Simplified Usual Money Flow (Figure 1)



Simplified APP Scam Fraud Money Flow (Figure 2)



Problems associated with the APP Scams arise from the following, and/or a combination of the following, that all arise within the ‘Fraud Operations / Networks’ box shown in figure 2 above – and associated with the receiving payment organisation – i.e. the Bank(s) involved.

1. Fraudster likely to have opened receiving bank account with fake identity details.
2. Money may be ‘paid-away’ in CASH if and where possible.
3. Money will be ‘paid-away’ to / through other organisations.
4. Money is often paid into/through multiple organisations to consolidate and then disseminate the funds from many such frauds.
5. The payee names in such organisations will often be different.
6. Payments organisations will often be newer organisations (or older errant ones) and those that have weak, ill-defined or poorly adhered to AML / KYC processes.

Problems associated with the APP Scams, that MUST to be addressed.

This list is an example of the structure and solutions that need to be applied to the scams to address the problems: it is not intended to be an exhaustive list, but to give a flavour for the right actions that should be being progressed.

- a) Poor controls in payee banks over onboarding customers and in identification of the ‘true’ customers
- b) Payee banks/organisations that do not compare payee details with the accounts involved: even when the transactions may be considered higher risks (see PSD2 customer authentication requirements)

- c) Payee banks/organisations that do not 'risk score' money that they RECEIVE (most efforts at such organisations are focused upon PAYMENTS instruction validation, whereas the receiving money requirements of the Money Laundering law receive less attention.
- d) Payee banks/organisations treat all transactions whatever the value, account longevity, account type, expected transaction volumes, historical transactional history.
- e) Banks/organisations who accept payments instructions for on-payment of transactions / consolidation of funds / dissemination of funds without raising suspicions. i.e. failing to KNOW-THE-CUSTOMER, and to understand the nature of the transactions where these are fraudulent.
- f) An absence of challenge when handling these transactions that are clearly fraudulent.
- g) A reliance upon a defence of "can't disclose due to GDPR/UK Data Protection issues" when challenged, rather than co-operating in accordance with the 'crime prevention' exemptions in these laws.
- h) An absence of clear co-operation across the sector (strategically and operationally), as had/has previously been the case within the anti-fraud community within the UK Payments industry prior to the reorganisation of the sector.
- i) Initiatives such as these being co-ordinated within the sector by media/public and industry relations specialists rather than banking / risks representatives from the payments sector.
- j) A lack of available analytics about the problems and issues as evident in this consultation: i.e. where is the money paid to for these scams (organisations / countries / same-name account-names, individuals or companies; are there commonalities of payees, where is the money THEN paid to thereafter – and so forth to the final destinations; how much is tracked to the end-point and recovered, what mechanisms are there for tracking and recovering etc.
- k) No recovery mechanisms as above in (j).
- l) There is no fraudster mapping, no understanding of the fraudsters' networks, the key ('Mr Big') ultimate perpetrators if through organised crime.
- m) No name & shame programme for the guilty parties
- n) No fining mechanism of the guilty payment institutions by/from regulator or pseudo -regulator industry body.
- o) No current 'chargeback mechanisms' to reapportion the losses.
- p) No announcements or analytics on the fines, chargebacks and/or recovery mechanisms; about the recoveries, prosecutions and operations.
- q) No on-going working party and action / strategy taking bodies.
- r) An absence of understanding of the issues and the need for action by and within the PSR / FSA and Pay.UK to drive and address an appropriate agenda.
- s) The absence of a regulator that addresses the marker rather than operating ONLY as an "economic regulator".

#### Confirmation of Payee

The Confirmation of Payee work / consultation:

1. Does not address ANY of the underlying issues shown above in a) to s).
2. Addresses only a perceived problem
3. Introduces a great cost to the UK Plc payments systems
4. Introduces a solution that will quickly be undermined by fraudsters, who will simply move into the large gaps (as they always do, and as proven by initiatives that are incomplete and ill-conceived – and as academia always predicts).
5. Is not part of the Fraud and Financial Crime strategy of the PSR / FCA as it seems to imply.
6. Will only pay lip-service to the WHICH? Supercomplaint.

#### Formal Response

Detail will follow in the tables below where we will address the comments and paper in **SECTION 1**, and then the specific questions in **SECTION 2**

General Comments on the COP Consultation

Ref	Challenge / Issues	Comments / Reasoning
1.2 / 1.3	Executive Summary	<p>It would be useful to know a lot more about the victims and <i>modus operandi</i>. E.g.</p> <ul style="list-style-type: none"> <li>- Which Banks/Financial Institutions involved: what were the outcomes</li> <li>- Amounts involved / value bands etc</li> <li>- What were the payments for: e.g. house purchases / builders etc</li> <li>- How the scams were perpetrated: e.g. conman / conwoman, intercepting post / email etc</li> <li>- Payee banks</li> <li>- How the money was dispersed / where the money subsequently went</li> <li>- What account opening failures occurred</li> <li>- Whether the payee accounts were / were not in different names</li> <li>- And so on</li> </ul> <p>Of all the frauds and fraud types, can these be categorized and quantified, and can it be explained exactly how each such category of fraud will be deterred or avoided?</p> <p>Understanding these things will help the readers to determine what other actions could be taken. There are ALWAYS easier and quicker ways that fraud can be addressed when the data / analysis is available. It feels that the solution has been proposed and now we are searching for the rationale: rather than looking at the problem and finding the right solutions.</p> <p>Incomplete catch-all solutions such as this never (ever) work in the anti-fraud world. Incomplete because solutions need to be for a such transactions for a products to avoid mitigation. A fraud problem must always involve a wide variety of tactics (quick and cheap) solutions.</p> <p>Where a catch-all solution must be implemented, it should be done with a FULL understanding of the problem and the nuances, as well as the areas of risks, gaps in the solution, mitigation, keep hood; it must be fully implemented, fast to implement; and above all, it must address the infrastructure issues, cut off the offending process and have a recovery process and strong management information. THIS PROJECT PROPOSAL HAS NONE OF THESE THINGS. It breaks all the rules and does not address the underlying issues.</p> <p>This really is a solution that is scrambling around to solve a problem that it will not solve. It is ONLY a solution that will address a potential customer need; and not a solution to address fraud. It WAS NOT a solution that arose from any of the <b>PSR Fraud and Financial Crime Working Group projects</b> as it was not a critical-path solution.</p> <p>There is no data here to support this as a project for addressing fraud.</p>
1.4	<p>Executive summary</p> <p>“Should significantly reduce the incidence of fraud”</p>	<p>This is a subjective statement. Our members are anti-fraud specialists who have mostly directed fraud projects for over 25 years for major payments organizations.</p> <p>Fraud, fraudsters and payments solutions do not work in this way, and fraud solutions cannot be driven by subjective ideas that do not address the underlying failings in process and infrastructure.</p>
1.5	Executive Summary	The statements here do not make sense

Ref	Challenge / Issues	Comments / Reasoning
		<p>The payee name in banking law and in banking practice has always been the responsibility of the ACCEPTING bank to ensure is correct; and to make sure that the accepting bank is not converting the funds</p> <p>The payer would not expect the r bank / PSP to be able to check the details of the payee as the payee bank accounts will be at another bank maybe in a different county Consumers are MORE likely to EXPECT not to have their own bank account details distributed amongst ALL other banks/PSP Doing so breached data protection law greatly</p> <p>We have not seen nor been presented with data protection advice on this matter anywhere in spite of promises being made within many forums on this subject that such data will be presented</p> <p>Any shared data MUST under Data Protection Law in the EU and in the UK (strict part of the EU but having strong and a good Data Protection Law); must be shared on only with explicit consent from the Data Subjects involved</p> <p>Data Protection Law allows for sharing of data for crime and fraud prevention purposes without explicit consent: but the advice from the Information Commissioners Office (ICO) is that such shared data MUST then only ever be used:</p> <ul style="list-style-type: none"> <li>- By Fraud/Crime prevention professionals</li> <li>- For no other purpose (i.e. customer assistance transaction validation and process smoothing as here are not compliant)</li> <li>- Not for disclosure to any other party</li> <li>- Not for automated decisions</li> </ul> <p>When will the issues around data protection be acknowledged and addressed? Decisions cannot and should not be made without this How will this issue be addressed?</p>
1.6	<p>If payers were able to compare the name on the receiving account with their intended recipient, they would have a much better chance of avoiding scams or misdirected payments.</p>	<ol style="list-style-type: none"> <li>1 What is the evidence of this? This is an assumption not supported by any evidence</li> <li>2 This is illegal under Data Protection eg s17 see above under 1.5</li> <li>3 Were this to be made possible this would be a fraudsters charter This is as Naïve as Jeremy Clarkson was when he published his account number in the Sunday Times qv</li> <li>4 Fraudsters would immediately use this facility to perpetrate more complex and more dangerous types of fraud</li> </ol> <p>If this is a cumulatively worded claim and in reality only exact matches will be returned as acceptable: then this will lead to major problems and inhibitors in the UK payment systems Eg There are 47 ways in which "J Salisbury PC" might easily be presented / written as a payee without ever making a spelling mistake</p> <p>It is then a simple matter for fraudsters to move to a system of committing fraud using similar names Or exact matches to another account opened for the purpose</p> <p>Follow the logic forward.....</p> <ul style="list-style-type: none"> <li>- The fraud will escalate but will use more closely matching and duplicated account details</li> <li>- There will need to be a new initiative to address this which will require the industry to address the problem AT THE PAYEE bank / payment organisation</li> </ul> <p>Accordingly we should address the problem in the proper way NOW</p>

Ref	Challenge / Issues	Comments / Reasoning
1.7	<p>Executive Summary</p> <p>CoP is the industry-agreed way of ensuring that names of recipients are checked before payments are sent, so the payer can be confident that the payee is who they expect it to be.</p>	<p>This is NOT the "industry agreed" way</p> <ul style="list-style-type: none"> <li>- This was not agreed by the PSR working groups for Fraud and Financial Crime – see this working group's report</li> <li>- This has not been agreed by the Payment Institutions</li> <li>- This has been driven forward as a knee-jerk reaction to the WHICH? Super-complaint with an absence of understanding or ideas on how to address the problem</li> <li>- The majority of people on the working group are consumer representatives – relationship management lobbyists and/or others that do not represent the industry</li> </ul>
1.8	<p>Executive Summary</p> <p>CoP has been identified by both us and industry as an important tool for reducing losses from APP scams, particularly through significantly reducing the number of 'malicious redirection' scams – where a scammer tricks the victim into sending money for a genuine payment to the wrong account. Of the £145.4 million value of APP scams in the first six months of 2018, £93.9 million was attributed to malicious redirection.</p>	<p>See above in 1.7. Also:</p> <ul style="list-style-type: none"> <li>- Nothing has been published that has demonstrated any consideration or costing of the wide array of possible other solutions – infrastructure changes, tools, or initiatives that could also be used</li> <li>- This is a customer solution, not a fraud solution as has been shown elsewhere</li> <li>- Whilst it has been alleged that £93.9m could be the size of the problem, we are not convinced by this analysis as this has not been broken down in any way by the types of accounts that these funds would have been sent to: e.g. personal or corporate, types of PSP, types of payment systems, collection accounts that would be excluded (and other excluded categories) etc. Most of these areas of refinement are questioned elsewhere in the document, and each time one of them is EXCLUDED, the target will shrink</li> <li>- WE CANNOT SHOW THE BIGGEST TARGET POSSIBLE, and in the business-case assume that this can be addressed, and yet erode this target in a most alternative questions and areas under consideration</li> <li>- The entire ability for there to be any savings or any legal construct for addressing the Data Protection issues is questionable</li> </ul> <p>As a starting point, we would expect to have seen a presentation of an analysis here to support many of the bold claims and assertions e.g. Of the £93.9m:</p> <ol style="list-style-type: none"> <li>a) How much of this was paid to accounts in a firm's name?</li> <li>b) How much was paid to collection accounts?</li> <li>c) How much was paid in each payment scheme included / not included?</li> <li>d) How many payments were fraud-related and how many were errors and returned?</li> <li>e) How many were paid to accounts where there were errors or shortcomings in the account opening processes and therefore available for claims against the payee bank/PSP for a refund due to negligent contribution?</li> <li>f) How often were the funds still available and potentially recoverable?</li> <li>g) How many were for new accounts whereby the account holder could have / should have been under stricter observation: with a possible transfer of liability to the payee PSP?</li> <li>h) How many accounts were short-lived and why would this have not aroused suspicions?</li> <li>i) How often were the payee banks able to make contact with and engage the customer for repayment, and if not, were the account opening AML and KYC processes inadequate to an extent that the payee bank/PSP could be held liable?</li> <li>j) Were the payee banks negligent in the subsequent processing of the funds and potentially liable for negligent onward-processing instructions?</li> <li>k) How many payments were received that were inconsistent with expected and anticipated levels of processing that would have caused the banks/PSPs to be considered negligent to a degree where they should be held liable?</li> <li>l) Etc</li> </ol>

Ref	Challenge / Issues	Comments / Reasoning
	GENERAL	<p>There appears to have been the consideration of the myriad of alternative technical and infrastructure change possibilities that could be adopted. Many solutions could be implemented that are faster, easier, cheaper and simpler than a major change. These that will most likely address and save very little.</p> <p>We have seen no analysis that has considered alternatives with either an acceptance of any or even a rejection of any alternatives.</p> <p><b>This is one highly questionable / remiss of the industry and of the regulator itself</b></p>
	TECHNICAL SOLUTIONS	<p>Leading solutions in most other sectors in payments in particular at retailers, bulk payments organisations, card issuers and card acquirers include validating transactions in real time by the organisation at risk and where the losses can be controlled.</p> <p>In this case it is clearly a job/task to be undertaken at the payee banks/PSP and should include:</p> <ul style="list-style-type: none"> <li>A) Transaction risk weighting scoring</li> <li>B) Transaction checking for consistency</li> <li>C) Electronic message checking (e.g. against the payment instruction provider's hardware and software and technical contact details). This should include establishing a routeway for processing such details with the payment instruction such that the payee bank can receive these and make a decision based upon the authenticity and anonymity of the data provided.</li> </ul> <p>It is remarkable that such considerations fall out of scope here in lieu of a basic and simple solution that is hard to implement and most likely to fail in today's world.</p>

Specific Consultation Questions

Questions	Comments / Reasoning
<p><b>Question 1</b> Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?</p>	<p><b>NO – this is not the right approach.</b></p> <p>Mandating poorly thought-out requirements that will:</p> <ul style="list-style-type: none"> <li>a) Move fraud around rather than removing it</li> <li>b) Add massive costs to the industry</li> <li>c) Increase barriers to entry</li> <li>d) Remove competition in the industry and create new barriers for entry to new-entrants by creating a cost that only big-banks can understand and afford</li> <li>e) Inconvenience customers</li> <li>f) Add a new product that fraudsters will quickly infiltrate and USE to perpetrate more frauds</li> </ul>

Questions	Comments / Reasoning
	<p>internationally</p> <p>g) Make the UK payments industry more expensive less competitive and less accessible</p> <p>This will make the PSR the FCA the key payers in the PSR appear ridiculous and give rise to a major credibility loss overall</p> <p>The PSR MUST take action but it MUST take action in a way that will start the industry down a route of addressing the problem; rather than moving it around rather than punishing the customers / consumers with added processes compromises of data and potentially greater abuses</p> <p>The PSR must develop a requirement for a programme of work that addresses the problem at the PAYEE banks where the problems are caused</p> <p>The credibility issues for the PSR continue in relation to the projects that have been adopted across its remit without proper and proper consideration of the risks the abuses and potential gaps left</p> <p>AIRFA have been raising this as an issue / predicting this in a consultations and workshops since the PSR's inception</p>
<p><b>Question 2</b></p> <p>Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?</p>	<p><b>All fraud solutions should and must – as a basic requirement: be applied 100%. Fraud solutions with 'opt-outs' always fail. This is a basic 'Fraud 101' principle.</b></p> <p>However this is NOT an anti-fraud solution that will not save any fraud. The project should have a aspects of fraud savings considerations removed from it and addressed on a customer service programme of work</p> <p>The exclusions exemptions and missing aspects (thus far) of the project already remove more benefits than actually exist</p>
<p><b>Question 3</b></p> <p>Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?</p>	<p>What a strange question</p> <p>If no-one responds to the requests then nothing will happen and the impact will be irrelevant</p> <p>The key should be to hold the payee bank/payment organisation accountable and to encourage them to improve their processes and acceptance of fraudulent payments. This is NOT achieved here at a. Accordingly the questions are so rather redundant</p>
<p><b>Question 4</b></p> <p>Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or</p>	<p>Not applicable</p> <ol style="list-style-type: none"> <li>1 As the project should be STOPPED forthwith</li> <li>2 Were it to be continued and assuming that it could be considered effective and actually in some way work to reduce fraud in the schemes in which it is introduced: then fraudsters</li> </ol>

Questions	Comments / Reasoning
<p>more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?</p>	<p>would simply address themselves to the payment systems where working so unions not applied</p> <p>3 These type of solutions (where they work and clearly this appears to be an inadequate solution as it does not address the problem) simply push fraudsters around the processes and systems to the next weak point adding costs endlessly and removing no fraud</p>
<p><b>Question 5</b> Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?</p>	<p>We have engaged formally and informally with many leading fraud specialists who find this scheme / work of little value but of no relevance as an infrastructure project that will impact fraud losses in any way</p> <p><b>Accordingly, the project should be considered ONLY in the context of a customer service solution. And then as such a solution there is no business case, and a strong case for NO ACTION as it will add only costs, inconvenience, uncompetitive UK marketplace, stifling of innovation and barriers to entry.</b></p>
<p><b>Question 6</b> How should any directions deal with the potential for people to opt out of the CoP process?</p>	<p>A large portion of the population should opt-out of the COP:</p> <ol style="list-style-type: none"> <li>1 To STOP the r data being compromised</li> <li>2 To remove the barrier to payments</li> <li>3 To facilitate the use of services that will evolve that we need simple fact on and no COP</li> <li>4 Because organisations will recommend this: e.g. even WHICH? Should do so as this programme is massively counter-productive and does not cause the banks / payments organisations to address the underlying issues [see a) to s) above]</li> <li>5 It may be likely that the ICO could intervene with the sharing of data that has not been authorised and received explicit consent for customers to share throughout and across the payments/banking systems</li> </ol> <p><b>DURING THE CONSULTATIONS / STAKEHOLDER MEETINGS, there were repeated questions and promises of delivery of assessments of the CoP scheme by the Information Commissioner's Office (ICO). These are not included here, and we have not seen any publication of these elsewhere.</b></p>
<p><b>Question 7</b> Should any directions cover the sending of money from both individual and business accounts?</p>	<p>This question fails to show an understanding of the problem and how fraudsters operate</p> <p>Fraudsters will use whichever products have the fewer controls and processes applied to them. Not necessarily by design but by pure osmosis</p> <p>Accordingly why this project will fail is that it MUST:</p> <ul style="list-style-type: none"> <li>- Be applied to ALL possible payments to actually work</li> <li>- Be applied to all high-risk payments</li> <li>- Be applied to all solutions e.g. all name variations. Fraudsters are capable of and WILL open and use accounts in the name of "Mr In and Revenuesk" (real example) to divert</li> </ul>

Questions	Comments / Reasoning
	<p>payments m s-spe ed / near-m sspe ed</p> <p>Accord ng y the attr t on when app ed to a payments w be s gn f cant for a users and w :</p> <ul style="list-style-type: none"> <li>a) Make payments systems use n the UK expens ve</li> <li>b) Cause PSD 2 n the UK and assoc ated Open Bank ng and PISP creat on and API use to become too onerous for the UK to rema n compet t ve aga nst non-UK payment organ sat ons</li> <li>c) G ve r se to fewer nnovators</li> <li>d) Make compet t on harder n the UK</li> <li>e) Add barr ers to entry n the UK</li> </ul> <p>At the same t me fraudsters w s mp y f nd the eas est routes n to cont nue the r frauds They DO NOT s mp y pack-up and go as they have bus nesses to run too: and they w m grate to the eas est next frauds wh ch w rema n n APP scams but w th s ght y changed <i>modus operandi</i></p>
<p><b>Question 8</b> Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?</p>	<p><b>Neither</b></p> <p>The prob ems e n the rece v ng bank and the prob em that the rece v ng bank causes by:</p> <ul style="list-style-type: none"> <li>a) Rece v ng a payment for the cred t of an account n the name of "X" and</li> <li>b) App y ng t to an account n the name of "Y"</li> <li>c) Not accept ng such payments w th a r sk-hat and scor ng such transact ons and then mak ng appropri ate enq u res and protect ng the money f t appears to have e ements about t that are nd cators of fraud/ APP scams: e amounts frequency age of account eve of due-d gence undertaken on-payments contacts w th customer certa nty of KYC taken etc etc etc</li> </ul>
<p><b>Question 9</b> Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.</p>	<p>No Th s pro ect shou d be serous y recons dered and rep aced w th work that w address the nfrastructura ssues and poor pract ces at the payee bank/organ sat on end of the payments va ue chan</p> <p>Th s pro ect shou d be progressed w th ONLY f the pro ect s requ red and ust f ed from a customer process mprovement a one It shou d not be progressed w th any us on that t w address any under y ng fraud prob em</p>
<p><b>Question 10</b> Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?</p>	<p>The PSR MUST start to address tse f to so v ng the under y ng prob ems of these frauds and stop them by prevent ng the fraudsters from be ng ab e to access bank ng fac tes and track ng down the fraudu ent money</p> <p>Th s w need to be done by remov ng the weaknesses from the systems and the poor pract ces that</p>

Questions	Comments / Reasoning
	<p>are accumulating in the payments systems</p> <p>SEE DETAILS above in a) s) and in the general details at the start of this document</p>
<p><b>Question 11</b></p> <p>Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.</p>	<p>i) <b>No.</b> The benefits will not be realised at this level. This project is a customer-service enhancement project derived from customer perspective and NOT from a Financial Crime &amp; Fraud perspective</p> <p>ii) <b>Benefits:</b> (from cursory reviews and oversight of fraud projects over the last 25 years but also from experience in poor implementation and thinking over many years):</p> <ul style="list-style-type: none"> <li>a) 20% - 50% reduction in the first month</li> <li>b) Reversion to the same levels in 2<sup>nd</sup>/3<sup>rd</sup> months</li> <li>c) Significant growth by 100% in month 4 to month 6 as the fraudsters identify the gaps re-group and recover lost income. This is not enough of a change to deter them for long or drive them into other sectors / products. This will NOT deter organised criminals at a level that deters opportunists only for a short period of time</li> </ul> <p>iii) <b>Further losses:</b> It is likely that further fraud / scam growth will occur once the fraudsters start to infiltrate payment organisations and obtain access to COP systems and/or harvest payee details from multiple payment record confirmations and use these to perpetrate NEW FRAUDS. Equally these NEW frauds will take place on these same payment products and also be used with new payment product types as this information will have value to fraudsters</p>
<p><b>Question 12</b></p> <p>Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.</p>	<p>No view on cost values. How were these costs arrived at?</p> <p>Have these been obtained from the payment institutions that will implement this initiative</p>
<p><b>Question 13</b></p> <p>Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.</p>	<p>Very strange assumptions used throughout:</p> <ul style="list-style-type: none"> <li>a) Capital Expenditure will be needed immediately; not over 5-10 years</li> <li>b) Why is growth in APP scam rates expected at 0-10% - unaddressed fraud growth rates are always EXPONENTIAL. The underlying fraud issues have not been addressed and there are more GAPS in the COP enterprise than solutions</li> <li>c) Prevention rates likely to be MUCH MUCH lower. Where there is no infrastructure change fraud becomes deterred in the short-term (days) as the fraudsters re-group and find the exceptions and holes in the processes and systems (of which there are many here). Accordingly <b>the prevention rate here should be lower than the growth rate</b></li> <li>d) No fraud project delivers 90% prevention unless the entire infrastructure problems are addressed</li> </ul> <p>Where did these assumptions come from?</p> <p>Early implementation will allow earlier discovery of the findings and an earlier re-think</p>

Questions	Comments / Reasoning
	<p>Please can the individuals/organisations associated with the assumptions be NAMED in the document in order that these can be reviewed at a later date</p> <p>Will the PSR UNDERWRITE formally the value of expected benefits. We believe that it should do so in order for the organisation to assess the CBA analysis properly rather than relying upon what appears to be rather an unsubstantiated piece of guesswork</p>
<p><b>Question 14</b> What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?</p>	<p>This should not be imposed as it adds major costs for a minimal customer benefit</p> <p>The BENEFITS make assumptions that are not valid and fail to include estimations of FRAUD mitigation (amounts and timing) not have the fraud losses (and therefore the benefits) been assessed according to the payment types that will be covered by these changes. How many of the frauds will not be affected because they are paid into current account or other non-included account types</p> <p>Imposing this as a requirement will add a cost that will be prohibitive for new payers. This will:</p> <ol style="list-style-type: none"> <li>Increase the cost of access to innovation and <b>reduce innovation</b></li> <li><b>Restrict competition</b> making it easier for larger banks with the infrastructure</li> <li><b>Increase the costs</b> and remove the competitive nature of the UK payment systems</li> <li><b>Remove payments from the UK</b> as fraudsters use more payments organisations that fall outside the purview of this regulator</li> <li><b>Lead to more organisations establishing their payments businesses with non-UK regulators</b> but still based in the UK</li> </ol>
<p><b>Question 15</b> Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?</p>	<p>Not considered here. Our focus is elsewhere even though it is accepted that this is an important issue</p> <p>Equality from financial surveys of people making payments where banks have started to implement “are you sure?” type hurdles over the last few months for their customers when making payments; these have been considered to be:</p> <ul style="list-style-type: none"> <li>Annoying to many especially businesses</li> <li>Unnecessary and introducing a suspension</li> <li>Have already started to be ignored</li> <li>Confusing</li> <li>Slowing down the process / productivity and adding costs to businesses / people making payments</li> </ul> <p>These comments apply equally to people who are vulnerable who will be equally confused and find such things an unnecessary complication in a process that may already be complicated enough for them</p> <p><b>THIS IS NOT A RISK ISSUE / FRAUD &amp; FINANCIAL CRIME ISSUE</b></p>

### Receiving Banks / Payments companies

There seems to have evolved a culture of resorting to excuses / defences by the payment receiving banks/organisation: i.e. those that have failed in their duties of care and enable fraudsters to hide behind a stance of 'DATA / CUSTOMER protection' issues rather than exposing the fraudsters and their own culpability. This is much more the case with the preponderance and proliferation of the volume of new entrants in the market of 'receiving' funds (without doing their legally required due diligence).

Too many organisations operate in this 'space' – i.e. accepting and converting scam/fraudulent funds without the understanding or knowledge of what they are doing and not having the concerns that could be sharper if they also had the liability for the losses that they help cause.

We MUST NOT CONFUSE the genuine mis-redirection of funds (which is generally easily reversed and corrected) with the fraudulent mis-direction - as this position is routinely quoted as the rationale for project initiation.

Analysis of the problem has been distinctly wanting: with these situations (APP SCAMS) a starting point MUST ALWAYS be to understand where the problem exists. There has been no publication of where these losses have occurred from a RECEIVING BANK/ORGANISATION. Were this to be available, then it will reveal those parties who are more negligently carrying out their customer due diligence and allowing for fraudsters to hide within their accounts network. Members of this organisation would be happy to help evaluate this problem and drive solutions.

It is good to have an economic regulator, but regulation must also include aspects of routing-out the problems and addressing the errant parties in any transaction and ultimately seeking compensation from the errant parties (where they cannot recover the scam funds), rather than seeking recompense from victims or from ALL service users.

The common factor in APP scams is that the receiving bank/organisation has received funds to an account for a fraudster and is then quickly 'paid away' these proceeds of crime to another party and somehow assisted in the distant party / cash withdrawal etc. Historically, this will often happen through several accounts and with foreign banks etc., but increasingly now is processed through transient payment facilities set-up with limited due-diligence. In all cases the receiving bank/organisation cannot recover and return the fraudulently paid away funds, because they have subsequently paid these away.

### Fundamentals on how the fraudsters succeed

In these cases, the receiving banks/organisations will have been defrauded and will have set-up an account for a fraudster (or had an account taken-over by a fraudster). The receiving banks/organisations are unlikely to help the paying bank - because the money has usually and already been 'paid away' to a fraudster and/or through a series of further banks/organisations, such that it is most likely to be culpable in the failure in their ID&V processes for the fraud account set-up and/or receipt and execution of the payment instructions. The receiving bank is placed in a difficult position:

1. They may not know that there has been a fraud – in which instance they will not want to assist with any investigation. Data protection risks are potentially valid for them in this case.
2. They will argue that the payer and payer's service provider did authorise the push payment.
3. They may argue that the payer could in fact be collusive in the performance of the fraud scam
4. They are unlikely to be able to return the funds because the funds are no longer there.

5. If they return funds or offer to return funds, there will be a liability to a potential genuine customer and the talk of assessing whether to do so and to set up a process that would allow this would need to involve the signing of an indemnity against loss.
6. Doing this would potentially indicate a culpability or liability for failure in their ID&V
7. If the money has been paid onto further parties, there would be considerable work involved to recover this from subsequent receiving banks/organisations for all the same reasons as above.

For payments by cheque, bills of exchange etc., in the past, it was normal for the banks (as they were historically only banks) to co-operate in this process on a reciprocal basis. With the introduction of new parties within payments, the reciprocity has disappeared, and all parties are affected of the position above today. Accordingly, through this the industry-level co-operation has been lost and the processes for protecting the customers have been lost.

Apart from the timing, it could be argued that the increased regulation, introduction of innovation and new and increased competition established by the set-up of the PSR and its initial actions, has played a major contributing factor in raising awareness of these new types of fraud and the escalation of the problem. These types of risks have been introduced and exploited as they have not been properly considered. AIRFA members have previously raised these potential risks and this risk in particular since the initial consultations for the formation of the PSR.

### Data Sharing Issues

Such frauds and fraudster-details MUST be exposed and shared across the industry in every case, along with the sharing of data about the organisations that aid in the frauds through their failure to adopt proper ID&V processes: so that the paying banks can be more wary of payments made to such organisations (as a whole rather than within their records individually).

Listing of fraudsters (through say accepted fraud data-sharing arrangements such as through CIFAS) must be a major part of the strategy moving forward. **NOTE:** The UK Data Protection Act 2018 provides for this with a well-trodden series of remedies for these situations in law, and in many other payment systems.

### WAY FORWARD

- A. There should be an agreed compulsion for the receiving banks, upon confirmed frauds being discovered, to provide full details to the paying bank – and/or to an advocating/reporting third-party (Pay.UK). The data protection exemptions for fraud reasons always apply in such cases.
- B. Full details of the networks of fraudsters adopting these fraud methods should be linked and investigated by the payment organisations and prosecuted – with a primary aim to also capture/block and recover stolen funds from whichever organisations ‘collect these funds’.
- C. The organisations that collect the funds should be held liable and to recompense the system, and therefore the customer(s) involved.
- D. There should be a mechanism for exposing such organisations to allow paying banks and paying customers to be wary and for some degree of regulatory sanction / fines to apply.
- E. A system of fines should be introduced to compensate victims for their errant behaviour / errors in due diligence and/or AML / KYC processes and thereby through reporting introduce some element of ‘name and shame’.
- F. An audit regimen should be introduced that is linked to licencing and membership to payment schemes.
- G. Proof for all frauds by the receiving banks should include full customer due diligence details - i.e. when account was set up, how, addresses, timing, contact details, proof of customer etc.
- H. For clarity and fairness, proof for all frauds from the paying bank should also include full customer due diligence details - i.e. when the payer account was set up, how, addresses, timing, contact details, proof of customer etc.

- I. “Follow the money” from the FIRST receiving bank through to the ultimate receiving party MUST always be discovered/disclosed for every APP scam loss.

#### WHY THIS IS IMPORTANT

The challenge is that there are increasingly failures in the identity / AML procedures at many new and existing organisations / banks. These are typically driven for competitive and cost reasons, as they may 'short-cut' traditional customer identification, do not fully comprehend such requirements, or connive to compete with lower 'barriers to entry' for new customers (in this case fraudsters). It is the accepted 'narrative' that Banks unnecessarily 'over-do' customer identification, which becomes the area in which new-entrants and established players compete - i.e. within the area of minimising 'customer friction'.

Accordingly, the fraudsters chase any new or established organisation with new licences, new processes, poor controls, lower barriers to entry. Insider information will often be utilised to divulge process / procedure issues and weaknesses as well as system shortcomings.

Receiving entities have almost no incentive to stop this. Indeed, it is IN THEIR INTEREST and they can profit from this, especially if they can:

1. REFUSE to return the funds to the paying bank, and
2. Identify a PAY-OUT transaction as fraudulent by carrying-out proper identification of the customers at the later stage of identifying the customer as fraudulent upon receipt of a payment instruction.

# The Association of Corporate Treasurers



LEADING TREASURY  
PROFESSIONALS

## The Association of Corporate Treasurers

Comments in response to  
***Consultation on general directions on  
implementing Confirmation of Payee***  
November 2018

January 2019

### The Association of Corporate Treasurers (ACT)

The ACT is a professional body for those working in corporate treasury, risk and corporate finance. It is established by Royal Charter in the public interest. Further information is provided at the back of these comments and on our website [www.treasurers.org](http://www.treasurers.org).

Contact details and a link to our approach regarding policy submissions can also be found at the back of these comments.

We canvas the opinion of our members through seminars and conferences, our monthly e-newsletter to members and others, *The Treasurer magazine*, topic-specific working groups and our Policy and Technical Committee.

### General

The ACT welcomes the opportunity to comment on this matter.

This document and its content are on the record and may be freely quoted or reproduced with acknowledgement but external material we have ourselves quoted may be subject to rights of the copyright owner.



*The Association of Corporate Treasurers, London, 4 January 2019*

**Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

We support the approach and have no other comments on the issues raised in this section.

**Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP**

To ensure that the benefits are achieved and there is no “leakage” to non-participating institutions we believe that directions should be applied equally across all PSPs.

**Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

No as the ability to support CoP should be aligned with the overall participation of that PSP with CoP.

**Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

As the FPS payment limit continues to increase, the direction should be kept consistent across both payment schemes. Any approach that differs between the two carries the risk that potential benefits will be reduced and that criminals will target the payment scheme that does not have mandatory CoP.

**Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed**

To reduce payment friction and support efficient payment processing we believe that CoP should only be applied for new or amended beneficiaries.

**Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

The default should be for individuals to opt in. Opting out should require several re-confirmations and possible Strong Customer Authentication.

**Question 7: Should any directions cover the sending of money from both individual and business accounts?**

Yes – both individuals and businesses are affected by payment fraud. The value at risk is larger in business and therefore required.

**Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**



We have no comment.

**Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

We have no comment.

**Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

We have no comment.

**Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

Many businesses employ complex, time-consuming and manual processes to limit the impact of fraudulent payments. Although difficult to quantify, it is an impediment to greater adoption of Straight Through Processing of payments. The problem has been exacerbated by the move to same day processing for small payments and we expect it to become worse as consumers increasingly use smartphones to make payments.

**Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

We have no comment.

**Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

We have no comment.

**Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

We have no comment.

**Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

We have no comment.





**LEADING TREASURY  
PROFESSIONALS**

## **The Association of Corporate Treasurers**

The Association of Corporate Treasurers (ACT) sets the benchmark for international treasury excellence. As the Chartered body for treasury, we lead the profession through our internationally recognised suite of treasury qualifications, by defining standards and championing continuing professional development. We are the authentic voice of the treasury profession representing the interests of the real economy and educating, supporting and leading the treasurers of today and tomorrow.

For further information visit [www.treasurers.org](http://www.treasurers.org)

Guidelines about our approach to policy and technical matters are available at [www.treasurers.org/technical](http://www.treasurers.org/technical)

	<p>The Association of Corporate Treasurers 69 Leadenhall Street London EC3A 2BG, UK Telephone: 020 7847 2540 Fax: 020 7374 8744 Website: <a href="http://www.treasurers.org">http://www.treasurers.org</a></p>
--	--

*The Association of Corporate Treasurers, established by Royal Charter*



*The Association of Corporate Treasurers, London, 4 January 2019*

# Atom Bank



Atom Bank  
The Rivergreen Centre  
Durham  
Dh1 5TS

07/01/2019

APP Scams Policy Team  
Payment Systems Regulator  
12 Endeavour Square  
Stratford  
London  
E20 1JN

Email [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)

PSR-CP-18-04 - Consultation on general directions for the implementation of Confirmation of Payee

Launched in April 2016, Durham-based Atom bank is committed to building a customer-driven bank, designed to meet continually evolving customer needs. The bank currently offers non-payment accounts; Fixed Saver accounts, residential mortgages, and secured business lending for SMEs. Since launch, Atom bank has lent in excess of £2 billion to small businesses and homeowners across the UK and is, based on UK Finance data, the UK's fastest growing mortgage lender, also achieving good growth in Fixed Term Savings accounts with deposits now in excess of £1.7 billion.

From the start, Atom set out to build a customer-focused bank, designed to meet their new needs and optimised for mobile technologies. Atom is here to change banking, creating a disruptive and digital bank, keeping costs low and passing back the value to its customers. The Atom app is at the heart of the bank, with a 24/7 support team on hand to help with any customer queries through phone, chat, email and social media, working out of the Durham HQ.

Atom would like to commend the Payments System Regulator (PSR) on their push to build controls in the financial services eco-system to prevent consumers falling victim to Authorised Push Payment (APP) scams and reducing misdirected payments. Secondly, Atom would like to seek clarification on the General Direction, specifically on the implementation & scope of Direction to support the development of the Confirmation of Payee solution with the goal of reducing fraud & customer errors.

**Question 1** - Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?

Atom agrees that the industry must do more to protect consumers against Authorised Push Payment (APP) scams. In addition to this, Atom believe the industry could make better use of established and emerging technologies to more effectively provide consumers certainty of the destination and fate of payments to reduce consumer errors and fraud.

In Atom's opinion; the introduction of Confirmation of Payee (CoP) is a solution which may enable customers to gain additional confidence when initiating payments and therefore should be implemented by the industry.

A Direction from the Payment Systems Regulator (PSR) for Payment Service Providers (PSPs) to implement CoP may act as a catalyst to the market to work to a common goal in delivering CoP. However, Atom also believes that the use of such a Direction combined with additional pressures such as the proposed timeframe may result in a suboptimal delivery of the CoP solution.

Whilst a fast implementation of CoP may provide consumers with greater protection against APP scams & misdirected payments quickly, Atom believes that an even greater benefit will be realised by consumers from a coordinated delivery across the industry to achieve the required network effect to gain mass adoption by consumers. It is not believed that such an impact can be achieved within the timelines recommended within the PSRs consultation (all PSPs to be able to receive by 1<sup>st</sup> April 2019 and all PSPs to be able send by 1<sup>st</sup> July 2019).

This is the key concern for Atom as the potentially harmful consequences of an ineffective delivery will undoubtedly outweigh any short-term benefits. If consumers perceive the solution negatively, it is likely to be subject to slow adoption rates and will therefore not act as a protection from APP scams & misdirected payments.

Atom also would like to highlight that many PSPs are looking to use common suppliers to deliver their CoP solution. This poses additional risks including:

- The delivery of CoP may be deficient due to capacity challenges / significant pressure on the suppliers.
- Smaller participants may not receive the same support from suppliers as larger participants because of prioritisation.

- Due to the timelines for delivery, PSPs may be at a competitive disadvantage and may not be able to use preferred suppliers to meet tight deadlines.

Whilst Pay.UK have developed the CoP proposition Atom believes there is a gap which must be filled for delivery of this proposition. Atom would support a body, such as Pay.UK or UK Finance, facilitating the creation of an industry delivery group to:

- Take responsibility to develop a coordinated delivery plan with participants and suppliers;
- Act as a forum to support the ecosystem to progress against this delivery plan;
- Seek to understand and mitigate risks of delivery, such as those associated with common suppliers and suboptimal delivery methods;
- Have the mandate to raise and escalate all identified risks appropriately; and
- Have appropriate knowledge and skills to ensure that the delivery of the solution achieves a network effect across the industry to ultimately result in mass adoption by consumers.

As mentioned, Atom believes that a Direction from the PSR may act as a catalyst for PSPs to deliver CoP however to ensure that this is done successfully, the Direction and timelines associated with it should only be confirmed following appropriate analysis from the above-mentioned delivery group.

### **The proposed scope of the directions**

**Question 2** - Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?

Atom would welcome more clarity on the scope of the proposed Direction. APP scams are impacting consumers in different ways across different types of accounts. Also, the way consumers send payments varies by account type meaning some accounts are less prone to misdirected payments.

Due to the nature of most non-payment accounts requiring payments from an account to be sent to a single defined account, there is evidence (which can be provided to the PSR on request) that consumers see very low volumes of APP scams & misdirected payments. Therefore, Atom suggests that consumers will see significantly less benefit for non-payment accounts.

If the decision is made by the PSR to exclude non-payment accounts from the scope of the Direction, it is suggested that these account types are monitored following the industries go live so that if fraudsters decide to adapt and migrate to these types of accounts the industry can adapt quickly.

Atom would like to see the Directions cover both individual and business accounts but believes that to mitigate risk against the delivery of the solution this should be phased. Atom believes that personal customer to customer payments should be focused on initially to mitigate the risk of the overall delivery of a CoP solution. Atom notes there may be challenges within the business account segment which could impact the delivery of the initial solution, such as account names for legal entities, and therefore this should be delivered in a subsequent phase.

**Question 3** - Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?

Atom's view is that, to achieve a network effect and enable consumers to receive a consistent experience across all financial products (specifically those that enable payments via Faster Payments & CHAPS), all PSPs will need to be able to respond to CoP requests.

Please note that this is subject to the view provided in the response to Question 2 – i.e. PSPs should not be required to send CoP requests for every type of account.

**Question 4** - Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?

Atom believes that the Direction should apply to both Faster Payments & CHAPS to enable consumers to receive a consistent experience across all financial products which will help achieve a network effect. Atom does not believe that the Direction should apply to more than Faster Payments & CHAPS.

**Question 5** - Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?

It is believed that that CoP should apply across all channels where the consumer interacts with the solution via a user interface. There are challenges applying a CoP solution via verbal or physical interactions which could expose PSPs to data protection breaches when delivering a CoP response (Beneficiary name) under some conditions within the current CoP proposition.

It is felt that CoP should apply when a payment mandate is set up or amended in line with the above-mentioned channels.

**Question 6** - How should any directions deal with the potential for people to opt out of the CoP process?

Whilst the CoP proposition & consultation from the PSR focuses on the premise that all consumers are automatically opted in to CoP, Atom would like to propose that the recommended Industry Delivery Group (response to Q1) looks to fully understand the benefits of requiring consumers to opt in to the CoP service.

This could bring multiple benefits; for example, the CoP brand will grow naturally, and consumer adoption rates will follow a more controlled curve.

Atom understands that for the solution to work high volumes of users need to have opted in to the service. Therefore, the scenario where a significant number of consumers chose to either not opt in (or opt out) of CoP, needs to be planned for as this will impact the experience of the overall CoP solution.

Should the decision be made to continue to require all consumers to be automatically opted in to the proposition, Atom understands why some consumers may want to opt out of CoP and believes that the ability to opt out should be possible. It is important to define a clear and consistent approach for consumers to opt out of the solution and the legal basis for this should be understood.

**Question 7** - Should any directions cover the sending of money from both individual and business accounts?

Atom would like to see the Directions cover both individual and business accounts but believes that to mitigate risk against the delivery of the solution this should be phased. Atom believes that personal customer to customer payments should be focused on initially to mitigate the risk of the overall delivery of a CoP solution. Atom notes there may be challenges within the business account segment which could impact the delivery of the initial solution, such as account names for legal entities, and therefore this should be delivered in a subsequent phase.

#### **The rationale for our timeframe**

**Question 8** - Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?

Atom believes that to achieve a network effect and therefore more likely mass adoption by consumers, all PSPs in scope of the Direction should be required to both respond & send CoP requests unless the account type is a non-payment account due to the reasons outlined within Atom's response to Question 2.

It is believed that to mitigate the risk of delivery for PSPs, a phased delivery will ensure greater outcome for consumers. Atom believes there is benefit from asking PSPs to create the ability to Respond to requests initially and then to Send requests in a following phase.

**Question 9** - Do you agree with the deadlines for the introduction of CoP?  
*If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.*

Whilst Pay.UK have developed the CoP proposition Atom believes there is a gap which must be filled for delivery of this proposition. Atom would support a body, such as Pay.UK or UK Finance, facilitating the creation of an industry delivery group to:

- Take responsibility to develop a coordinated delivery plan with participants and suppliers;
- Act as a forum to support the ecosystem to progress against this delivery plan;
- Seek to understand and mitigate risks of delivery, such as those associated with common suppliers and suboptimal delivery methods;
- Have the mandate to raise and escalate all identified risks appropriately; and
- Have appropriate knowledge and skills to ensure that the delivery of the solution achieves a network effect across the industry to ultimately result in mass adoption by consumers.

As mentioned, Atom believes that a Direction from the PSR may act as a catalyst for PSPs to deliver CoP however to ensure that this is done successfully, the Direction and the timelines associated with it, should only be confirmed following analysis from the above-mentioned delivery group.

### **Alternative approaches**

**Question 10** - Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?

Atom believes that the Direction is an effective way to act as a catalyst for PSPs to deliver CoP in a coordinated way. But believes that the timing of this Direction is important and that this should be given when a clear delivery plan is understood by the industry.

### **Cost Benefit Analysis**

**Question 11** - Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Atom believes that the quantitative figures provided by the PSR are the best figures currently publicly available and therefore are the most appropriate to be used as a benchmark. Atom understands from conversations with industry colleagues via UK Finance, additional enhancements can be made to these figures to more accurately reflect the position of the proposition that has been developed by Pay.UK. Atom understands that more detail on this will be provided within the UK Finance response.

Atom agrees with the qualitative statements given and believes that these appropriately describe the benefit that could be seen from implementing CoP in a coordinated way.

That said, Atom does not believe an accurate cost benefit analysis can be performed until clarity is given on the scope of the Direction, implementation timelines and an understanding of consumer adoption is known. This is due to assumptions made which may have a significant impact on the overall benefit depending on the delivered solution.

**Question 12** - Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Atom is unable to provide a view of the costs associated with CoP until clarity is given on the scope of the Direction, implementation timelines and an understanding of consumer adoption is known.

**Question 13** - Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Atom is unable to provide a view of the costs associated with CoP until clarity is given on the scope of the Direction, implementation timelines and an understanding of consumer adoption is known.

For example; if sending CoP requests from Non-Payment accounts are in scope of the Direction then this will impact the cost benefit, as the benefit is not substantial.

**Question 14** - What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that

imposed April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?

It is believed that the dates proposed (all PSPs to be able to Receive by 1<sup>st</sup> April 2019 and all PSPs to be able send by 1<sup>st</sup> July 2019) will have a negative impact on the costs & benefits. Atom suggests that by extending the timelines to one that is proposed by an industry delivery group as outlined in the answer to Question 1 will greatly reduce the costs and significantly increase the benefits from consumers.

*“This is the key concern for Atom as the potentially harmful consequences of an ineffective delivery will undoubtedly outweigh any short-term benefits: if consumers perceive the solution negatively, it is likely to be subject to slow adoption rates and will therefore not act as a protection from APP scams & misdirected payments.*

Atom also would like to highlight that many PSPs are looking to use common suppliers to deliver their CoP solution. This poses additional risks including:

- The delivery of CoP may be deficient due to capacity challenges / significant pressure on the suppliers.
- Smaller participants may not receive the same support from suppliers as larger participants because of prioritisation.
- Due to the timelines for delivery, PSPs may be at a competitive disadvantage and may not be able to use preferred suppliers to meet tight deadlines.

Whilst Pay.UK have developed the CoP proposition Atom believes there is a gap which must be filled for delivery of this proposition. Atom would support a body, such as Pay.UK or UK Finance, facilitating the creation of an industry delivery group to:

- Take responsibility to develop a coordinated delivery plan with participants and suppliers;
- Act as a forum to support the ecosystem to progress against this delivery plan;
- Seek to understand and mitigate risks of delivery, such as those associated with common suppliers and suboptimal delivery methods;
- Have the mandate to raise and escalate all identified risks appropriately; and
- Have appropriate knowledge and skills to ensure that the delivery of the solution achieves a network effect across the industry to ultimately result in mass adoption by consumers.

*As mentioned, Atom believes that a Direction from the PSR may act as a catalyst for PSPs to deliver CoP however to ensure that this is done successfully, the Direction and timelines associated with it, should only be confirmed following analysis from the above-mentioned delivery group.”*

## Equality Impact Assessment

**Question 15** - Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?

Atom feels that the timelines proposed by the PSR will not give PSPs the appropriate time to consider implications of the proposition on those consumers who are vulnerable or are within protected groups.

Whilst vulnerable consumers will get significant benefit from CoP, the proposition must be built to be inclusive of all disabilities and Atom believes more work is still required for the proposition to be fully inclusive. An example could be those consumers who struggle with sight, the method in which the CoP response is relayed back to the consumer must be consistent and effective across participants but may not always best done so via a user interface.

It is believed that a coordinated approach across the industry to deliver CoP via an Industry Delivery Group (response to Question 1) will enable a better assessment of how best to meet the needs of all consumers.

# Bank of America Merrill Lynch

## Consultation on general directions on Confirmation of Payee - Questions

Number	Question	Bank of America Comments
1	Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?	<ul style="list-style-type: none"> <li>• We believe that mandating this as an industry requirement is the correct approach provided that the deadlines are achievable.</li> <li>• This is due to our experience with the SEPA migration also being mandated which increased adoption.</li> </ul>
2	Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?	<ul style="list-style-type: none"> <li>• We agree that all PSPs should be subject to this CoP rule as well as needing to be able to respond and send CoP requests.</li> </ul>
3	Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?	<ul style="list-style-type: none"> <li>• We agree that all PSPs should be subject to this CoP rule as well as needing to be able to respond and send CoP requests.</li> </ul>
4	Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?	<ul style="list-style-type: none"> <li>• The urgent nature of CHAPS payments may mean that waiting for or querying the returned information of a COP request delays a critical payment.</li> <li>• This constraint doesn't apply to FPS which are not real-time settled nor are they for as high a value as CHAPS payments on average.</li> <li>• As such we would like to understand the SLA for responding to a COP request</li> <li>• There are some channels where a corporate or individual asks their PSP to effect a GBP payment without specifying the clearing. Where a PSP has a high level of interoperability their back office engine may be nimble enough to settle the payment by all three UK payment clearings e.g. settle via FPS instead of CHAPS as CHAPS has closed, settle via BACS instead of CHAPS as the sort code is only BACS reachable etc. If the PSR only mandates COP for certain clearings it may actually make the technology build more complex for PSPs, it may be easier to have CHAPS/BACS/FPS all in scope, or at least move to this model long term</li> <li>• We would like to understand why BIC and IBAN appear to be out of scope as a number of our corporates provide us with this to effect payments</li> </ul>
5	Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?	<ul style="list-style-type: none"> <li>• There should be consideration of the requirements when making single payment initiated through online channels (ad-hoc payments) and those from a regular file base transmission.</li> <li>• There should also be consideration of alias based processing such as Pay-M, PayPal etc.</li> </ul>
6	How should any directions deal with the potential for people to opt out of the CoP process?	<ul style="list-style-type: none"> <li>• Providing account holders with the right to individually opt out increases the complexity of implementation. This is due to there now being the possibility of two separate populations within the in-scope CHAPS and FPS payment worlds; those that have/haven't opted out.</li> <li>• If an individual/corporate opts out of this process and a subsequent fraud occurs we would not expect the bank to be liable for any potential loss</li> </ul>
7	Should any directions cover the sending of money from both individual and business accounts?	<ul style="list-style-type: none"> <li>• APP fraud affects corporate as well as retail users therefore there is no immediate need for BAML and it's business/corporate client base to be excluded.</li> </ul>
8	Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?	<ul style="list-style-type: none"> <li>• Agree that bifurcating the implementation dates ensures that CoP is deliverable in a safe and stable fashion.</li> <li>• We agree that mandating the ability to respond to COP requests should come before mandating the ability for banks to allow clients to send these</li> </ul>
9	Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.	<ul style="list-style-type: none"> <li>• The effectiveness of COP is, as highlighted in the report, derived not only by making sure it is widely adopted but also through it being accurate and robust. In light of the technological change required on all front end systems, a four month window appears to be too short to enable robust technical building and testing of the COP feature that has both client and PSP impact.</li> <li>• We believe the deadlines are inappropriate and should be pushed further out.</li> <li>• We believe a 12 month implementation period for PSPs to respond to COP requests would be more realistic</li> <li>• We believe a 15-18 month implementation period for PSPs to send COP requests would be more realistic</li> <li>• In the absence of any technical documentation these are our best estimates, when these are published these may change and be pushed out further</li> </ul>
10	Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?	<ul style="list-style-type: none"> <li>• No</li> </ul>
12	Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.	<ul style="list-style-type: none"> <li>• Depending on the level of accuracy required for the name match, we believe that the costs could vary. If the accuracy needs to be higher, then the costs will be higher.</li> </ul>

Barclays

# Payment Systems Regulator (PSR) consultation on general directions on implementing confirmation of payee

## 1. About Barclays

- 1.1. Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

## 2. Executive summary

- 2.1. Barclays welcomes the opportunity to provide a response to the PSR's consultation on general directions on implementing confirmation of payee.
- 2.2. Barclays understands the importance of there being a comprehensive approach to both tackling the increasingly common and sophisticated scams which can cause significant financial and non-financial detriment to consumers, and to providing customers with greater certainty that they are paying the individual or organisation that they intend to.
- 2.3. We therefore welcome the confirmation of payee initiative, which we believe will help provide consumers with greater assurance when they make payments. Importantly, we believe that confirmation of payee can help reduce payments made in error, as well as contributing towards combatting maliciously misdirected payment scams.
- 2.4. From our understanding of consumers and businesses' behaviours, and the workings of the UK's payment systems, we believe that to have the greatest positive impact it is important that the confirmation of payee initiative encompass all Payment Service Providers (PSPs). Through this universal adoption, consumers and businesses would be guaranteed a consistent payment experience – whoever they are paying – helping maximise the benefits secured from the initiative and building trust in the overall payments ecosystem.
- 2.5. Furthermore, we believe that all PSPs should implement confirmation of payee across their consumer-facing channels.
- 2.6. This is not to underestimate the scale of this challenge. Confirmation of payee could be the biggest change in electronic inter-bank payments since the introduction of the Faster Payments Service (FPS), and it will add an extra step to the initiation of every new real-time or same day payment.
- 2.7. Indeed, there are a number of significant challenges that participants, Pay.UK and PSR must work together to address. These include:
  - Changing user behaviour: Often payers do not provide sufficiently accurate information to receive a positive confirmation of payee response. This will have to change, and the industry must work with consumers and businesses to make this change happen.
  - Confirmation of payee requires payee PSPs to implement fast and resilient matching services. The industry must have sufficient time to build, test and prove those capabilities before implementation with customers.

- The Pay.UK specifications and governance documents for the service need to be stable, certain and sufficient. We need certainty on the service's data transfer arrangements and an appropriate liability model or we risk poor outcomes for consumers and businesses.

2.8. However, they are challenges that can, with the right cooperation between all the participants in the payments ecosystem, be overcome. We would therefore welcome the PSR's guidance and assistance in helping industry to resolve the aforementioned issues. With this help, industry will have a greater chance of launching a confirmation of payee service that commands the confidence of all payment service users, and delivers the greatest benefits. We would suggest that this guidance, including plans to resolve the aforementioned issues, be delivered in advance of the PSR imposing any directions in relation to confirmation of payee.

2.9. Barclays can understand why PSR wants to move quickly; we understand why PSR thinks *respond directions* have merits as they could help ensure ubiquity of the service. We do think that if *respond directions* are imposed it should apply to all PSPs with accounts in scope of the service. However, we do not think PSR should impose the *send directions* in the form proposed. We think that PSR should instead require the production of detailed implementation plans that explain a PSP's plans for the rollout of confirmation of payee.

### 3. Reflections on Pay.UK's confirmation of payee service

3.1. We want confirmation of payee to be a success, and we have worked closely with Pay.UK to ensure that their confirmation of payee service achieves the PSR and industry's ambitions. We believe that all PSPs with payment accounts in scope of the service must be able to respond to a confirmation of payee messages. PSPs should also implement confirmation of payee across their consumer-facing channels.

3.2. As we believe confirmation of payee must apply broadly, then we think the introduction of confirmation of payee has the potential to be the most significant change in UK interbank electronic payments since the introduction of FPS. It will add an extra step to the initiation of every new real-time or same day payment [REDACTED]

[REDACTED]

3.3. Considering this level of change, we have some observations that we would like to highlight to PSR. We want to work with PSR and the rest of the industry to solve these issues so that confirmation of payee is the success we all want it to be.

#### The customer behaviour challenge

3.4. The biggest challenge to make confirmation of payee a success will be to change user behaviour. We believe the industry needs to work together to achieve this change. Under confirmation of payee consumers and businesses will have to provide sufficiently accurate information to receive a *yes* or *close match* response. [REDACTED]

[REDACTED]

[REDACTED] If they do not, they will get a *no* or *close match* response. This may cause

[REDACTED]

difficulties for customers and they may end up using alternative methods of payment or just not make the payment.

- 3.5. Similarly, businesses can have account names that differ substantially from the name of the company. Businesses often include their bank account details on their invoices, but this tends not to include the account name details. They will need to alter their approach to ensure that they receive the monies owed to them. This change will take businesses time and cost them money.
- 3.6. This is not just a theoretical problem. We know that the payee name information provided by payers often bears minimal resemblance to the account name information that we hold on the payee. [REDACTED]
- 3.7. In practice, we do not know how consumers will react to a *no* or *close match* response, and we do not control how the payer PSP collects the payee name information from their customers. We hope that when the industry introduces confirmation of payee, payer PSPs will have an incentive to redesign their channels and processes so that they obtain the correct information from their customers, but we have no guarantee that this will happen. The industry needs to work together to make sure it does.

**Implementing confirmation of payee safely**

- 3.8. The second biggest challenge of confirmation of payee is ensuring a smooth and safe implementation. We think sufficient testing and sensible implementation are a prerequisite. Confirmation of payee requires a fast data exchange between PSPs. It is reliant on the different technical solutions adopted by different PSPs and the robustness of the Open Banking directory. If we are the payer PSP we have no control over the speed, the capacity and the resiliency of the technical solutions adopted by the payee PSP. If a payee PSP is slow to respond, fails to respond, or responds unexpectedly what do we tell our customers and how will they react? We believe that poor performance in the network will affect the confidence that consumers have in confirmation of payee.
- 3.9. We know from our experience of Open Banking that the time taken to respond to a message can vary dramatically between participants. [REDACTED] So adequate testing of the speed of responses in a variety of circumstances is a prerequisite for success.
- 3.10. The speed of response is just one dimension; capacity and resiliency are also crucial. In many respects, confirmation of payee brings a greater reliance on other PSPs' technical infrastructure and the Open Banking directory. It puts them into the centre of UK payments infrastructure. Currently, if a PSP is having technical difficulties with its FPS connectivity it can adopt a position where it is able to accept payments, but not send them. This allows other PSPs and their customers to continue making payments to the impacted PSP without really noticing any difference. When confirmation of payee has launched, a payer will become aware very quickly if a payee PSP is having technical difficulties with its matching solution. We do not know how customers will react in such circumstances; they may make the payment and take the risk, try a

confirmation of payee request again, or make the payment some other time or in some other way.

- 3.11. Similarly, PSPs will be reliant on the accuracy and stability of the Open Banking directory to know where to send their confirmation of payee requests. We have not seen any detail on the agreements between Pay.UK and the Open Banking Implementation Entity (OBIE), but we think they are critical to the success of the service. Pay.UK and PSR need to consider how the reliance on the directory should be governed; this would include understanding the legal frameworks, controls, funding, and the overall capacity of OBIE to support confirmation of payee.
- 3.12. We would expect a testing and proving stage of a sufficient period so that the industry can be confident that the various implementations of the confirmation of payee service are robust, resilient and user-friendly. We would not support the truncated schedule that the PSR's proposed directions imply. We advocate a testing and launch schedule akin to that used for the Current Account Switching Service (CASS).

#### The Pay.UK specification and governance documents

- 3.13. We do not consider that when PSR published its consultation document on confirmation of payee the specification and governance documents for the service were complete and ready for implementation by PSPs. We need stability of the proposition, certainty on the service's data transfer arrangements and a clear liability model.

3.14. [REDACTED]

3.15. Through the reviews of the available documents, we have three main concerns. The first is the instability of the proposition. Until we are presented with a stable specification and final suite governance documents it is difficult to proceed at pace. [REDACTED]

3.16. Another critical issue is the data transfer that will occur in confirmation of payee. In a *close match* response payer PSPs will receive personal data relating to individuals who are not necessarily their customers, [REDACTED]. The payer will also get this personal data and they may have no connection with the data subject. All of this will happen without the consent of the data subject. Pay.UK has completed a *legitimate interests* assessment of confirmation of payee. It has concluded that the data processing and transfer to third parties without the data subject's consent inherent to the confirmation of payee service is lawful based on *legitimate interests* in the Data Protection Act 2018 (the UK legislation that implemented the General Data Protection Act 2018).<sup>4</sup> That may be the correct interpretation, but the integrity of

<sup>4</sup> Page 12, Pay.UK (October 2018), *Confirmation of Payee: Understanding consumer and stakeholder perspectives*, <<https://www.paperturn-view.com/?pid=MzU35982>> [accessed January 2019]

the entire service turns on that assessment. In the light of recent scandals where citizens' data has been given to others without their consent, we think a level of caution is sensible. [REDACTED]

3.17. We expect that confirmation of payee will lead to a significant level of personal data transfer and storage. [REDACTED]

[REDACTED] PSPs that participate in confirmation of payee will quickly amass large amounts of personal data that does not belong to their customers and was obtained without the data subject's consent. We think it is important to have certainty that ICO does not object to the reliance on *legitimate interests* for confirmation of payee, and to ensure that the underlying data protection rules and governance for confirmation of payee are sufficient.

3.18. [REDACTED] PSR should also assure itself that the confirmation of payee service includes a suitable and robust approach to data protection, data security, and has adequate processes to manage any data breaches. We believe that these processes must consist of the contractual right of recourse if a data breach by another participant in confirmation of payee leads to customer loss.

3.19. [REDACTED]

#### The way forward

3.20. We believe that if we resolve the issues we have highlighted above the industry will have a greater chance of launching a confirmation of payee service that commands the confidence of all payment service users. To this end, we have asked Pay.UK to support testing, implementation and communications around confirmation of payee. We extend our request to PSR. However, we do think that the approach and timelines proposed by PSR in its consultation might require reconsideration.

3.21. We believe that if PSR decides to impose *respond directions*, it must only do so once it has confirmation that ICO does not object to the data transfer inherent to confirmation of payee, and that the data protection arrangements are sufficient. It also must impose *respond directions* on all PSPs with payment accounts in scope of Pay.UK confirmation of payee service. We think PSR should be more flexible with the *send directions*. We think that sufficient time needs to be devoted to the testing of the service and a credible plan to change customer behaviour developed. When PSPs do implement confirmation of payee, it should be on managed rollout basis and not rushed.

[REDACTED]

#### 4. The PSR's approach

Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce confirmation of payee the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?<sup>6</sup>

- 4.1. Barclays can understand why PSR believe that directions to require PSPs to respond to confirmation of payee requests (the *respond directions*) have merits. To help combat malicious misdirection scams the service has to have ubiquity. PSR may conclude that a regulatory intervention to accelerate the deployment of matching solutions by payee PSPs will help achieve that ubiquity. However, we do not think that the use of PSR's powers to rollout of confirmation of payee to a PSPs' customers (the *send directions*) in the manner currently envisaged is appropriate. We consider that a more flexible approach than directions may be desirable. We expand on our views on this later in this response.
- 4.2. We do agree that confirmation of payee will assist in efforts to reduce Authorised Push Payment (APP) scams and accidentally misdirected payments. However, PSR must guard against overstating the efficacy of confirmation of payee at combatting APP scams.
- 4.3. The vast majority of APP scams are malicious payee type scams (malicious payee scams accounted for 79% of all cases in H1 2018).<sup>7</sup> PSR does acknowledge that confirmation of payee is unlikely to have an impact on these type of scams; and the benefits case is based on combatting malicious misdirection style scams. Malicious misdirection style scams do tend to have a higher value per case, and accounted for 65% of the value of cases in H1 2018.<sup>8</sup> They warrant attention on that basis. Nevertheless, we have some concerns that unreasonable public and media expectations are being set about confirmation of payee. Consumers need to understand that a yes response does not mean that the goods a fraudster is ostensibly selling them exist. All it does is confirm that the name provided to the victim by the fraudster *matches* the name on the account where the victim is sending money. PSR can help by being clearer on these limitations.
- 4.4. It is also worth remembering that the payment is merely the last step of a scam and focussing on this aspect, while logical, is limited. In our view, and as we set out in our response to the contingent reimbursement model consultation, policymakers – including PSR – should take the opportunity to adopt a long-term and all-encompassing view of the issue of scams. Government and regulators should set out the actions that are required from all players in the APP scam ecosystem to stop the scams before the customer attempts to make a payment to a fraudster. This would include technology platforms and companies, the telephony industry, conveyancers and law firms, and pension firms. By the time a victim is filling out a payment instruction successful intervention is harder and not as effective.
- 4.5. Extending regulation so that other actors in the ecosystem are required to ensure that fraudsters cannot use their systems and services should be a higher priority. We think that PSR, working with Government and FCA, must consider what other actions need doing to ensure that scams are prevented at source.
- 4.6. Failure to strike at source gives fraudsters the opportunity to alter their *modi operandi*. Such criminals may even exploit interventions like confirmation of payee to provide victims with false confidence. For instance, fraudsters may utilise organisations with similar names, dupe

---

<sup>6</sup> Please note that where appropriate we have combined our answers to PSR's consultation papers to minimise duplication

<sup>7</sup> Based on 27,059 malicious payee cases out of 34,128 in total in H1 2018. Figures from table titled "YTD Overview," UK Finance (September 2018), *2018 half-year fraud update: Authorised push payment fraud industry statistics, January to June 2018 (annexe)*, <<https://www.ukfinance.org.uk/wp-content/uploads/2018/09/APP-Appendices-File-June-18-Release-ONLINE.xlsx>> [accessed January 2019]

<sup>8</sup> Malicious redirection accounted for £93.9 million out of £145.4 million in total in H1 2018, Figures from table titled: "YTD Overview," UK Finance (September 2018), *ibid*

customers to use or expect a different account name, or exploit change of name processes. Fraudsters may also turn their focus to payment accounts or payment systems not in scope of the service designed by Pay.UK. For instance, Bacs payments accounted for 10% of the value of malicious redirection scams in H1 2018.<sup>9</sup> Fraudsters targeting non-personal customers have tended to shy away from this payment system due to the three-day processing cycle. While Pay.UK does intend to extend confirmation of payee to include Bacs payments, in the meantime fraudsters may be willing to be patient and exploit the fact that the confirmation of payee service is only focussed on FPS and CHAPS transactions.

- 4.7. We must also acknowledge the role of data breaches in seeding such scams, and those responsible made appropriately liable for their role in enabling such scams. Provision of information on their victims allows criminals to engineer their interactions with the victim socially. As we have already noted, the confirmation of payee service will create very large databases of individuals' confirmed account details which, if breached, could aid criminals in their activities.

## 5. The scope of the directions: PSPs

Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?

Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?

- 5.1. Confirmation of payee will be most useful if it provides an even and ubiquitous experience across all users. This is why if PSR decides to introduce *respond directions* it should do so on a broad basis.
- 5.2. It is our view that all PSPs that provide payment accounts that can receive a FPS or CHAPS payment addressed only by sort code and account number – and so in scope for Pay.UK's confirmation of payee service – should be able to respond to a confirmation of payee request. The reasons for our position are twofold: To ensure the customer experience of confirmation of payee is consistent; and, to reduce the risk of negative selection of PSPs by fraudsters, and maliciously misdirected payments continuing unabated.
- 5.3. We think it is essential that once confirmation of payee is generally available the customer experience should be similar. A Barclays' customer paying, for example, a Lloyds' customer through their Barclays' application will expect the same experience when they are paying, for example, a Tesco Bank customer through the same application.
- 5.4. We also believe that all PSPs with accounts in scope of the service should be included to reduce the risk of negative selection biases. Criminals may seek to identify and utilise mule accounts with those PSPs out of scope for the *respond directions*. Such criminals are adept at social engineering  
[REDACTED]  
[REDACTED]  
[REDACTED] Victims will make such payments, and this may jeopardise overall consumer confidence in the service and reduce the benefits of the service.
- 5.5. We appreciate that there is a technical challenge to be able to *respond* to confirmation of payee messages. PSPs will have to enrol in Open Banking, as well as to build or procure the matching service. This may have an impact on PSR's proposed timescale.
- 5.6. We do not support the *send directions* as currently framed. We expand on our views on this later in our response.

<sup>9</sup> Calculated from table titled: "YTD Payment Type," UK Finance (September 2018), *ibid*

<sup>10</sup> 5.D.xi.1, Pay.UK (30 November 2018), *Confirmation of Payee Operating Guide, version 1.2*

## 6. The scope of the directions: Products and services covered

Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?

Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?

- 6.1. Barclays agree that if PSR imposes *respond directions* they should apply to inbound FPS and CHAPS payments. However, we remain unpersuaded that the proposed *send directions* are the most appropriate method of safely achieving PSR's objectives. We believe that PSR should be more flexible.
- 6.2. As we made clear in section three of this response, successful delivery of confirmation of payee requires a significant level of user behaviour change. Considering the need for widespread user change, we do not think that a hard and immovable deadline to rollout an unproven service to the UK public is sensible.
- 6.3. We have no evidence about how a consumer would react to a *no* or *close match* response in practice. We do not know what consumers will understand by a *yes* response. We do not know if the infrastructure, in Open Banking and within other PSPs, is resilient for the expected volumes, and we do not know whether PSPs will be able to perform the matching in a sufficiently fast time. We do not know what channel changes and customer messages will be effective at getting the correct payee information from payers.
- 6.4. We believe that PSPs will need to *live prove* their matching approaches and assess the impact of channel changes to ensure that customers are providing the correct information. The *live proving* will also give PSPs the opportunity to understand the resilience of the matching infrastructures within PSPs and the time taken to produce matches.
- 6.5. While we do not support *send directions* as currently framed, we do recognise the desire of PSR to act quickly. However, the provision of only three months to complete the necessary testing and proving work, and rollout the service to all customer-facing channels is not realistic or safe. Like our recent rollout of Open Banking account information services, it takes time to deliver new services to customers. Customers need additional support and education to get used to new services, and we need to be confident that the service works and does what it supposed to do. PSPs also need to be able to take a step back if it is not working as expected or is causing customer difficulties.
- 6.6. The approach we think PSR should take is to require PSPs with payment accounts in scope for the confirmation of payee service to provide PSR with detailed implementation plans for confirmation of payee. Such plans would include:
  - detail on channels included in scope of their implementation, and explanations for any exclusions;
  - the current payment volume and expected volume for each channel (and overall share of payment volume);
  - the different customer base being addressed, for instance rollout could target consumer channels first, followed by SMEs and then corporates;

- the anticipated impact on maliciously misdirected APP scams at different points of the rollout and in different channels;
- the timescales envisaged;
- decision points and criteria for deployment; and,
- contingency planning.

- 6.7. PSR could review, challenge and, when content, approve such implementation plans. However, we believe that PSR should not demand a truncated proving stage. The implementation approach expected should reflect that of CASS.
- 6.8. If PSR wishes to persist with a hard deadline for the *send directions* and require rollout of confirmation of payee to any channel that could initiate an FPS or CHAPS payment, then we would welcome confirmation that the *send directions* can only apply to channels where the PSP directly controls the messages provided to customers; the customer is talking to a Barclays' employee, or we are providing a graphical user interface (GUI) directly to the customer. If we are not doing so, we cannot be sure that the customer receives the correct messages to support confirmation of payee. This would mean that direct submission methods, like direct corporate access for FPS and file input, would be out of scope, as would host-to-host connectivity, users of payment initiation service providers (PISPs), and SWIFT users. Although nothing should stop PSPs developing services for such channels should they wish to.
- 6.9. There may also be complications concerning our financial institution clients who may use one of our GUI channels for third-party payments. We would expect that since we do not have a contractual relationship with the instructing payer, we would not be responsible for providing the confirmation of payee service to the third party.
- 6.10. We also would be grateful for PSR, if it continues to pursue the directions as proposed, could provide clarity on how they expect the directions to apply to payments to and from accounts in the Channel Islands and the Isle of Man (where payments are made through the same channels as the UK). And, if they are not in scope confirm that we are not precluded from bringing additional jurisdictions in scope.

**Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

6.11. [REDACTED]

6.12. Pay.UK is trying to balance the legitimate interest in the transfer of the personal data against the individual's interests, rights and freedoms. Therefore, we see the inclusion of opt-out as fundamental to the case that *legitimate interests* provide a lawful basis for the transfer of the personal data required by confirmation of payee.

6.13. But, as mentioned in section three of this response, we believe that any directions cannot proceed until consultation with ICO has taken place to confirm that it does not object to Pay.UK's interpretation.

**Question 7: Should any directions cover the sending of money from both individual and business accounts?**

6.14. If PSR persists with the *send directions*, we believe they should apply to all payment accounts within the scope of service. However, we do not think that Financial Institution clients should

have to *send* confirmation of payee requests in advance of making payments. This is particularly relevant for payments related to financial market infrastructures. We also think that larger companies should have the option of utilising confirmation of payee before initiating payments, rather than it being a requirement. Corporate clients may have existing payment workflows that would need amendment to accommodate a confirmation of payee request for new or amended mandates. Such firms may not be able to alter their workflows in advance of the deadlines proposed by PSR.

- 6.15. Although, as previously explained we do not think PSR should impose the *send directions* in the form proposed by PSR. We think that PSR should require the production of detailed implementation plans that explain a PSP's plans for the rollout of confirmation of payee. The implementation plans would explain which customer groups and channels would get the confirmation of payee service, when they will get it and on what basis (e.g. mandatory or optional).

## 7. The rationale for the PSR's timeframe

Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?

Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.

- 7.1. We support the separation of the directions. Barclays can understand why PSR believes *respond directions* have merits as they could help ensure ubiquity. However, we have proposed an alternative approach to the *send directions* to ensure a safe, sensible and timely rollout of confirmation of payee.
- 7.2. Concerning the timeline proposed, we do not consider that, at time of writing, we have sufficient clarity and certainty on the end-to-end confirmation of payee service from Pay.UK. We do not think it is reasonable to impose *respond directions* on PSPs until all relevant documents are suitable, stable and PSPs have sufficient time to implement. We also need to be comfortable that the data processing the service will require is lawful.
- 7.3. We strongly believe that all PSPs with payment accounts in scope for the confirmation of payee service must be able to provide responses to confirmation of payee requests. If PSR decides to impose *respond directions*, all PSPs with payment accounts addressable by sort code and account number must be in scope of those directions. However, we recognise that this will further challenge the deadline proposed. In that case, PSR may wish considering delaying any *respond directions*.
- 7.4. With the *send directions*, we have suggested an alternative approach that will, we believe, achieve PSR's objectives in a more sensible and less disruptive manner. If PSR rejects our suggestion, then we urge PSR not to impose a deadline of the 1 July for the *send directions*. PSR should not underestimate the level of consumer change necessary to make confirmation of payee a success; the need to ensure the resiliency of the PSP infrastructure that will support confirmation of payee; and, all the while maintaining a smooth customer experience. PSR should await successful delivery, testing and proving of the *respond* functionality before acting.

## 8. Other alternatives:

Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?

- 8.1. We have provided an alternative approach to the *send directions* at our answer to questions 4 and 5. We do not agree with the *send directions* as currently framed. We think that PSR should instead require the production of detailed implementation plans that explain a PSP's plans for the rollout of confirmation of payee. The implementation plans would explain which customer groups and channels would get the confirmation of payee service, when they will get it and on what basis (e.g. mandatory or optional).

## 9. Cost benefit analysis

Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?

- 9.1. We are responding to the PSR's information request that will provide further information to enhance PSR's cost benefit analysis. However, we would like to take this opportunity to make a number of points.
- 9.2. We consider that expectations on the efficacy of confirmation of payee at combatting maliciously misdirected payment scams will turn on the inclusion of all relevant PSPs within PSR's *respond directions*. Failure to do so will leave an opportunity for fraudsters to continue their activities. We also note that PSPs that provide payment accounts addressable using secondary reference data will not be in scope of the first phase of the confirmation of payee service. Until we understand the scope of any directions from PSR, we think it is difficult to agree with PSR view that confirmation of payee will prevent 90% of malicious misdirection scams.
- 9.3. The benefits case does not consider the displacement effect. We expect fraudsters will soon find new opportunities and exploit them. This is why we advocate an approach to combat scams at source.
- 9.4. Finally, we would like clarity on £93.9 million figure that underpins the benefits case.<sup>11</sup> That figure is the total value of malicious redirection scams in H1 2018. However, we understood that £93.9 million consisted of redirection scams from all different payment types, not simply FPS and CHAPS payments.
- 9.5. According to UK Finance published data, the £93.9 million consists of £60.3 million of FPS malicious redirection scams, £10.8 million of CHAPS payments, £9.3 million in Bacs transactions, £0.8 million in inter-bank payments, and finally £12.6 million of international payments.<sup>12</sup> Our

---

<sup>11</sup> Page 20, PSR (November 2018), *Consultation on general directions on implementing Confirmation of Payee*, <<https://www.psr.org.uk/sites/default/files/media/PDF/PSR-CP-18-4-consultation-general-directions-confirmation-of-payee.pdf>> [accessed January 2019]

<sup>12</sup> Figures from table titled: "YTD Payment Type," UK Finance (September 2018), *ibid*

understanding of the proposed scope of PSR directions, and the confirmation of payee service designed by Pay.UK, is that it would only apply to FPS and CHAPS payments (although phase two of Pay.UK's programme will extend to Bacs payments). In our view, this would mean that the directions proposed would only address £71.1 million of APP scams that typically involve malicious redirection, not £93.9 million.

- 9.6. Based on the three above points, and assuming our interpretation is correct, we believe PSR should revisit its cost benefit analysis.

## 10. Equality impact assessment

Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?

- 10.1. Barclays has no specific comments on the equality impact assessment. [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] PSR and Pay.UK should ensure that the final service has adequate protections for *at risk* individuals and should monitor the impact post implementation. We would not support the service unless it incorporates robust safeguards for vulnerable individuals into the process.
- 10.2. We also think that PSR or Pay.UK should commit to monitor and conduct a post-implementation review of the impact of Pay.UK's confirmation of payee service on those payers and payees with protected characteristics and vulnerable individuals. We consider that the service design will pose specific additional difficulties for vulnerable and protected individuals. Individuals who may face additional difficulties are likely to include; those individuals that struggle with basic literacy skills or dyslexia; individuals who do not speak English as a first language; and, individuals whose ethnic background may mean that they have complex first and family names, for instance their name may originate from a different alphabet and rendered into the Latin alphabet.

- 10.3. [REDACTED]

# British Retail Consortium (BRC)



BRITISH RETAIL CONSORTIUM  
4<sup>TH</sup> FLOOR, 2 LONDON BRIDGE  
LONDON, SE1 9RA  
+44 (0)20 7854 8900  
BRC.ORG.UK

## BRC response to PSR consultation: General directions for the implementation of Confirmation of Payee (CoP)

January 2019

### Introduction

- 0.1 The British Retail Consortium (BRC) is the trade association for the entire retail industry, the UK's largest employer, with a membership accounting for half of UK retail by turnover. Our diverse industry spans large multiples, independents, high street and out of town retailers, from online to bricks and mortar, selling goods across all sectors to increasingly discerning consumers.
- 0.2 All BRC members have an interest in the payment system as end users, in fact retailers are one of the most significant end user groups, processing more than 50 million transactions per day and around £366 billion per year for products & services sold in store, online & over the phone. A priority for the BRC has therefore been to ensure an innovative, transparent and competitive payments market for all retail end users and their customers.
- 0.3 As the PSR has rightly identified, the losses to individuals and businesses of scams and accidentally misdirected payments can be significant and life changing. More needs to be done to protect people and businesses from scams and Confirmation of Payee (CoP) is one important tool for prevention.
- 0.4 The BRC welcomes that technical standards for CoP have now been agreed and are ready for implementation by banks and other payment service providers (PSPs). CoP should now be implemented quickly, in a coordinated way, without any undue delay, and it must be widely available to individuals and business – whoever they choose to bank with.
- 0.5 Now that CoP is available it should be supported ubiquitously across all relevant payment channels – FPS and CHAPS – by all PSPs. Adoption of CoP must be a regulatory requirement, and PSPs should not be free to operate if they will not adopt such an elementary tool of due diligence to protect their customers.
- 0.6 Regulatory intervention is also required for the sound logical reasons set out by the PSR under section 3 (3.13) of the consultation paper, and the BRC agrees that directions are the best way to achieve the roll-out of CoP in timely and coordinated fashion.
- 0.7 The BRC strongly encourages that these directions cover the sending of money from both individual and business accounts given that, as the PSR states in section 4 (4.19) of the consultation document, “both individuals and businesses can be victims of scams and can suffer from accidentally misdirected payments.”
- 0.8 The need for either individuals or businesses to opt out of CoP (for which few legitimate reasons present themselves) is easily outweighed by the need to ensure the efficacy of CoP – the ability to identify the recipient of their payment is a not a high expectation for a payer to impose upon a payee.

# Building Societies Association (BSA)

# Consultation on general directions on implementing Confirmation of Payee

Response from the BSA

Restricted  
02 January 2019



Set out below is the response from the Building Societies Association to the above consultation.

The Building Societies Association (BSA) represents all 43 UK building societies, as well as 4 credit unions. Building societies have total assets of over £400 billion and, together with their subsidiaries, hold residential mortgages of over £315 billion, 23% of the total outstanding in the UK. They hold almost £280 billion of retail deposits, accounting for 19% of all such deposits in the UK. Building societies account for 37% of all cash ISA balances. They employ approximately 42,500 full and part-time staff and operate through approximately 1,470 branches.

The BSA and BSA members support the Payment Services Regulator's (PSR's) overarching objectives in respect of reducing levels of authorised push payment (APP) fraud and the harm it causes.

## Summary

The BSA and BSA members support the objectives of Confirmation of Payee (CoP). We also support the need for a clear timetable for introduction of CoP in order to give certainty to firms and reassurance to consumers.

We understand the technical logic of splitting CoP into two phases – though lower APP fraud protection for some consumers will have to be addressed in consumer messaging at launch of Phase 1.

However, we do not believe the timetable for Phase 1 proposed in this consultation to be realistic:

- **We need urgent clarification as to whether CHAPs and FFP transfers to and from savings accounts with an addressable sort code are to be included in Phase 1 or Phase 2. This will have a significant effect on some of our members' ability to meet any proposed timetable.**
- Firms, outsourcers and the PSR itself anyway have a great deal to complete for the build phase of CoP1 to be ready by 1 April 2019.
- Pay UK has already raised concerns about Open Banking's and its own capacity on on-board all phase 1 firms by 1 April.
- There are no visible plans for testing CoP between firms – essential if the requirement that all Phase 1 PSP must be capable of receiving and responding to CoP requests from other PSPs.
- There are potential competition issues if smaller firms are disproportionately impacted by the intensive development requirements – particularly if they are pushed out of the market for outsourced CoP services and specialist technical resource.
- There appears to be no central coordination of crucial aspects of delivery such as testing, communications or consumer education.
- The timetable appears not to have taken account of concurrent activity required by other regulators – again this is particularly relevant to smaller firms.

While the BSA is a relative newcomer to CoP, from our perspective the PSR's proposed timetable doesn't allow enough time for the above to be done properly and therefore carries significant risk. We would recommend the following next steps:

- The PSR reviews all of the above - including liaison with the other financial services regulators on their plans for 2019 - so that an informed decision on an alternative timetable can be made.
- Options might include sub-phasing delivery of Phase 1 with those firms who are most ready to deliver CoP going first.
- CoP should be formally set up as an industry delivery programme led by a suitable body from the payments sector with accountability for co-ordinating the industry's approach to build, testing and launch (as Pay UK did for the design solution) and delivering Phase 1 to whatever timetable is set - and then to design and deliver Phase 2 of CoP.

## The position of building societies

Building societies who offer current accounts are well-advanced in their CoP Phase 1 preparations – though they still see considerable risk in the PSR's proposed timetable.

Building societies who offer CHAPs and FFP transfers to and from savings accounts with an addressable sort code are currently unable to move forward as Pay UK has not been able to confirm whether these accounts are in scope for Phase 1 or Phase 2 of COP. Pay UK's latest opinion as of December 2018 was that these accounts were “possibly in scope” for Phase 1.

**This places CoP provision for millions of savings accounts at building societies, banks, credit unions and other providers in limbo – which is unacceptable at this late stage. Could the Payment Services Regulator arrange for clarification to be provided as a matter of urgency?**

The majority of smaller building societies will fall into Phase 2 as providers of “transactions to or from a Head Office Collection Account (HOCA) and then associated with a roll number or other identifier” through offering CHAPS payments to and from savings accounts via the CHAPs facilities of a sponsoring bank. Plans for supporting Phase 2 firms and consumers to mitigate the lower level of protection against APP fraud that they will receive need to be incorporated into the launch of Phase 1.

We continue to be concerned that though the decision as to the scope of Phase 1 and 2 was made by Pay UK and the Payments Forum “with industry participation” neither body consulted with representatives from building societies or others outside of the clearing banks at the time. There has been a similar lack of wider industry consultation during the development of the draft CRM code.

We want to make sure that lessons are learned for the delivery of CoP phase 1 and development of CoP Phase 2. The BSA and our members will commit to working closely with Pay UK and others – if asked - to deliver an appropriate way forward.

## Our comments on individual consultation questions:

*Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.*

We strongly agree with the need for a co-ordinated timetable for delivery of CoP to give clarity to firms and reassurance to consumers. However, the consultation's proposed timetable for PSPs using FPS and CHAPS (set out below) is heavy with risk.

- By 1 April 2019: A PSP must be capable of receiving and responding to CoP requests from other PSPs.
- By 1 July 2019 A PSP must send CoP requests and present responses to their customers.

Pay UK have informed us that CoP Phase 1 will require 300 PSPs to prepare to build, test and launch COP infrastructure based on a design released in October 2018.

- Pay UK tell us that they engaged with "around 200 PSPs" in the design stage – which presumably means that 33% of the PSPs that need to be ready to build to this design have not been party to the design phase of CoP and have a significant amount of work to catch up on by 1 April 2019.
- In December 2018, Pay UK were unable to confirm whether savings accounts with an accessible sort code are within scope of Phase 1 or Phase 2 (see above).

To meet the proposed deadline of 1 April 2019, 300 PSPs will have had to have built and tested their CoP infrastructure, including requirements to participate in Open Banking and register with Pay UK.

- Pay UK have expressed concerns about the ability of Open Banking to handle the required volume of new participants.
- Pay UK themselves are unsure of their own capacity to on-board the required number of PSPs within a short timescale.
- Where firms are using / considering an outsourcing arrangement as the delivery option for CoP infrastructure, all firms in this situation will have needed to complete supplier due diligence on their chosen outsourcer – and probably at least on other – before they select their partner and build their CoP infrastructure.
- Time pressure will also create competition issues where larger firms can use their size to gain priority access to outsourcers and specialist contractor / consultant resource whereas smaller firms are likely to struggle for access.
- CoP testing will need to be a standardised approach so the all parties can test interfaces with other firms on an equal basis and have time to iron out any problems encountered. Testing is usually against a centrally developed test script for consistency of approach.
- We presume that, as regulator, the PSR will also want to have completed risk assessments on concentration risk associated with a small number of outsource providers providing CoP services to PSPs and on operational resilience impact tolerances etc. for CoP as a whole.

To meet the next proposed deadline of 1 July 2019, participating PSPs will need to have completed integration testing of CoP infrastructure, have completed development, build and testing of CoP at consumer-facing channels and prepared industry-wide usage instructions and communications messages for consumers – including an explanation of lower APP fraud protection for Phase 2 customers.

- We can't see any plans for delivering co-ordinated pre-launch requirements for CoP, either at individual firm or industry level, in this consultation or anywhere else.

In addition, pressures on firms' development resource and management time from other sources must be factored in. The regulatory world will not stand still and regulators' requirements on Open Banking, vulnerability, operational resilience etc. plus preparing for the other aspects of implementation of the CRM code will all have to be managed and resourced at the same time as CoP, plus ongoing upgrade and maintenance of systems & processes. This particularly affects smaller PSPs who do not have the depth of resource to take on significant additional development without corresponding opportunity cost elsewhere.

While the BSA is a relative newcomer to CoP, from our perspective the PSR's proposed timetable doesn't allow enough time for the above to be done properly and therefore carries significant risk. This is best summarised by feedback from a building society currently engaged on Phase 1 CoP preparations:

*"We are in agreement with the idea of CoP and its aims however April 2019 is a really struggle for us given the work required for PSD2. PSD2 relies on some of our key third party suppliers for delivery of the SCA and open banking work, some of which would also be required to deliver CoP and to add these requirements into the already tight schedule feels unachievable. The costs of delivery are understandable and can be factored into our 2019 plans but it is this reliance on our third parties that is our key concern."*

In terms of suggesting an alternative timetable, the BSA doesn't have the information needed as to how long above preparations will take firms, outsourcers, Pay UK, the APP Scams Steering Group and other stakeholders to deliver CoP alongside normal business and other regulatory policy implementation so cannot provide a definitive alternative.

We strongly suggest that, as a next step to this consultation, the PSR reviews all of the above - including liaison with the other financial services regulators on their plans for 2019 - so that an informed decision on an alternative timetable can be made. Options might include sub-phasing delivery of Phase 1 with those firms who are most ready to deliver CoP going first.

*Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally mis directed payments as soon as possible?*

*Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they?*

Direction from the PSR by itself is not the right approach to deliver CoP effectively to consumers and needs to be combined with creation of a CoP implementation programme to provide central co-ordination of the build, test and launch phases. Otherwise, it runs the risk of not achieving the PSR's objectives on reducing APP fraud within the UK.

As pointed out above, the PSR is not the only regulator operating in financial services who has powers to direct firms to particular courses of action and firms already know that both the PRA and FCA have extensive plans for regulatory initiatives in 2019. If regulators do not co-ordinate their requirements, firms, particularly smaller firms, will struggle with implementation – with a knock on effect on costs, resources and focus on providing day to day services to customers.

Also, given the size and complexity of CoP and its key role in supporting the CRM Code, we would have expected there to be some element of central programme management to co-ordinate design, build, test and launch across a large range of firms of different sizes and to take overall accountability for delivery of both CoP and implementation of the Code.

This lack of central co-ordination is evident in the variable on-boarding of firms at design stage and the obvious lack of co-ordination with the APP Scams Steering Group over the CRM Code. If this state of affairs continues into testing and launch - where central co-ordination is key to successful delivery and a consistent outcome for consumers - the risk of the PSR not securing its objectives becomes much greater.

We would strongly recommend that CoP is formally set up as an industry delivery programme led by a suitable body from the payments sector with accountability for co-ordinating the industry's approach to build, testing and launch (as Pay UK did for the design solution) and delivering Phase 1 to whatever timetable is set - and then to design and deliver Phase 2.

*Do you have any other comments on the issues raised above?*

We are also conscious of the potential knock-on impact on phase 2 if there are significant delivery problems for Phase 1. The phased approach already means that most building societies will not be able to offer CoP facilities to their customers (see below) which therefore makes both firm and customer exposed to higher levels of APP fraud. This will be longer and more risky if Phase 1 is not successfully delivered.

*Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?*

This consultation confirms that some PSPs and their customers will not be offered the benefits of CoP in Phase 1 leaving their customers less protected against APP fraud than customers of phase 1 firms. In particular “transactions to or from a Head Office Collection Account (HOCA) and then associated with a roll number or other identifier” will cover most building societies offering CHAPS payments to and from savings accounts via the CHAPS facilities of a sponsoring bank.

We understand the technical logic of postponing solution design for this until (a yet to be confirmed) Phase 2 of CoP but there will be implications. We expect that Phase 2 firms and their customers will be particularly targeted for APP fraud and the laundering of proceeds for fraud because of this decision.

Plans for supporting Phase 2 firms and consumers to mitigate the lower level of protection against APP fraud that they will receive need to be incorporated into the launch of phase 1.

*Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?*

Yes.

*Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?*

Yes. Direction should cover both FPS and CHAPS payments.

*Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from?*

Yes – though where a request for a CHAPS or FPS transfer is made at a branch counter firms should continue to use the Banking Protocol when they have suspicions that a customer is being targeted for fraud.

*Should a CoP request only apply when a new payment mandate is being set up or changed?*

This would appear sensible as a start point but policy must be flexible to allow CoP to react to fraudsters who will look for ways to use CoP to their advantage.

*Should any directions cover the sending of money from both individual and business accounts?*

Building societies are restricted in the types of account they can provide for non-individuals.

From the consumer's perspective, it would be better for both individual and business accounts to be covered as long as there is sufficient capacity within CoP to do so. Individual and business accounts are both targeted for APP fraud.

*Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?*

Direction should cover both sending and receiving.

# CashFlows

**3.21 Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

We are pleased that COP has been considered as a measure to help prevent Fraud and misdirected payments. CashFlows had been in an agency banking agreement with a high street bank, during our time within this relationship we have experienced a vast amount of payments which could have benefited from the COP measure. Especially as the FPS/Chaps are somewhat instant transfers it has been extremely difficult to monitor payments of this type, other than validation of bank accounts and manually checking payments which hit our internal rules.

**4.6 Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

We believe that not all PSP will have the resources in place to adopt the COP, however FPS/CHAPS are all put through a clearing bank and we believe all members within the network could mandate this their end. Technically how this would feed through to PSP such as CashFlows, we are unsure of.

It would be more practical for direct members to be mandated with the direction but for indirect members, such as CashFlows, a voluntary scheme should be in place. The reason for this is that direct members are likely to have the technological systems and resources available to implement such a change, which could have an adverse impact, in terms of cost and resource, on indirect members. As all payments implemented by an indirect member essentially through a direct members system, this would not impact on the effectiveness of CoP

**4.7 Question3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

Yes, otherwise the COP process remains incomplete.

**4.12 Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

We understand the scope for COP to be implemented for both FPS/Chaps as there are limited number of banks involved. If COP can be adopted to SWIFT/SEPA this would be extremely beneficial too. However, we can not see the scope for this, as this will involve every bank internationally.

**4.14 Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

We do not see a benefit for a COP be applied to every payment. We trust this should be applied to every payment during the set up. However, we should consider a COP when a name change has been applied such as marital name change etc.

**4.18 Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

We trust that this should be mandated to all members of the FPS/CHAPs scheme and PSP of an X amount of turnover. As we are an indirect member, and therefore smaller in size than direct members, we believe this will not be beneficial for us to adopt considering the operations/technical and capital this may involve. We believe there should be no opt out option.

**4.20 Question 7: Should any directions cover the sending of money from both individual and business accounts?**

Both yes to confirm the COP is conducting fully.

**5.4 Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

Should cover both sending and responding.

**5.7 Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

We believe that, while these deadlines may be achievable to direct members, who are larger in size and therefore have more resource to meet them, this may not be achievable for smaller, indirect members. As mentioned in previous responses, if indirect members were encouraged to volunteer, rather than be mandated, to implement CoP, then this would be a more balanced way.

**6.3 Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

Direction to be applied to the FPS participants.

**7.10 Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

The benefits and advantages have been outlined correctly.

**7.19 Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

No further comment.

**7.26 Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

No further comment.

**7.27 Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

No further comment.

**8.6 Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

No further comment.

CBI

04 January 2019

APP Scams Policy Team  
Payment Systems Regulator  
12 Endeavour Square  
E20 1JN London

Dear APP Scams Policy Team,

**CP 18/4 Consultation on general directions on implementing Confirmation of Payee**

In response to the PSR consultation CP 18/4, I am writing to outline the key aspects raised by CBI members about implementing Confirmation of Payee (CoP).

The CBI welcomes the opportunity to share these views.

**In this response, we highlight that:**

- The CBI welcomes CoP as a mechanism to help reduce APP fraud for SMEs;
- The CBI urges the need for smarter, fit-for-purpose regulation;
- Whilst the CBI understands the need to implement CoP swiftly, the PSR should adopt a more flexible timescale for implementation with smaller firms in mind.

**Financial services at the CBI**

The CBI is the UK's leading business organisation, speaking for some 190,000 businesses that together employ around a third of the private sector workforce. With offices across the UK as well as representation in Brussels, Washington, Beijing and Delhi the CBI communicates the British business voice around the world.

The CBI financial services policy work is focused on two objectives: assessing the potential impact of Brexit on the UK's financial services sector and highlighting the sector's role as an enabler for growth.

**The CBI welcomes CoP as a mechanism to help reduce APP fraud for SMEs**

The CBI welcomes this consultation and the opportunity to share the views of CBI members in more detail through regular dialogue with the PSR.

Each year, thousands of businesses are victim to APP fraud. Making CoP available to payers will help SMEs prevent misdirected payments and will offer more protection as part of their payment experience. The PSR's proposed general directions should help coordinate the industry's efforts in protecting

consumers and will ensure a swift implementation. Confirmation of Payee is a step in the right direction, but we have concerns as to its implementation plan.

### **The need for smarter regulation that puts customers first**

The UK's position as a global leader and innovator in payments is an integral element of the UK's status as a global leader in financial services. Smarter regulations that puts customers first will contribute to this success.

Regulation is critical to protecting customers of financial services, but members are clear that what is required is smarter, fit-for-purpose regulation. This is regulation that safeguards financial stability and protects consumers, without infringing on the space businesses require in order to grow and innovate. It is proportionate and targeted regulation, with the benefit of cooperative, collaborative and engaged supervision.

Customers must be able to rely on the financial products and services provided to them as well as trust firms to provide these in a secure and timely way. To meet these expectations, firms need the freedom and flexibility to develop new products and services while treating customers fairly and acting in a socially responsible manner within a regulatory framework that supports financial stability. But a key challenge is the lack of focus in policy discussions on customer needs and how these developments will impact them.

The CBI would therefore suggest the PSR considers the application and timeframe of implementation of the general directions.

### **The implementation plan**

#### *Application*

In relation to the types of payment products that should be covered by the directions, we would support the application of CoP to both FPS and CHAPS transactions.

The CBI understands that in the interests of consumers CoP requests should only apply when a new payment mandate is being set up. CoP will be helpful for first time transactions as this will prevent customers from sending payments to an account under the control of a fraudster. Once a new payment mandate has been set up, the CoP will provide greater confidence to payers that the person being paid is the right one and will avoid unnecessary costs to firms.

The application of CoP should help prevent future fraudulent transactions – in our view this means only new transactions should be in scope.

#### *The timeframe*

The consultation considers a phased implementation commencing on 1<sup>st</sup> April 2019 (for responding to CoP requests) and on 1<sup>st</sup> July (for sending CoP requests). In our view, Payment Service Providers (PSPs) will struggle with the deadlines and will not allow enough time to educate consumers.

Even though early implementation would be preferable to prevent fraudulent transactions, the CBI have some concerns as to the readiness of business users to adapt to the new processes. The CBI understands

that these timescales will be onerous for some PSPs as they will need time to build in the right processes. This is particularly relevant for those businesses working with third party providers.

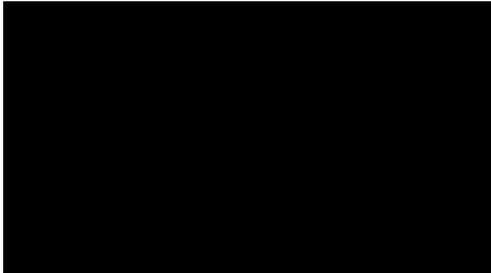
This timeframe will also need to provide enough time for customer education. With the proposed deadlines there is a risk in that customers may not have enough time to understand how CoP works. This could be an impediment for meeting the overall objective of protecting users.

The CBI would therefore recommend a more realistic deadline to enable smaller companies implement CoP efficiently. A company's capability to respond and to send CoP requests needs to be successfully tested before implementation and needs to allow enough time to educate customers. This, in our view, would prevent any unintended consequences (i.e., a payment failure resulting from an error in a payee name).

### Closing comments

The UK needs a financial system based on protecting consumers and fostering innovation through smarter, fit-for-purpose regulation. The Confirmation of Payee proposals are a good step in this direction as they will help consumers be better protected from scams. The CBI supports the general directions given by the PSR and we believe that these measures, if implemented in a timely and balanced way, will benefit consumers and financial services providers.

Yours sincerely,



# Clydesdale Bank PLC



Our Ref MC/DB/PD  
Your Ref  
Date 4th January 2019

Clydesdale Bank PLC  
57 Queen Street  
Glasgow  
G1 3ER

Tel 0141 2423757

## **Consultation on general directions on implementing Confirmation of Payee**

Dear Sir

### **Consultation on general directions on implementing Confirmation of Payee**

We thank you for inviting us to respond to the Consultation on general directions on implementing Confirmation of Payee (CoP). Clydesdale Bank notes that this consultation document has been prepared to seek views on whether to give general directions to payment service providers (PSPs) on the implementation of CoP. Clydesdale is responding as a participant in the FPS, Bacs and CHAPS payment schemes and separately from Virgin Money.

As a full-service bank with a retail-focused customer base, and as a direct participant in the above-mentioned UK payment schemes, Clydesdale are supportive of the introduction of CoP across the banking sector. We recognise that CoP, if implemented properly, will provide an important additional tool that will reduce the harm associated with APP scams and misdirected payments. CoP will be effective alongside other measures such as the contingent reimbursement model and increased customer awareness and education; it should be noted that CoP in itself will not prevent all APP scams.

Clydesdale would encourage the PSR to consider some of the underlying issues associated with CoP and would encourage further industry engagement prior to deciding on any general direction. Specifically, we understand that there are potential issues around Head Office Collection accounts, businesses that use trading names different to their actual account name and the difficulties of utilising 'fuzzy logic' until or unless there is an agreed standardised approach. Unless addressed, any or all of these issues could reduce consumer confidence in electronic payments, the reverse of what CoP is aiming to achieve.

The key area of concern is around the suggested timescales for implementation. The proposed dates in early 2019 would conflict with changes around PSD2, Strong Customer Authentication and the challenges presented by Brexit meaning that customers would potentially be bombarded with changes and updated information on several different fronts all within a compressed time period.

These same changes will also be extremely challenging for smaller PSPs who have committed significant resource to achieving the above changes and, in many cases, would require many of the same resources to also work on implementing CoP. From a project perspective therefore, there is additional risk in managing these different projects in parallel. An implementation date of 2020 for example would remove some of this overlap and in addition

would allow time for better industry coordination, development of potential solutions by vendors and allow for improved customer education and awareness.

In respect of scope, Clydesdale would suggest that the PSR considers whether it would be more effective to prioritise certain customer payment channels, particularly online / mobile, and allow these channels to be used to test and embed the CoP process before rolling out to other channels such as telephony or in branch transactions. Successfully implementing on one or two channels first would build awareness and confidence before rolling out to a wider audience with potentially more complex channels and communication needs.

Clydesdale agrees that both CHAPS and Faster Payments should be in scope for CoP, as both methods are currently utilised to effect APP scams. The PSR may wish to further consider whether Bacs payments should also be in scope.

We look forward to continuing to work with the PSR, and as the results of this consultation are assessed we would welcome further discussion on our opinions offered above.



# Dudley Building Society

## Confirmation of Payee Proposal - Gap Analysis

Ref	Requirement	Observations / Notes
<b>Payment Systems Regulator</b>		
<b>Consultation Paper - November 2018</b>		
<b>Executive Summary</b>	We are considering regulatory intervention to ensure that PSPs implement CoP in a timely and coordinated way. We believe there may be weak incentives for a PSP to be an early adopter of CoP, as its benefit depends on widespread take-up by other PSPs. In our view, for CoP to be effective and achieve the potential benefits for PSPs and their customers, it needs to be implemented quickly and be widely available to payers. <b>People making electronic payments should be familiar with seeing CoP as part of their payment experience, and be afforded the protections it offers.</b>	
1.10		
<b>Issues We Want to Address</b>	The outcome we want to achieve is to reduce significantly losses from APP scams so that individuals and businesses do not face such financial loss nor the other non-financial consequences of such scams. We also want to reduce significantly the number of accidentally misdirected payments and any consequential harm and financial loss.	How will this align to the APP CRM proposal; not all firms can participate and are potentially at an increased risk of suffering loss
2.5		
<b>Issues We Want to Address</b>	CoP was one of those initiatives. In brief, CoP is a process for checking that the name of the account holder being sent money matches the name the sender is expecting.	There are some limitations e.g. this proposal won't help with ACTO fraud; the party making the payment will be expecting the account to be in the fraudster's name and therefore will see a positive CoP result.
2.7		
<b>Why Are We Consulting</b>	The section of the draft code dealing with the reimbursement of customers following an APP scam says that a firm may choose not to reimburse a customer where:  "The customer did not take appropriate actions following a clear negative Confirmation of Payee result, where the firm complied with SF1(3) or SF2(2), and those actions would, in the circumstances, have been effective in preventing the APP fraud"	We cannot comply with this and therefore cannot exercise this right. Surely customers won't be able to claim reimbursement if we are unable to offer CoP?
3.10		
<b>Why Are We Consulting</b>	.....further; fraudsters may well try and use accounts at a PSP that does not provide a response to a CoP request to carry out their scams	
3.13		
<b>Why Are We Consulting</b>	We are however considering, if there are obstacles to CoP's timely introduction and whether it is appropriate to give directions to PSP's, using FSBRA (Financial Services Banking Refers Act) to mandate the introduction timescales.	Agency banking users cannot comply and therefore must be descoped from any regulatory directions otherwise we will find ourselves in a position of regulatory breach from Day 1
3.16		
<b>Opting out of CoP</b>	Need to consider whether it would be legitimate for a person to opt out of CoP. How should any directions deal with the potential for people to opt out of the CoP process?	There should be clear liability on the customer's part if they have opted out; they should not then be eligible to claim under the CRM
4.18		
4.2	Should any directions cover the sending of money from both individual and business accounts?	Yes - to offer increased protection against invoice and internal frauds
<b>Costs</b>	.... customers will need to use CoP under the proposed directions and should learn to use it. Therefore, for CoP, we expect that the consumer awareness campaign and support costs should be incurred in the lead up to, and during the early stages of, implementation.	Is there any expectation for warning / notification messages to be standardised across the industry? If the reliance is being placed on customers to "learn to use it" and all the messages they see are different between different firms; how fair is that?
7.17		

# Electronic Money Association (EMA)



**Electronic Money Association**

Crescent House  
5 The Crescent  
Surbiton  
Surrey  
KT6 4BN

United Kingdom

Telephone: +44 (0) 20 8399 2066

Facsimile: +44 (0) 870 762 5063

[www.e-ma.org](http://www.e-ma.org)

Confirmation of Payee Consultation  
Payment Systems Regulator  
12 Endeavour Square  
London E20 1JN

Email to: [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)

8 January 2019

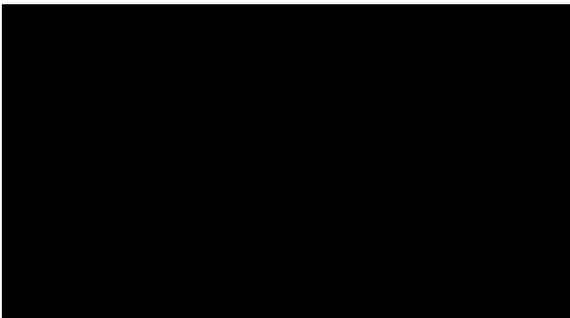
Dear Hannah

**Re: EMA response to PSR Consultation on general directions on implementing Confirmation of Payee**

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a large number of smaller Payment Service Providers, including startups. The majority of EMA members are authorized in the UK, and operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

We would like to highlight the difficulty with responding to this consultation without full access to the details of how the Confirmation of Payee (CoP) service will operate. We cannot adequately assess the impact and consequences of the proposed PSR directions on the PSP community without access to technical specifications. Our responses are therefore based on assumptions about how the service may operate and not a full analysis of the impact on our Members.

I would be grateful for your consideration of our concerns.



## **EMA response to consultation**

### **General comments**

We would like to highlight the difficulty of responding to this consultation without full access to the details of how the Confirmation of Payee (CoP) service will operate. Specifications, documentation, and guidance on the CoP service are only available to PSPs under NDA with Pay.UK. Without access to the operational details of CoP it is impossible to adequately assess the impact and consequences of the proposed PSR directions on the PSP community.

Separately, some of our members have raised significant concerns in relation to the NDA that PSPs are required to sign in order to obtain the technical specifications for the CoP service.

Specifically, these concerns are:

- Disclosure of the specification and rules documents are limited to entities and individuals in the EEA. This is problematic for EMA members that operate on a global scale, and may have IT operations based outside the EEA, who will be building the service. This will also be problematic for all PSPs based in the UK in the event of a “hard Brexit”, as UK staff will no longer be in the EEA.
- The IP protection clause in the NDA is very broad and goes beyond ensuring that Pay.UK remains the owner of any specs produced. It prevents Fintech PSPs that may be working on something similar product enhancements already from signing the NDA, due to the risk that the disclosing party later claims ownership of IP in the PSP’s end product by arguing that the information they provided was used by the PSP in their product.

As a result, many of our Members have, as yet, not been able to assess the full details of the CoP service and our responses are based on assumptions about how the service may operate.

### **Consultation Questions**

**Q1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

We understand and welcome the PSR’s aims to address the negative consequences resulting from misdirected payments, whether malicious or not. However, we note that the PSR’s projected benefits of implementing the Confirmation of Payee (CoP) service has not been based on quantified evidence demonstrating the effect of Confirmation of Payee on losses due to APP scams.

In addition, the consultation does not indicate that the payments industry should conduct technical trialing of CoP as a service to generate such evidential data.

We recommend that the PSR base any decision to give directions under section 54 of FSBRA to **all PSPs** on proven evidence that CoP is effective in reducing APP frauds. Following the experience of the Netherlands, PSPs could be required to operate CoP in the background for several months before displaying any CoP information to the end customer. During this time PSPs could monitor and report on the performance of their and other PSPs' algorithms in order to assess the effectiveness of different implementations of CoP in reducing losses due to malicious misdirected payments. At the same time, this trial period would minimise the impact on customer experience and allow any issues to be addressed before payments are affected, thus ensuring the service will run as expected when rolled out, and offering the opportunity to iron out any unintended consequences and educate and inform consumers.

We also note that the success of CoP will depend heavily on the name-matching algorithm that each PSP employs and hence the quality of response that can be provided by payee PSPs. Neither of these appear to have been standardized, although we understand that the specifications provide some level of direction in this area, so there will likely be a high percentage of inconsistencies and false negative responses. For example, more unusual names, or names from cultures where several different names can be used interchangeably, or with different spelling are likely to come back with a 'no match' result, even if the details are correct.

**Q2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

We support as wide adoption of CoP as possible, and that adoption should be coordinated between all relevant PSPs. However, as mentioned under Question 1, there appears to be little quantified evidence that CoP will have the intended effect on APP fraud reduction. We therefore propose that the PSR require PSPs to run CoP in the background for a number of months before displaying any information to the customer to manage any unintended consequences or technical issues.

The position of **indirect participants** of the Faster Payments scheme in terms of connection to CoP remains unclear, so we propose this is clarified before CoP is rolled out to participants. Initially Indirect PSPs are likely be dependent on a software vendor for providing a solution to participate in the CoP service. Pay.UK report that several vendors are developing CoP solutions but the level of maturity of their solutions is not confirmed, and none have so far built a solution for receiving CoP requests. We propose therefore that the PSR deadlines are applied once a sufficient number of vendors have developed products that are available at a reasonable price that is affordable for smaller PSPs.

In terms of which accounts should be in scope, on the payee side we support all accounts (consumer and business) falling within scope. However, the percentage of negative name matches is likely to be much higher for business accounts than for consumer accounts. We therefore propose that before applying CoP, PSPs should be required to capture nicknames, trading names, and other alternative names for their business customer accounts so that name-matching algorithms can also accommodate the types of variations seen in business account names without impacting on the effectiveness of the CoP service.

On the payer side, the CoP service may impact on the payment service user's experience, and slow down the payment process. We therefore propose that the payer's PSPs may exercise discretion on whether to opt customers out of the service. For example, an acquirer transferring funds to a merchant's bank account using bank details provided by the merchant at an earlier date. In this case, the PSP may assess that the risk that this payment would be maliciously misdirected as low and should have the discretion to not apply CoP. The sending PSP in this scenario would therefore take on the risk that the payment was fraudulent.

Please note that smaller PSPs, in particular non-banks, may not have a distinction between business and consumer accounts, and may wish to apply CoP to the full customer database. They should not be prevented from doing so if they wish.

We welcome the exclusion of **Head Office Collection Accounts (“HOCA”)** at this stage, and the consultation states that this exclusion is designed mainly to account for Building Society accounts. E-money institutions (EMIs) often operate accounts in a similar way (i.e. that the sort code and account number are associated with the e-money institution rather than the individual customer) and we understand from Pay.UK that the intention is that EMI's operational bank accounts structured in this way would also fall under the HOCA definition. However, we would welcome confirmation from the PSR on this issue, as EMIs and their customers are likely to suffer a high level of confusion if this issue is not clarified. EMIs may also need to change the payment instructions given to their customers, as well as obtain comfort that payments into their customers' accounts won't be delayed or disrupted as a result of being excluded from CoP.

In terms of **geographical scope**, we note that transactions where “one or more of the parties is outside the UK” are out of scope. This is clarified as “where either the sender or the payee is outside of the UK”. We would welcome further guidance as to whether this geographical limitation applies to the jurisdiction of the contractual relationship between PSP and customer, or to another geographical indicator (such as physical location of customer, physical location of PSP etc.). We believe it would be simpler to limit the Direction for CoP to FPS/CHAPs payments only, regardless of geography. Some PSPs may apply CoP to all customers, in which case customers from non-UK jurisdictions are likely to be confused by the response received.

The consultation contains a broad definition of PSP and we would welcome clarification on whether the PSR intended to include PISPs in the scope of the proposed Directions.

We would recommend that CoP as a service should be optional for **PISPs** to offer their customers and as a result PISPs should not be within the scope of any proposed PSR directions. Without access to the technical specifications for CoP it is unclear if PISPs could offer CoP directly to their customers or via the ASPSP from which payments are initiated. The focus should be on ensuring the customer experience is a positive one for customers using PIS. The need for a PISP to offer CoP depends on the interaction between ASPSP and PISP. As the PISP does not hold customer funds, but merely provides the setting up and initiation of a payment, there may be many circumstances where a requirement to offer CoP may confuse the customer.

**Q3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

We support the PSR's approach to require implementation of CoP first on the receiving side and later on the sending side.

**Q4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

We support the proposed approach to apply CoP to FPS and CHAPS transactions only.

**Q5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

A CoP request should only apply when a new payment mandate is being set up or changed, and only to new payees set up after CoP has been implemented. There is limited value in applying CoP to any payments where the payee is not new as a payee's personal details are unlikely to change very often. On a risk weighted basis, PSPs may opt to offer CoP for existing payees to customers when the CoP service is first implemented but this should not form part of the PSR's directions. It would also be disproportionate to require CoP to be applied to all payments made to existing payees once the service is introduced.

**Q6: How should any directions deal with the potential for people to opt out of the CoP process?**

The PSR does not set out in which circumstances an individual or a business may wish to opt out, and in the absence of data indicating the effectiveness of CoP as a service, the EMA cannot make

any recommendations on the necessity or benefit of opting out of CoP. We do recognise that the creation of any mechanism for opting out will create a fraud vector and this should be considered in the PSR's analysis.

We do however believe there may be legitimate reasons for a payer (as opposed to payee) to wish to opt out of CoP. For example, a business sending high volumes of individual payments (non-batch) on a regular basis, particularly where these are time-sensitive, may wish to opt-out of applying CoP to every transaction based on its own risk analysis.

As discussed in our response to Q2, sending (payer) should be able to exercise discretion on whether to opt customers out of the service. The PSPs would then take on the risk of a misdirected payment, whether maliciously misdirected or not.

**Q7: Should any directions cover the sending of money from both individual and business accounts?**

As set out in our response to Q2, the CoP service may impact on the payment service user's experience, and slow down the payment process. We therefore suggest that any directions on the sending of payments should give sufficient flexibility to allow the payer's PSPs to exercise discretion on whether to apply the CoP service from either individual and business accounts.

If the paying PSP operates business accounts and assesses the risk of misdirected payments from those accounts to be low, then that PSP could opt not to apply CoP to transactions from those accounts. Equally, PSPs should not be prevented by the Directions from applying CoP to business accounts should they require.

**Q8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

As mentioned above, it is difficult to respond to this consultation without full access to the details of how the Confirmation of Payee (CoP) service will operate. As a result, our response is based on assumptions about how the service may operate.

Yes we agree that the directions should separate out responding to CoP requests from being able to send them.

In relation to the Directions covering the sending of CoP requests, as set out in Q8 above, the CoP service may impact on the payment service user's experience, and slow down the payment process. We therefore suggest that any directions on the sending of payments should give sufficient flexibility to allow the payer's PSPs to exercise discretion on whether to apply the CoP service from either individual and business accounts.

If the paying PSP operates business accounts and assesses the risk of misdirected payments from those accounts to be low, then that PSP could opt not to apply CoP to transactions from those accounts. Equally, PSPs should not be prevented by the Directions from applying CoP to business accounts should they require.

**Q9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

We do not agree with the deadlines for the introduction of CoP.

Indirect PSPs are likely be dependent on a software vendor for providing a solution to participate in the CoP service. Pay.UK report that several vendors are developing CoP solutions but the level of maturity of their solutions is not confirmed, and none have so far built a solution for receiving CoP requests. We propose therefore that the PSR deadlines are applied once a sufficient number of vendors have developed products that are available at a reasonable price that is affordable for smaller PSPs.

Although the technical specifications are available, the NDA required in order to obtain them is very restrictive and difficult for global firms to sign, as it limits the sharing of information with non-EEA staff and the IP provisions are restrictive. A number of firms are still in discussion with Pay.UK regarding these and other elements of the NDA, and unless these issues are resolved in time for firms to be able to review the specifications in order to implement them, it will be impossible to meet the April and July deadlines.

[Members to indicate what alternative timescales are feasible]

**Q10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

We recommend the PSR consider requiring PSPs to run CoP in the background for several months before displaying any information to the end customer. During this time PSPs could monitor and report on the performance of their and other PSPs' algorithms in order to assess the effectiveness of different implementations of CoP in reducing losses due to malicious misdirected payments. At the same time, this trial period would minimise the impact on customer experience and allow any issues to be addressed before payments are affected, thus ensuring the service will run as expected when rolled out, and offering the opportunity to iron out any unintended consequences and educate and inform consumers.

**Q11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

We believe that CoP will benefit the UK payments industry, UK customers, PSPs, and reduce fraud. However it is unclear where the figure of an estimated 20% reduction in malicious APP scams has been obtained. In fact, the implementation of CoP as a service may lead to a number of unintended consequences, which we have set out under Q12, thus reducing the benefit of the service set out in the PSR's consultation.

We also note that whilst CoP may reduce some types of APP fraud, it will have no impact on many other types of APP fraud, for example investment scams (which are second to highest in terms of value) and advance fee scams. For other types of scams, the effectiveness of CoP and thus any benefits to consumers will depend on the scope of implementation and the algorithms that are developed by PSPs to send a response to the sending PSP.

We believe the estimated reduction in APP scams of 20% is too high, and would welcome evidence to support this figure.

**Q12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

Whilst the PSR has identified the technical build costs of CoP, and estimated the on-going costs, it is not clear which operational costs are included in the anticipated annual running costs. There is also no indication of estimated loss of PSP revenue when customers abandon a transaction due to the CoP response (for non-fraudulent transactions). As a result, we consider that the estimated costs are too low.

The cost of helping customers to resolve issues with using the CoP service will not be insignificant. For instance, customer service contact rates will increase as customers try to understand negative or 'maybe' CoP responses whilst making a payment. It is not clear whether these costs have been included within the estimated annual costs to the industry of the CoP service and we would welcome more details on how the annual costs were calculated. EMIs whose accounts fall within the definition of a Head Office Collection Account may need to change the instructions they provide to their customers for the funding of their e-money accounts. Depending on the messaging instructions set out in the CoP specifications, they may also be required to address a high level of customer confusion, or worse, a loss of business.

Another significant cost that it is not clear has been taken into consideration is the cost over time of the increase in volume of API calls. As the number of PSPs participating in the service increase over time, volumes of API calls will increase, and PSPs will need more hardware to respond to such calls, as well as engineering to optimize the searches. The number of new (direct and indirect)

participants in FPS has doubled in the last 18 months. It is reasonable to consider that this growth rate will continue and each new member in the future will introduce a new set of CoP API calls for participating PSPs

The cost to PSPs may be higher for their vulnerable customers who are accustomed to the payment process with which they are familiar, and may need a higher degree of customer education and information to transition to the CoP customer experience. Participant PSPs will need to account for this cost when analysing the total cost to them of implementing CoP.

**Q13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

As mentioned above, the PSR may have overstated the benefits of CoP in terms of the impact on APP scams, and failed to account for the costs associated with the likely high number of false negative responses.

**Q14: What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

If PSPs are unable to obtain the technical specifications in good time due to issues with the NDA required by Pay.UK, there might be additional cost as they may have to outsource some services. Pay.UK report that several vendors are developing CoP solutions but the level of maturity of their solutions is not confirmed, and none have so far built a solution for receiving CoP requests. We propose therefore that the PSR deadlines are applied once a sufficient number of vendors have developed products that are available at a reasonable price that is affordable for smaller PSPs.

**Q15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

The cost to PSPs may be higher for their vulnerable customers who are accustomed to the payment process with which they are familiar, and may need a higher degree of customer education and information to transition to the CoP customer experience. Participant PSPs will need to account for this cost when analysing the total cost to them of implementing CoP.

**List of EMA members as of January 2019:**

[Airbnb Inc](#)  
[Allegro Group](#)  
[American Express](#)  
[Azimo Limited](#)  
[Bitstamp](#)  
[BlaBla Connect UK Ltd](#)  
[Blackhawk Network Ltd](#)  
[Boku Inc](#)  
[CashFlows](#)  
[Circle](#)  
[Citadel Commerce UK Ltd](#)  
[Coinbase](#)  
[Corner Banca SA](#)  
[Curve](#)  
[eBay Sarl](#)  
[ePayments Systems Limited](#)  
[Euronet Worldwide Inc](#)  
[Facebook Payments International Ltd](#)  
[First Rate Exchange Services](#)  
[Flex-e-card](#)  
[Flywire](#)  
[GoCardless Ltd](#)  
[Google Payment Ltd](#)  
[IDT Financial Services Limited](#)  
[Imagor SA](#)  
[Intuit Inc.](#)  
[Ixaris Systems Ltd](#)  
[Merpay Ltd.](#)  
[MuchBetter](#)  
[myPOS Europe Limited](#)  
[Nvayo Limited](#)  
[One Money Mail Ltd](#)  
[Optal](#)  
[Ozan](#)  
[Park Card Services Limited](#)  
[Paybase Limited](#)  
[Paydoo Payments UAB](#)  
[Payoneer](#)  
[PayPal Europe Ltd](#)  
[PayPoint Plc](#)  
[Paysafe Group](#)  
[PPRO Financial Ltd](#)  
[PrePay Solutions](#)  
[QIX Ltd](#)  
[R. Raphael & Sons plc](#)  
[Remitly](#)  
[SafeCharge UK Limited](#)  
[Securiclick Limited](#)  
[Skrill Limited](#)  
[Starpay Global Ltd.](#)  
[Stripe](#)  
[Syspay Ltd](#)  
[Transact Payments Limited](#)  
[Transact24 \(UK\) Ltd](#)  
[TransferMate Global Payments](#)  
[TransferWise Ltd](#)  
[TrueLayer Limited](#)  
[Trustly Group AB](#)  
[Uber BV](#)  
[Valitor](#)  
[Vitesse PSP Ltd](#)  
[Viva Payments SA](#)  
[Wave Crest Holdings Ltd](#)  
[Wirecard AG](#)  
[Wirex Limited](#)  
[Worldpay UK Limited](#)  
[XCH4NGE LTD](#)

# Emerging Payments Association (EPA)

## Response for PSR – Consultation on general directions on Confirmation of Payee

### The Emerging Payment Association's response

**Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

We are, broadly, supportive of the CoP initiative, which we consider will be an important contribution to minimising payments misdirected in error as well as certain types of push payment fraud. The EPA is supportive of efforts to reduce maliciously directed scams and wider financial crime.

We do not disagree with the PSR's approach to ensuring that CoP will be fully implemented in the UK in a timely manner by giving directions under section 54 of FSBRA. For the CoP to be successful there has to be universal adoption. If uptake is partial, the effectiveness of and confidence in CoP will be undermined.

However, we are disappointed with the PSR's choice of timing in two respects. Firstly, this consultation has been issued with a very short response period over the Christmas holidays. Secondly, the implementation period is incredibly short given the significant regulatory obligations imposed by the RTS on open access and strong customer authentication due next year and the uncertainty of Brexit.

From our discussion with payment service providers, we believe there is limited awareness of the details of the voluntary code and the technical specification of the CoP scheme. A more realistic lead-in time is necessary to allow payment service providers to meet the envisaged obligations.

We also believe that there is insufficient time allowed for all relevant parties to undertake sufficient testing across all PSPs using the service. There is a risk that, without sufficient time to test, the infrastructure built may be ineffective and expose weaknesses – thereby creating a financial and criminal risk.

We would encourage the adoption of an industry standard for 'Close Match' situations. Whilst high level minimum guidelines have been provided for these participants, the capability is relative to the data sources available to the Payee (or recipient of the CoP request) PSP.

Further to this, UX and liability needs to be defined and agreed for situations in which when the Payee PSP's matching service is down due to technical or operational failure.

We would recommend that the PSR review its proposed timescales in light of the aforementioned reasons, and to identify a roadmap that is mindful of existing requirements (such as the implementation of Open Banking) and once the above elements have been clarified and/or confirmed. We strongly encourage the PSR to work collaboratively with all PSPs within the scope of confirmation and Pay.UK to maximise awareness of CoP and its ensuing activity, and to undertake sufficient testing within a workable timeframe. We would also encourage the PSR to work with industry and relevant associations to drive consumer education and awareness of CoP, and on how to use CoP most effectively as a Payer.

**Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

PSPs that receive and send FPS and CHAPS payments, on behalf of their customers, could be given directions by the PSR and thereby ensure that both direct and indirect participants are covered.

The PSR may seek to give direction to PSPs relative to the volume of transactions enabled by a PSP or relative to the average transaction value

**Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

Full coverage on the recipient side is important to maintain confidence in and the effectiveness of the system. We agree that coverage on the receive side should include all payment accounts (consumer, business and corporate) as well as all types and sizes of payment service provider to ensure effectiveness and prevent migration of fraud.

We believe that payment service providers should be allowed to choose whether there should be coverage on the send side. Payment service providers can make their own decision on whether to implement based on the risk of fraud in the particular circumstances. The pressure from the contingent reimbursement model to implement CoP will lead to correct outcomes without artificially imposing this on payment channels with low or no risk.

**Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

We believe directions should be payment system-neutral so that payment service providers that enable authorised push payments in Sterling and within the UK must take responsibility to assess the risk of fraud and misdirected payments and take appropriate and proportionate action. As noted above, the contingent reimbursement model incentivises appropriate behaviour.

**Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

We recommend that the PSR does not provide directions on this but allows payment service providers to take appropriate action according to their own assessment of the risk.

**Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

We do not believe this should be a matter for the PSR's directions but, instead, for the individual payment service providers.

**Question 7: Should any directions cover the sending of money from both individual and business accounts?**

As above, we believe the directions should only be in relation to the recipient side. However, we recommend that the CoP on the recipient side is extended to confirming or otherwise whether the account type is as the payer expected (i.e. if it is a business or personal account) as this additional information will help payers identify any irregularity with the payee account.

Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?

As above, we believe the directions should only be in relation to the recipient side.

Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.

As noted above, we are concerned that there is a real risk to the payment systems if CoP were to be implemented too quickly without proper consideration. Noting there are no central infrastructure reference test systems available, the experience of the complexity of rolling out Open Banking, and that the premature integration of CoP on the sending side without adequate testing could adversely impact the core payment systems if match/error rates were unacceptable.

A similar scheme implemented in the Netherlands took at least a year to bring match/error rates into acceptable order and to be fully integrated in the payments system. On this basis we recommend that the receive side date should be no earlier than six months after the publication of the completed technical specification – which we understand has not been finalised.

It should be up to the discretion of the payment service providers to implement the send side but, to ensure momentum and incentivisation of implementation, we recommend that the contingent reimbursement scheme should come into effect a year after the deadline for the receive side.

### About the Emerging Payments Association

The Emerging Payments Association (EPA) is a thriving community of payments professionals to strengthen and expand the payments industry to the benefit of all stakeholders.

Since 2004 the EPA has been instrumental in helping to connect the ecosystem, encourage innovation and promote competition in this market.

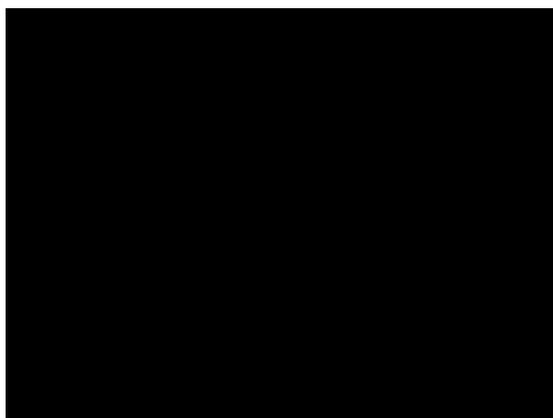
We achieve this by delivering a comprehensive programme of activities for over 130-member companies, with the help of our independent Advisory Board, which address issues affecting the payments industry and its users.

This include events, conferences, award ceremonies, research, projects and lobbying activities

Experian



**Experian's response to  
Consultation CP18/4 on  
General directions for the implementation of Confirmation of Payee (CoP)**  
Response sent to Payment Systems Regulator  
on 24 December 2018



## Introduction

Experian is pleased to offer its comments to the questions posed in the Consultation on general directions for the implementation of Confirmation of Payee (CoP).

We continue to understand how the payments landscape is changing, as well as contributing to help ensure the future is efficient and sustainable and we are exploring how we can help PSPs meet the PSR regulatory requirements as a vendor for overlay service.

## Background on Experian

Experian is a credit reference and data analytics business, providing services direct to consumers and to businesses across a number of sectors. We provide credit data services to lenders and operate in the price comparison website market.

Experian's data and analytics help people, businesses and organisations protect, manage and make the most of their data, creating better business and consumer outcomes and building stronger customer relationships.

Experian helps people, businesses and organisations to:

- **Lend and borrow responsibly:** by gathering information on past and present credit commitments, such as loans, mortgages and credit cards, Experian helps lenders to understand whether people and businesses can manage their debt repayments, so they can borrow and lend responsibly.
- **Treat people and businesses fairly:** because Experian helps organisations make decisions based on facts, they can treat people and businesses fairly and consistently, which in turn helps people to access credit.
- **Consumer empowerment:** because Experian provides consumers with access to their financial data, we can empower them to use it to make financial decisions through our personal credit information and comparison services.
- **Make better, more efficient decisions to create better business outcomes:** by gathering and analysing information supplied by people and businesses, organisations can make quicker decisions, now taking seconds and minutes instead of days. Organisations need to make fewer manual checks which means less administration and fewer bad debts. This means the cost of extending credit is lower.

## Response to Consultation Questions

**Question 1:** *Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?*

With current APP scams, we believe this is an appropriate first step to start eliminating APP fraud. However, fraud is an evolving situation, and often there is no silver bullet, so we feel it is important that Pay.UK and the financial systems continue to evolve in their approach to fighting this fraud, to not only include the proposed solution, but also allow the implementation of other value-added tools from consortium databases, analytics, and other hybrid solutions.

**Question 2:** *Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?*

No, the overall success and benefit of CoP will be dependent on all PSPs contributing to the infrastructure. If certain PSPs are considered non-inclusive then the efficiency and confidence of the service will be impacted.

**Question 3:** *Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?*

If PSPs are not required to send requests, they should all be required to respond. For the overall success and benefit it should be inclusive of all, with everyone following the same set of regulations.

**Question 4:** *Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?*

We agree with the approach to give directions against FPS and CHAPS transactions. It's not clear whether Bacs direct credit and debit payments are included in the initial phase of CoP? Our view is that these should be included.

**Question 5:** *Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?*

Yes, we agree, directions should apply to all payment channels.

In terms of a CoP request only being applicable to new or changed payment mandates, we can understand the logic and this is likely to be a good first implementation. After that initial implementation is complete and deemed a success, there may be other considerations, for example:

- Payment amount: If the payment amount exceeds a given threshold a CoP request is mandated?
- The payment channel the mandate is being derived from: Will payment fraud via certain channels change over time?
- Annual CoP check: Whether all payment mandates old or new, need to be checked at least annually?

In the first phase of implementation, we suggest that CoP should occur when the mandate is being set up and/or changed for any reason. After an agreed implementation period (18-24 months) with financial institutions and consumers alike, we believe it should be extended to all transactions, as fraud will evolve to take advantage of the limited mandate from the beginning. By having this phased approach, the industry can eliminate the initial causes of APP frauds with minimal disruption to the consumer experience, but then provide comprehensive coverage once the technology becomes standard.

**Question 6:** *How should any directions deal with the potential for people to opt out of the CoP process?*

The ability to opt out would appear to be the anti-thesis of CoP - individuals who opt out of the system would more than likely be at the highest exposure to fraud.

If the consumer mindset was to opt out and this became a frequent request, it could impact the efficiency and success of CoP. The value is being able to complete a CoP request as close to 100% of cases. If that percentage drops to low, then PSPs and consumers will lose confidence.

Clearly consumers need to be given the option to opt out, however it should come with clear guidance and risk articulated to the consumer. The benefits of not opting out should be used.

**Question 7:** *Should any directions cover the sending of money from both individual and business accounts?*

We believe CoP should cover both individual and business accounts. By leaving businesses out of the scheme, this will be an obvious first route for APP scams to move to and shift fraud in the commercial sector, which may cause significantly higher losses to a critical part of the UK economy. CoP should be in place to protect all parties within a transaction.

Also, businesses have been shown to be prone to scams where a fraudster informs the accounts department that the payee's bank account details have changed and often large sums of money are lost.

**Question 8:** *Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?*

Yes, we agree they should be separated out to ensure a smooth transition and cover both sending and responding.

**Question 9:** *Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.*

We agree that a definitive timeline for rollout and adoption of CoP by PSP is put in place by Pay.UK, however, the current timelines of April and July 2019 feel optimistic if you consider the work required to be ready for those dates.

PSPs and/or TPSP will need to develop, test and implement the required technology within an extremely tight timeline if these dates are fixed post consultation. Given the overall importance of this service and potential consumer detriment, it is imperative that enough time is provided to the market to ensure phase 1 and the adoption is successful.

We would therefore recommend a small change and extension to the timelines:

1<sup>st</sup> April 2019 – PSPs are mandated to have a plan in place to meet CoP guidelines. This could be buy, build or partner. However, they must be able to demonstrate they have considered the options available to them and have a firm plan and project in place to meet requirements.

1<sup>st</sup> July 2019 – PSPs are mandated as addressable and capable to respond to CoP requests.

1<sup>st</sup> September – PSPs are mandated to respond and send CoP requests.

With this approach we believe the industry does not lose any momentum in addressing the APP scam issue, enabling the correct and successful adoption of CoP in a timely manner. The revised April deadline will ensure the PSPs are taking the appropriate action to remediate and will also enable the PSR to demonstrate the industry is taking CoP seriously, with the correct consideration.

**Question 10:** *Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?*

We believe the directions set out by Pay.UK are reasonable and appropriate.

**Question 11:** *Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.*

Yes, we agree the assessment methodology is the right one.

**Question 12:** *Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.*

From a cost of running perspective, we do not have a full view of what will be required for various financial institutions to run these systems and so we are unable to answer this question.

**Question 13:** *Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have*

Yes.

**Question 14:** *What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the*

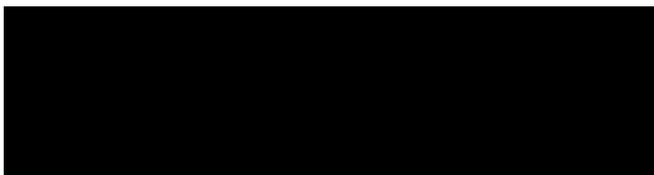
*costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?*

We believe that a delay in the implementation of CoP will ultimately lead to a worsening of the problem over time. Further, by pushing dates, which have been communicated openly, right before the deadlines, will likely imperil the entire program by throwing doubt into the overall program. Thus, we feel the dates should remain, but regulatory enforcement levels be structured to have lighter punishments for non-compliance at the initial dates and a sliding scale of enforcement actions within 3 months of initial date required.

Discussions we have had with PSPs to date have suggested the current timelines are not achievable and as a result they are now waiting for further guidance from the consultation before making any decision on how to meet the requirements. We believe that by updating the timelines as described in the answer to question 9, would result in quicker compliance and increasing the benefit over the timescales under consideration.

**Question 15:** *Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?*

We believe that APP type scams have a higher impact on the most vulnerable of consumers who often lack the sophistication to spot APP type scams. By implementing CoP, Pay.UK will have a positive impact on the UK citizenry by providing protections for the UK's most vulnerable individuals.



# HSBC Bank PLC

**HSBC BANK PLC**

**CONSULTATION ON GENERAL DIRECTIONS ON IMPLEMENTING CONFIRMATION OF PAYEE**

---

---

**RESPONSE TO CONSULTATION NOVEMBER 2018**

**04 JANUARY 2019**

---

---

## COVER SUBMISSION

Following the establishment of the HSBC Group retail bank HSBC UK Bank plc on 1 July 2018, HSBC Bank plc (HSBC) is the UK's non-ring-fenced bank within the HSBC Group. HSBC Bank plc's customers in the UK include our Global Banking and Markets clients within our wholesale and investment banking division, relevant Financial Institutions, large UK Corporate Banking customers and customers of non-UK branches of HSBC Bank plc. This includes those customers for whom we provide Indirect Access to one or more of the UK's main payment systems via our own Direct Access to these systems under a contractual arrangement.

HSBC welcome the opportunity to respond to the Payment Systems Regulator's consultation on general directions on implementing Confirmation of Payee.

The scope of Confirmation of Payee (CoP) relates primarily applies to personal customers, small businesses and charities. These customers are managed by HSBC UK Bank plc (HBUK) and accordingly HSBC UK have submitted a full response to the consultation. HSBC is fully supportive of the HSBC UK consultation response and echo the concerns in relation to our corporate and government customers with accounts in the UK.

We particularly encourage the PSR to consider a direction tailored to focus on the customer groups that are most at risk of harm from Authorised Push Payment Scams and Misdirected Payments, namely personal and small business customers making single transaction payments. Large corporate and government customers making batch file payments are at a lower risk, and at this stage, the industry does not yet have a design or solution to accommodate batch files of Faster Payments or CHAPS payments given the complexity of this payment process.

Our implementation programme for CoP is a Group level transformation programme and therefore the implementation approach set out in the HSBC UK response is the same for our non-ring fenced bank. [Confidential text]

In terms of our readiness, our current planning suggests the following dates, [Confidential text]:

- **To receive and respond to COP requests:** [Confidential text] ; and
- **To send COP requests and present responses to our customers:** [Confidential text]

Branch payments, Direct Corporate Access and Head Office Current Accounts (HOCAs) are within Pay.UK planned Phase 2. However, it should be noted that, at this stage, we do not have a design or solution for CoP to accommodate batch files of Faster Payments or CHAPS payments. We are considering how it may be possible to support multiple payment requests.

However, there is one specific additional area where HSBC wishes to provide feedback. This is in the area of how the implementation of Confirmation of Payee applies to PSPs with

Indirect Access to payment systems (agency bank customers) and Indirect Access Providers (of which HSBC is one).

We are aware that for many smaller players and in particular, our agency bank customers, a General Direction covering all institutions was not anticipated. Some smaller players do not have 24/7 systems to support CoP requests and the proposed implementation of CoP will require significant technology and processes change. The customer base and business model of some indirect access clients, is such that they do not perceive the need to implement a CoP service.

The broader regulatory change landscape in 2019 is full and complex with the proposed General Directions coming at the time of a complex technical and regulatory change agenda with highly interconnected dependencies. These include, PSD2, the Contingent Reimbursement Model, the Future Generation of Open Banking, Brexit, and the continued migration to the Image Clearing System. A number of these legal and regulatory requirements place considerable pressure on the capacity of smaller players to accommodate the transformation safely and will mean change for their customers too, creating the risk of change fatigue on customers and the potential for confusion.

It is important here to recognise the variety of business models that agency banks have. The larger ones offer a wide range of banking services to their customers over a variety of channels. This type of agency bank is likely to recognise the need for CoP and want to offer the service. These larger agency banks would be at risk of fraud migrating to them if they did not implement CoP.

At the other end of the scale are considerably smaller indirect access participants, for example the London branch of an overseas bank, with a small but important customer base. This type of agency bank may not see the need to implement CoP, neither will they have technical or operational capacity to implement CoP. Indeed, they may not have 24x7 operational capability.

As a result, we have concerns regarding potential unintended consequences of the proposed General Direction on competition and innovation. The cost and complexity of implementing CoP may in some cases encourage smaller or niche institutions to exit the UK payments market or reduce the payment solutions that they offer their clients.

HSBC encourages the PSR to consider appropriate *de minimis* thresholds to ensure the customer benefits of CoP are captured without these risks materialising that could lead to detriment for end users.

Notwithstanding such a threshold, given that fraud may migrate to those PSPs that have not implemented CoP, we encourage the PSR to consider whether it would be acceptable to consider a timeframe for the General Directions that is set to be achievable for the many, driven by broad market readiness, whilst avoiding moving at the pace of the slowest. This

would facilitate the greatest participation by indirect access participants that have a business and customer model that supports CoP.

This issue directly impacts on two of the consultation questions which are set out below:

**2. Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis of your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

2.1 HSBC and HBUK always been committed to implementing CoP given the scale of our customer base and reach of our operations. However, we are conscious that for many smaller players and in particular, our agency bank customers, a General Direction covering the entire industry was not anticipated. Some smaller players do not have 24/7 systems to support CoP requests and the implementation of CoP will require significant technology change that may not be possible within the proposed timeframes, particularly give the immaturity and lack of readiness in the vendor market.

2.2 Other PSPs do not perceive their customer base and business model to demand a CoP service and are confident they can manage the risk of APP Scams and misdirected payments through their business processes. For example, this might include an international bank with a UK presence solely for a small discreet set of customers from that nation. A General Direction that provides flexibility for such small PSPs to make an active choice whether to develop CoP or not, would appear sensible.

2.3 [Confidential text]

**9. Question 9: Do you agree with the deadlines for the introduction of COP? If you do not agree, please set out why different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

9.1 HSBC and HBUK always been committed to the implementation of CoP given the scale of our customer base and reach of our operations. However, we have had feedback from our agency bank customers that a General Direction covering the full range of players was not anticipated. Some smaller agency banks do not have 24/7 systems to support CoP requests and the implementation of CoP will require significant technology change. Others do not perceive their customer base and business model require the development of a CoP service.

9.2 [Confidential text]

# HSBC UK Bank PLC

**HSBC UK BANK PLC**

**CONSULTATION ON GENERAL DIRECTIONS ON IMPLEMENTING CONFIRMATION OF PAYEE**

---

---

**RESPONSE TO CONSULTATION DATED NOVEMBER 2018**

**04 JANUARY 2019**

---

---

## COVER SUBMISSION

HSBC UK Bank plc (HSBC UK) is the new ring-fenced UK retail bank within the HSBC Group, which opened on 1 July 2018. Our customers include HSBC personal and commercial customers in the UK, including those UK Business Banking customers categorised as Non-Bank Financial Institutions, UK Private Bank clients and our other UK retail brands, M&S Bank and first direct.

HSBC UK welcomes the opportunity to respond to the Payment Systems Regulator's (PSR) consultation on General Directions on implementing Confirmation of Payee (CoP). A separate response has been submitted from HSBC Bank plc focused on a number of points relevant to the different customer groups of HSBC Bank plc.

### Introduction

HSBC UK is strongly supportive of CoP and we are committed to deliver it. Given the need for interoperability in CoP services, we support the use of a General Direction. We believe this will drive widespread industry adoption, support a good customer experience through interoperability and avoid fragmentation, with fraud migrating to PSPs, payment types, accounts or channels that have not implemented CoP.

Importantly, HSBC UK regards CoP as an effective way to minimise the volume of misdirected payments, providing it is implemented in a timeframe that ensures a smooth and effective delivery for customers. If delivered properly, CoP should increase customer confidence in the payment eco-system as they gain reassurance that they are paying the intended recipient. CoP may also be a useful component in the overall tool-kit to reduce some types of APP Scams (such as invoice fraud), however we expect scammers to attempt to subvert CoP by persuading the payer that there is a good reason for any difference in the name the scammer is using.

We want to see the CoP service deployed in a way that provides good outcomes for customers from launch and is viewed positively by customers. To achieve this, customer disruption and friction in the payments eco-system must be avoided, as well as ensuring customers understand and embrace the change. We encourage the PSR to consider how the General Directions can best facilitate these outcomes for customers and we have focussed our response on suggestions for how this can be achieved. Specifically:

- Preparing customers and testing the service well;
- Providing a timeframe that allows coordination around other regulatory change and is achievable;
- Tailoring the Directions to avoid unintended consequences across the industry; and
- Ensuring the industry framework for delivering CoP is ready, appropriately governed and funded.

In summary, we believe a timeframe for the General Directions that is achievable for the many, driven by broad market readiness, with appropriate *de minimis* thresholds to avoid unintended consequences, will allow the directions to create market momentum and critical mass, leading to a positive CoP launch where the service works well for customers.

### ***Preparing customers and testing the service well***

Our view is that CoP is a landmark development in the evolution of electronic payment solutions for customers and we believe it is imperative that it is launched in a way that customers understand and find easy to use and reassuring, so they can recognise the benefits. We want CoP to be a success. CoP will introduce a significant change to the way payments are initiated for customers and with a change of this magnitude, the industry needs to work together to provide the best customer experience, whilst minimising customer disruption and concern as far as possible.

To achieve this outcome, customer and front-line staff preparation and communication will be essential. A customer education campaign will be needed, including targeted messaging and support to some customer groups. Such a campaign will be extensive, including international customers who have a UK domiciled bank account. Adequate time will be needed to train branch and contact-centre staff to understand the changes and handle the range of queries customers will have. Our view is that more time to prepare and train staff is needed than the proposed timeframe set out in the General Direction allows.

Such communications will need to be led by individual PSPs. However, to ensure maximum impact, communications will need to be underpinned by a degree of industry collaboration and coordination, to provide a common message and help customers understand the change, whilst allowing the ability to tailor direct communications in tone and language. The benefits of such communications have been shown on many previous industry led change initiatives. We are aware of increasing customer focus on the use and sharing of their data and this initiative, with mandatory data sharing, will prompt questions from customers.

Furthermore, adequate time for industry testing and live proving is essential for the integrity of the overall payment system and to ensure the service instils customer confidence from the outset. We do not believe the proposed timescales allows adequate time for industry testing and resolution of issues identified, even on a limited industry basis.

For example, we are concerned that there is very likely to be a high number of 'partial matches' and that multi-banked customers will receive a different match result from different banks depending on their interpretation of the matching rules. The proportion of payments resulting in a 'partial match' will not be understood without testing, nor workarounds identified to improve the rate of matches.

A major part of this is the character limit of the payee name field which is 18 characters within the scheme message. This will not be adequate to identify accurately the customer real name

against the customer bank account name. As a result the operating guide specifies that the payee name field can be a maximum of 140 characters. To use this longer message an additional payee name field will need to be completed by the customer (which may populate the scheme message). However, there is no requirement to do this and without collaboration to manage the approach consistently, there may be an unnecessary high rate of failed matches from truncated account names where the scheme field is used. We have raised this issue with Pay.UK as an example of the urgent need for industry testing to identify how issues such as this are being addressed and to manage risks proactively in the interest of customers.

Customer education regarding the position where there is no match will also be very important if CoP is to have any impact on APP fraud.

HSBC UK notes that the CMA Open Banking remedy was introduced with a three month industry test process. Given the greater scale of CoP we believe Pay.UK will need to carefully coordinate a test process to ensure success and this will require at least three months to be effective. It should also be noted that there will be a high volume of transactions being routed from the go live date. Any significant defects could have an immediate impact on the ability of customers to complete transactions with confidence.

In our view, more preparation time for the industry will allow the potential for poor customer outcomes to be proactively minimised, such as confusion, complaints, high volumes of abandoned payments and high service opt out requests. We are concerned that there is a risk some customers might conclude that CoP is unreliable and pay little attention to CoP responses, compelled by media and political scrutiny on any the roll out failures. Such confusion could arm scammers to use social engineering to work around CoP messages.

***Providing a timeframe that allows coordination around other significant regulatory change and that is practicable***

An important context to the timeframe for implementation is the unprecedented volume of changes customers will see to their payment journeys in 2019. This will include change resulting from the APP Scam Contingent Reimbursement Model Code, PSD2, regulatory technical standards, secure customer authentication and common and secure open standards of communication. We note that some consumer groups are starting to express concern about the volume of change within the payments eco-system in 2019. We encourage the PSR to consider a timeframe for the General Directions that would allow the coordination of changes to simplify the customer experience and guard against customer change fatigue and customer friction.

One key area where coordination is needed relates to the APP Scam Contingent Reimbursement Model Code (CRM Code), to which CoP is closely inter-linked. In our view, the Code should be finalised, including the liability model and evidential standards required, before General Directions can be in place for CoP. This will enable there to be greater clarity with regard to how CoP will work alongside this voluntary Code, including the effect of the

various CoP responses on liability and disputes under the Code, to ensure consistent outcomes for customers.

For example, in relation to the CRM Code, it is understood that obtaining a match response would suggest that the payer has undertaken due level of care. A payer's decision to proceed with a payment after a no match response can be taken into account by the PSP when deciding whether to reimburse the payer. However, it is unclear what the impacts would be where a payer proceeds with payment after obtaining a partial match response, or if the payee has opted out of the service.

In terms of our own programme for implementing CoP, HSBC UK is committed to delivering CoP and we have mobilised a major programme to this end, across the HSBC Group. In practical terms, delivery is a large scale operational and technical change. [Confidential text] Furthermore there is a considerable operational and communication challenge to train branch and contact centre staff to deal with the large number of customer queries that can be expected after launch. Adequate time is needed from the point at which the service is ready to train our staff to be ready to support customers effectively.

Our plan is to implement CoP across our brands, channels and different customer products and groups. [Confidential text]

In terms of our readiness, our current planning suggests the following dates, [Confidential text]:

- **To receive and respond to COP requests:** [Confidential text] ; and
- **To send COP requests and present responses to our customers:** [Confidential text]

Branch payments, Direct Corporate Access and Head Office Current Accounts (HOCAs) are within Pay.UK planned Phase 2.

These dates are subject to stability in the Pay.UK Rules and Operating Guide, subsequent finalisation of our implementation plan and no major technical challenges within the programme. Our prioritisation is based on our APP Scam data.

[Confidential text]

Putting our own programme implementation to one side, we have a number of broader practical concerns about the implementation challenges against the timeframe proposed. Specifically:

- **The CoP Rules and Operating Guide is not yet finalised nor stable** - The draft Rules and Operating Guide were shared with the industry by Pay.UK in October 2018, delayed by around three months, and is not yet final (Version 3 issued 7 December 2018). Likewise, the Terms and Conditions are still in draft with version 2 issued on 11

December 2018 and a number of key issues remain under debate. We understand that discussions with the Information Commissioner's Office (ICO) have not gone beyond preliminary engagement. Resolution of data privacy concerns is critical to the launch of CoP and we urge the PSR to engage with the ICO directly to ensure there is no conflict between the General Data Privacy Regulation (GDPR) requirements and a general direction issued by the PSR. Without stability and certainty around the operational and legal framework for the service, we do not have the certainty required to push forward our implementation programme. We remain concerned that specifications will continue to evolve and change.

Specifically, there are a number of areas of the Rulebook which are still subject to industry discussion and debate and which create challenges for PSPs to implement CoP. These include issues around the roles and responsibilities of Account Servicing PSPs (ASPSPs), and uncertainty regarding the interaction between Pay.UK and Open Banking. ASPSPs are required to comply with a wide range of different rules and operation guides, which can be changed unilaterally or supplemented by Pay.UK without consultation and no materiality governing the implementation period. There is no clear governance around change control. There is also no liability cap and wide indemnity for third party claims. We do not believe this provides the foundation for a successful service at launch.

- **The vendor market is not ready** - The Rules and Operating Guide have not yet been shared with vendors, although on 12 December 2018, Pay.UK confirmed that these can be shared with vendors providing a Non-Disclosure Agreement is in place and Pay.UK has agreed. This process will take time. As a result, there is likely to be a limited vendor market that will be ready to support industry to deliver within the timescales of the proposed General Direction.

Likewise, given that the proposed coverage of the General Direction (PSPs using Faster Payments and CHAPS) is a wide PSP eco-system, vendor capacity to support the market will be limited, which will inevitably impact the pricing of such services and mean some PSPs will not be able to source a supplier. This situation has been seen in the market for expert software and technology providers for the new Image Clearing Service, where the tight timescales limited vendors' capacity to support the changes.

- **The broader regulatory change landscape in 2019 is full and complex** - The proposed General Directions come at the time of a complex technical and regulatory change agenda with highly interconnected dependencies. These include, PSD2, the Contingent Reimbursement Model, the Future Generation of Open Banking, Brexit, and the continuing migration to the Image Clearing System. A number of these legal and regulatory requirements place considerable pressure on the capacity of organisations to accommodate the transformation safely and will mean change for

their customers too, creating the risk of change fatigue on customers and the potential for confusion. There is a further risk that prioritising IT development for CoP risks IT delivery for other change such as PSD2. Alternatively, IT development work would be carried out in parallel, creating significant additional risk which could threaten the ongoing stability of the customer payment solutions, particularly if time for testing is compressed by aggressive timelines.

***Tailoring the Directions to avoid unintended consequences across the industry***

In our view, there are a number of potentially unintended consequences of the proposed General Direction on competition and innovation. The cost and complexity of implementing CoP could in some cases encourage smaller or niche institutions to consider the viability of their business model in the UK payments market. For institutions of all sizes, a one-size-fits-all approach materially increases the cost of small-scale pilot activity which could inevitably stifle innovation. HSBC UK therefore encourages the PSR to consider appropriate *de minimis* thresholds for a CoP service, such as using payment volumes, to ensure the customer benefits of CoP are captured without these risks materialising.

To support the broader market, we also encourage the PSR to consider whether it would be acceptable to consider a timeframe for the General Directions that is set to be achievable for the many, driven by broad market readiness, whilst avoiding moving at the pace of the slowest. Alongside appropriate *de minimis* thresholds for a CoP service, this will allow the directions to create market momentum and critical mass, whilst providing the benefit that some very small PSPs may choose not to implement CoP, if appropriate to a unique business model or customer base.

In addition, we encourage the PSR to consider a direction tailored to focus on the customer groups that are most at risk of harm from APP Scams and Misdirected Payments, namely personal and small business customers making single transaction payments. Large corporate and government customers making batch file payments are at a lower risk, and at this stage, the industry does not yet have a design or solution to accommodate batch files of Faster Payments or CHAPS payments given the complexity of this payment process.

***Ensuring the industry framework for delivering COP is ready and appropriately governed and funded***

There is a clear dependency for the implementation of CoP on registration with the Open Banking (OB) Directory. Given the range of PSPs that would need to register with the OB Directory to send and receive CoP APIs, we do not believe the Open Banking Implementation Entity (OBIE) would have the capacity to on board this volume of participants within the timeframe, particularly as the next release is scheduled for March 2019 with live testing running for three months thereafter. Furthermore, registration with the directory will mean smaller participants will be caught by Open Banking requirements, which they may not be ready for.

Notwithstanding capacity, we do not believe the governance, control framework or capital adequacy of OBIE is appropriate for a cross-industry service. Specifically:

- OBIE is constituted under the CMA Order and overseen by a Trustee who has a mandate with the CMA9 institutions. This makes its governance inherently unsuitable for the live running of a service not related to the CMA Order – it must prioritise the needs of the CMA Order ahead of any other activity. If it failed to do so, the CMA Order requires us to act, and the Trustee Mandate sets out the process by which this should be escalated to the CMA. This creates a clear conflict of interest with regards to an important non-CMA activity such as CoP.
- OBIE's control framework has not been subject to regulatory scrutiny, and its operating model lacks the maturity for a material 'run' service covering whole of industry.
- The CMA9 fund and backstop the OBIE. All its funds are hypothecated towards CMA needs. Therefore there is no capacity to absorb losses or make-good in the event of a service disruption. This creates a material weakness in CoP and the voluntary code. As a funding institution, HSBC is strongly opposed to bearing contingent liability against these risks.

We ask that the PSR mandate the transfer of the OB Directory asset to Pay.UK management and governance as a pre-requisite to CoP being enabled in order to address the three issues raised. We understand that all stakeholders (HMT, CMA, Pay.UK and CMA9) have agreed to this target state in principle, therefore we believe the transfer is achievable within the timescales required. This would also alleviate the current uncertainty regarding the roles and responsibilities of the parties.

1. **Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there any other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any comments on the issues raised above?**
  - 1.1 We support the use of a General Direction to secure the PSRs objectives. In our view, a General Direction is necessary to ensure widespread industry adoption in a coordinated timeframe which is essential because of the network requirement for CoP to work.
  - 1.2 However, we are concerned by the timeframes as they stand (please see our above cover submission and our response to Question 9) and encourage the PSR to consider a more nuanced direction (with *de minimis thresholds* for a CoP service such as payment volumes) to avoid potential adverse impacts on innovation and competition.
  - 1.3 Alongside the question above, the consultation asks for representations on whether it is necessary for any direction to include a provision requiring those PSPs which are not the sending or receiving PSP, but are in some way involved in the transaction (such as a Payment Initiation Service Provider (PISP)), to facilitate the CoP process. Our understanding on this point is that the obligations regarding CoP fall on the account holding bank and not the PISP. We do not have any objection to the PISP conducting CoP checks per se. However, given the structure of contingent liability set out in the voluntary CRM Code, HSBC UK is of the view that we could not reasonably be required to rely on CoP checks conducted by a PISP and this points back to the need to resolve the CRM code, particularly in respect of multi-party involvement in the payment initiation process.
  
2. **Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis of your view, particularly having regard to the likelihood of achieving the benefits of CoP?**
  - 2.1 To achieve the PSR's objectives, we believe a broad level of market consistency is critical. As an interoperable service, widespread industry adoption is necessary to make the service work well and to be effective.
  - 2.2 At HSBC UK, we have always been committed to implementing CoP given the scale of our customer base and reach of our operations. However, we are conscious that for many smaller PSPs, a General Direction covering the full range of PSPs was not anticipated.

- 2.3 Given that fraud is likely to migrate to those PSPs that have not implemented CoP, we support a timeframe for the General Directions that is achievable for the many, driven by broad market readiness, whilst avoiding moving at the pace of the slowest.
- 2.4 In broad terms, HSBC UK encourages the PSR to consider appropriate *de minimis* thresholds for a CoP requirement to ensure that the customer benefits of CoP are captured without adverse impacts on competition or innovation materialising. This will allow the directions to create market momentum and critical mass, whilst providing the benefit that some very small PSPs may choose not to implement if appropriate to a unique business model or customer base.
3. **Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**
- 3.1 HSBC UK believes it is imperative that the vast majority of PSPs are able to receive and respond to a CoP request. We do not want to implement our sending capability and find customers frequently are unable to receive a CoP response. This increases the vulnerability of our customers to scams when sending payments to such PSPs and provides an entry loophole for scammers.
- 3.2 Arguably, there is a competitive incentive for offering a CoP service to customers and the General Direction need not cover this aspect. However, we believe that CoP is a landmark change in the way payments are made in the UK. Providing the service is launched and implemented well, broad market coverage both for sending and receiving payments will deliver the best customer outcomes through interoperability, consistency of experience and communication of the development as a cross-industry change. As stated above, appropriate *de minimis* thresholds for the service will allow some flexibility for the benefit of competition and innovation.
4. **Question 4: Do you think that we should consider giving directions in relation to both FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment schemes should be in scope?**
- 4.1 The CRM Code covers both Faster Payments and CHAPS. Both schemes are vulnerable to APP Scams and misdirected payments and therefore we intend to deliver CoP for both payments made by Faster Payments and CHAPS. Our capability to receive and respond to CoP requests will be scheme agnostic.

5. **Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

5.1 In principle, we support delivery of CoP to a broad range of channels to ensure maximum coverage and market consistency. However, the breadth of technical change required to cover all channels will be complex and challenging to implement, and not achievable within the proposed timescales. Some legacy channels, such as in-branch kiosks are low priority. On the basis of a longer timescale, we support General Directions that apply to all main channels. If a longer timeframe is not acceptable, we suggest prioritisation of online and mobile channels.

5.2 We note that the draft Pay.UK rules apply only to when a new payment mandate is being set up or changed and therefore we have established our implementation programme on this basis. Our view is that applying CoP to all payment initiation requests introduces unnecessary friction into the customer payment experience for known payees. The risk of a scam or misdirected payment is vastly reduced for an existing or trusted payee and therefore we do not believe the General Direction should extend to existing payment mandates.

5.3 As noted in the introduction, a broad General Direction could have an adverse impact on competition and innovation. The cost and complexity of implementing CoP could in some cases encourage smaller or niche institutions to consider the viability of their business model in the UK payments market or reduce the payment solutions that they offer their clients.

5.4 For institutions of all sizes, a one-size-fits-all approach materially increases the cost of small-scale pilot activity which could inevitably stifle innovation. As stated, HSBC UK therefore encourages the PSR to consider appropriate *de minimis* thresholds to ensure the customer benefits of CoP are captured without these risks materialising.

6. **Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

6.1 The Pay.UK CoP proposition document states that ASPSPs will be responsible for deciding whether or not an opt-out request will be approved. At this stage, there are no parameters set for these decisions and it is expected that different PSPs will treat such requests differently. This may have implications for the CRM Code which the PSR may wish to consider in the context of the directions to ensure consistent customer outcomes are achieved in relation the CRM Code.

6.2 We believe it is critical that the opt-out provision is in place for vulnerable customers, however, there is a clear risk scammers may target any opt-out. There is also a risk that there will be some customers who wish to opt-out because they do not like the

idea of their account name being shared. The impact of refusing to allow a customer to opt-out of CoP must also be evaluated to ensure that this does not conflict with GDPR requirements.

6.3 We suggest the PSR take legal advice on whether the General Direction can provide a means for PSPs to reject such requests if it believes this is a risk that needs to be prevented and potential GDPR implications.

6.4 We note that there is currently no legal certainty on the basis for processing the account holder's name for the purpose of CoP within the Data Protection Act 2018 and GDPR. If participation constitutes a legal obligation for the PSP, this may need to be reflected within the existing UK Data Protection legislation. This may be necessary to avoid PSPs being in breach of GDPR if they refuse to allow customers to opt-out of CoP.

## 7. **Question 7: Should any directions cover the sending of money from both individual and business accounts?**

7.1 Both personal and small business accounts are vulnerable to misdirected payments and APP Scams. Our intention is therefore to implement our CoP solutions for both types of account to protect business and retail customers. We plan to implement our retail solution first as we see a higher volume of misdirected payments and successful scams against personal customers.

7.2 To achieve the PSR's objectives, we believe market consistency and coverage is critical. Covering both business and personal accounts will ensure customers have a consistent experience regardless of who they are paying and avoid scammers targeting business accounts for scams or as mules. Furthermore, given that the CRM Code covers both personal and business accounts, we believe it is appropriate for the General Directions to cover both.

7.3 However, developing CoP for business accounts adds to implementation complexity, not just technically but also in terms of staff training and customer messaging. The current proposed timescale for the General Direction is made more challenging with its scope covering both business and personal customers.

7.4 It should also be noted that we do not yet have a design or solution for CoP to support businesses using file based Faster Payments or CHAPS payments. A nuanced direction that focusses on personal and business customers making single transactions, would focus the delivery of CoP where we understand there to be the biggest risk of Authorised Push Payment Scams or misdirected payments and allow batch solutions to be developed competitively in time.

8. **Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

8.1 In line with our response to Question 3, HSBC UK believes it is imperative that the vast majority of PSPs are able to receive and respond to a CoP request. We do not want to implement our sending capability and find customers frequently are unable to receive a CoP response. This increases the vulnerability of our customers to scams when sending payments to such PSPs and provides an entry loophole for scammers.

8.2 Arguably, there is a competitive incentive for offering a CoP service to customers for sending and the General Direction need not cover this aspect. However, we believe that CoP is a landmark change in the way payments are made in the UK, and broad market coverage both for sending and receiving, providing the service is implemented well, will deliver the best customer outcomes through consistency of experience and communication of the development as a cross-industry change. Therefore we believe the directions should cover both sending and responding to CoP requests.

8.3 In practical terms, we believe a phased rollout of receiving requests and sending requests would be beneficial in terms of managing the complexity of our programme.

9. **Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

9.1 As set out in our cover submission above, HSBC UK is committed to delivering CoP. We support the approach of a General Direction but have a number of concerns that the proposed timeframe does not encourage implementation of CoP in a way that will provide good outcomes for customers. In summary, we believe a later timeframe than proposed will:

- Allow for well-planned and delivered customer communications and staff training, with appropriate collaboration across the industry for consistency – ensuring customers understand what is happening and why;
- Enable coordination of implementation around other regulatory change – avoiding customer change fatigue and confusion;
- Provide time for a good level of industry testing, to deliver a service that works well for customers and instils confidence from launch;
- Provide a timeframe that is practicable for a complex and major technical and operational change during a concurrent period of large scale change to the

payments eco-system, to avoid operational failures on launch risking customer distress and confusion;

- Ensure there is an adequate vendor market in place, to support broad market delivery of the service;
- Ensure the industry framework for delivering COP is finalised, ready and appropriately governed and funded and aligns with the CRM Code, to provide stability for individual PSP implementation programmes and to ensure consistency of customer outcomes in the CRM Code once CoP is live.

9.2 Given that fraud is likely to migrate to those PSPs that have not implemented CoP, we support a timeframe for the General Directions that is set to a timescale that is achievable for the many, driven by broad market readiness, whilst avoiding moving at the pace of the slowest.

9.3 We believe this is the best way to achieve the PSR objective and manage risks. A later date will enable market and industry readiness including a well-coordinated programme of testing, communications and implementation planning. We understand the PSR's desire to see CoP implemented quickly, however the focus must be on the right customer outcomes which will only come from market readiness.

9.4 A later date does not preclude firms the flexibility to move faster and carry risk under the CRM if they cannot deliver before then. In particular, it would allow firms to consider PSD2 changes to customer journeys jointly with CoP and ensure clear communication to customers. For a new TPP channel, it would not create a new requirement ahead of the fallback exemption application required under the Regulatory Technical Standards.

9.5 In terms of our own programme for implementing CoP, and as set out in the summary above, our plan is to implement CoP across our brands, channels and different customer products. However, our current view is that HSBC will need to prioritise delivery of some brands and channels over others and that even on this basis, we are unlikely to achieve the dates as set out in the consultation.

9.6 As stated above, in terms of our readiness, our current planning suggests the following dates, [Confidential text]:

- **To receive and respond to COP requests:** [Confidential text] ; and
- **To send COP requests and present responses to our customers:** [Confidential text]

Branch payments, Direct Corporate Access and Head Office Current Accounts (HOCAs) are within Phase 2. However it should be noted that, at this stage, we do not have a design or solution for CoP to work for batch files of Faster Payments or CHAPS payments. We are considering how it may be possible to support this.

[Confidential text]

These dates are subject to stability in the Pay.UK Rules and Operating Guide, subsequent finalisation of our implementation plan and no major technical challenges within the programme. Our prioritisation is based on our APP Scam data.

10. **Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

10.1 As set out above, we support the approach of General Directions to achieve the PSR's objectives, providing they are set to an achievable timeframe and encourage good customer outcomes.

11. **Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

11.1 We agree that CoP will deliver a reduction in misdirected payments and in some types of APP fraud (such as invoice fraud).

11.2 As already stated in our response, we are concerned that a too rapid implementation will lead to high numbers of partial matches and a poor customer experience. This could lead to customers being less receptive to CoP and responding negatively to partial or non-matches (either ignoring the message or abandoning the payment). We consider that a £75m benefit for 2H18 described in the consultation document is therefore likely to be over optimistic, and in the worst case lead to a decrease in benefits in future years.

11.3 The PSR needs to take account of the fact that any anti-fraud measure or anti-scramming measure will inevitably be met by fraudster and scammer reaction. This could include the migration of scams to PSPs or PISPs that have not implemented CoP.

11.4 Scammers are skilled social engineers and will inevitably seek to confuse the customer and make partial matches or declines acceptable. For example, they may tell the customer that they will see a decline and provide a false but persuasive reason, such as a maiden name, middle name, or trading name. Media noise around partial matches (which we expect if there are high numbers of partial matches) may further provide further fuel for scammers to convince a payer of a legitimate reason for the message.

11.5 The model of benefits achieved by the introduction of CoP therefore needs to factor in the efforts of scammers to subvert, reduce or even avoid it.

- 11.6 The CoP functionality will extend and improve over a ten year period, so this could offset declining benefit arising from scammers' workarounds. The PSR may wish to consult PSOs regarding their experience of the benefits over a period of time arising from anti-fraud measure. An example is 3-D Secure in the cards environment.
12. **Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**
- 12.1 It is difficult for HSBC UK to assess whether the capital expenditure cost of £200m across the industry is correct, likewise the annual running cost of £20m pa.
- 12.2 However, we are aware that for a large PSP that has multiple channels and brands the costs are substantial.
- 12.3 [Confidential text]
- 12.4 [Confidential text]
- 12.5 We note that the PSR have issued a notice requiring HSBC to support the gathering of evidence to inform the analysis of the costs and benefits of requiring PSPs to implement CoP. HSBC has provided a detailed request to that request alongside this response.
13. **Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree please set out what you consider would be more appropriate and your view of the impact that would have.**
- 13.1 The use of a sensitivity analysis is important in assessing the cost-benefit analysis. We agree that there is a significant benefit arising compared to the scenario of not implementing CoP at all.
- 13.2 The PSR may wish to place an additional filter to estimate high/medium/low effectiveness of the fraudster and scammer reaction.
- 13.3 The PSR may wish to place a filter relating to a successful or unsuccessful launch of CoP. An unsuccessful launch would be one that leads to high levels of customer confusion, significant numbers of partial matches or false negatives / positives. This could potentially lead to customers not having confidence in the responses they receive from CoP leading to an erosion in benefits.
14. **Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits? Do you consider that imposing April**

**and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example 2020 or later?**

- 14.1 We have concerns relating to the cost/benefit analyses of an April/July implementation date as compared to those of a launch in 2020 or later.
- 14.2 Clearly delaying a launch would reduce the benefits that could be expected to accrue in 2019. On the other hand if a later launch meant a more successful customer implementation this could lead to improved benefits over the longer term.
- 14.3 A short timescales for implementation does not provide sufficient time for vendor on-boarding and undertaking checks that PSPs are required to undertake when sharing data with third parties.
- 14.4 CoP is a large complex programme, and as already stated we have major concerns over an April / July 2019 launch. An unsuccessful launch is one that leads to high levels of customer confusion, significant numbers of partial matches or false negatives / positives. This could potentially lead to customers not having confidence in the responses they receive from CoP leading to a significant erosion in benefits. Therefore, we believe the overall effects of implementing CoP later on would be better because poor customer outcomes are more likely to be avoided.

**15. Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable customers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equity duty, in deciding whether to give directions and considering alternatives?**

- 15.1 This is a delicate area, as the implementation of CoP will encourage scammers to target those not using CoP whether due to their PSP/PISP not having implemented it or because the customer is unable to use CoP.
- 15.2 That said we accept that there are scenarios where a customer may need or wish to opt out of CoP or be unable to use the CoP service due to vulnerability.
- 15.3 There is a need also to consider the appropriate level of care in the voluntary code. If the customer is unable to use CoP for good reason, then the non-use of CoP is not customer fault, but also not the PSP's fault and leads to the no-fault scenario.

# Information Commissioner's Office

## **The Information Commissioner's response to the Payment Systems Regulator's consultation on general directions for the implementation of Confirmation of Payee**

The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Commissioner welcomes the opportunity to respond to the Payment Systems Regulator's consultation on general directions for the implementation of Confirmation of Payee.

We have reviewed the consultation paper and identified that the current focus of many of the questions does not specifically require data protection input at this point. However, there are aspects of Confirmation of Payee that may have implications for the privacy of individuals, depending on the nature of any Confirmation of Payee system and how individuals' personal data is used within that system.

The ICO would therefore welcome the opportunity to engage with the Payment Systems Regulator, and relevant stakeholders involved in the Confirmation of Payee process, to discuss data protection and privacy implications for the proposed system.

# Industrial Bank of Korea

To: [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)  
Subject: CONSULTATION ON GENERAL DIRECTIONS ON IMPLEMENTING CONFIRMATION OF PAYEE

---

Dear Sir/Madam,

We are not a direct participant of any payment system in UK. We are an indirect participant of BACS system through HSBC. As an institution which has come across several cases of APP scams, we would like to give our response to some of the questions in the consultation.

Question 4 and 5 : We receive large number of SWIFT messages from our branches in S.Korea which are again retransmitted by us to the Banks in UK/Europe for credit of beneficiaries' accounts. Most of these payments are trade related. We have faced several cases in which our customers in S.Korea are tricked to send payments to a different account. These messages are send by the fraudsters after hacking the email accounts of one of the parties to the transaction. Several customers of our bank have lost huge sums on account of these frauds. Many of the fraudulent credits have gone to accounts maintained with big banks in UK.

We use SWIFT to send these payment messages. We are of the opinion that the directions should apply to all payment channels (including SWIFT) that an FPS or CHAPS payment can be initiated from..

Question 7: The directions should cover the sending of money from both individual and business accounts. We have found that the losses incurred by Small businesses are huge in this kind of frauds.

Thanks and regards

████████



████████████████████  
████████████████████████  
██████████████████████████  
████████████████████████████  
██████████████████████████  
██████████████████████████  
██████████████████████████



Please consider the environment before printing this e-mail

This e-mail is intended only for the person to whom it is addressed. If an addressing or transmission error has misdirected this e-mail, please notify the author by replying to this e-mail. If you are not the intended recipient you must not use, disclose, print or rely on this e-mail. This e-mail is not intended nor should it be taken to create legal relations, contractual or otherwise. Industrial Bank of Korea, London Branch is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

# Link Asset Services

Confirmation of Payee Consultation  
 Payment Systems Regulator  
 12 Endeavour Square  
 London E20 1JN



Response sent via email  
 app-scam-pso-project@psr.org.uk

19 December 2018

Dear Sir

**Consultation on general directions on Confirmation of Payee – November 2018**

Link Market Services are part of the Link Group and provide share registration and value-added services to over 5 million shareholders on behalf of more than 1,100 companies in the UK and Ireland including the payment of 9 million separate dividend and interest payments annually. We are responsible for share registers and share registration, corporate actions, share plans, share dealing and company secretarial support (via our Company Matters business) across a base of clients that range from small or recently floated to large multinationals.

We also provide custody and settlement operation supporting overseas companies listing on the UK market and a share dealing service primarily aimed at shareholders in its client companies. Some of these client companies are based in other EU countries. Jai Baker, our Head of Industry, chairs the ICSA Registrars Group and Link sit on the ICSA Company Secretaries Forum. We are also a member of the Quoted Companies Alliance.

Thank you for the opportunity to respond to your proposals in the consultation.

**General**

The share registration industry in the UK and the individual registrars like Link Market Services are keen to support and promote changes that combat fraud and aim to increase protection for consumers and companies. However, we are conscious that more sophisticated payment message systems including Confirmation of Payee (CoP) need to be timely, bring benefits that are affordable and that outweigh the increasing potential points of failure that may be introduced by such sophistication.

**Specific comments**

**Why are we consulting on directions?**

<p><b>Question 1</b></p>	<p>Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that</p>
--------------------------	--

	would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?
<b>A1</b>	Giving directions would be the right approach to ensure an orderly and timely change within the market and would provide certainty to all those involved. However, there may be a need to adjust the timescales for implementation as not all stakeholders will be in the same position to move to implementation within the suggested timetable.

### The proposed scope of the directions

<b>Question 2</b>	Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?
<b>A2</b>	As paying agent to issuer clients, our role of distributing bulk payments (commonly dividend distributions) is limited to just that. There is no need, and perhaps no perceived benefit, in a registrars' participation in a full CoP program.
<b>Question 3</b>	Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?
<b>A3</b>	Yes
<b>Question 4</b>	Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?
<b>A4</b>	Limiting initial implementation to one payment system would allow systems and procedures to be tried and tested prior to extension to other payments systems. PSPs and customers would have an opportunity to experience the changes and fine tune the activity around CoP before further payments systems are brought online.
<b>Question 5</b>	Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?
<b>A5</b>	Only applying CoP to new payment mandates or changes to payment mandates would seem to be a sensible approach that would limit traffic and the unnecessary involvement of the payer. However, some thought would need to be given to those existing mandates in the payments systems that may require verification to avoid scams or continued misdirection.
<b>Question 6</b>	How should any directions deal with the potential for people to opt out of the CoP process?
<b>A6</b>	The primary risk is to the efficacy of CoP if opt outs are allowed. Such a possibility could allow payment scams and misdirection to continue unchecked even if the decision and liability rests with the payer. Controlling and managing opt outs may prove to be complex and unwieldy as systems would need to be able to enable and record opt out actions.

<b>Question 7</b>	Should any directions cover the sending of money from both individual and business accounts?
<b>A7</b>	Yes.

### The rationale for our timeframe

<b>Question 8</b>	Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?
<b>A8</b>	Yes but within defined and agreed parameters.
<b>Question 9</b>	Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.
<b>A9</b>	There may be a need to adjust the timescales for implementation as not all the players will be in the same position to move to implementation quickly in 2019 given the requirement for system changes, or third part solutions to be available and customer awareness to be completed. A phased implementation of CoP in different payment systems might help to keep costs down and ensure that issues encountered in operating the system can be rolled out into other payment systems as they are brought online.

### Alternative approaches

<b>Question 10</b>	Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?
<b>A10</b>	We have not yet been able to conduct a full analysis given the tight review timescales of this consultation. There will be alternatives available no doubt but we are not in a position to communicate what they may be.

### Cost Benefit Analysis

<b>Question 11</b>	Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.
<b>A11</b>	Not for us. We believe the cost of implementation will outweigh the benefits in our operations.
<b>Question 12</b>	Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.
<b>A12</b>	No. For us, there are multiple system developments required across our business lines and the timeframe alone does not lend itself to our reaching compliancy ahead of 1 April 2019.
<b>Question 13</b>	Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more

	appropriate and your view of the impact that would have.
<b>A13</b>	We believe the cost of implementation will outweigh the benefits in our operations.
<b>Question 14</b>	What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?
<b>A14</b>	Implementation in 2019 is likely to increase costs as more resources will be required to ensure system is in place quickly. Some assumed cost saving benefits may not materialise if solutions do not function as planned and errors or “bugs” take time to fix. In addition, trust in the system may be harmed if early implementation goes ahead.

**Equality Impact Assessment**

<b>Question 15</b>	Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?
<b>A15</b>	No.

We would be happy to discuss our comments further if required.

Yours faithfully,



# Lloyds Banking Group PLC

**LLOYDS BANKING GROUP PLC**

**Response to PSR Consultation on general directions  
for the implementation of Confirmation of Payee**

Submission Date 04/01/2019

## Introductory Comments

Lloyds Banking Group (LBG) welcomes the opportunity to respond to the Payment Systems Regulator's (PSR) consultation on general directions for the implementation of Confirmation of Payee (CoP).

The UK payments landscape is changing. Advances in technology and initiatives such as the revised Payment Services Directive (PSD2) and open banking are increasing the use of digital payment services. As usage increases, the risk of customers falling victim to fraud online also increases, bringing the issue of fraud and how to tackle it to the forefront of the regulatory agenda.

We are supportive of any initiatives that can help to tackle fraud and give customers peace of mind that their payments have reached the right recipients. We agree strongly with the PSR that implementing CoP is the right thing to do. However, we caution that CoP won't provide a comprehensive solution to Authorised Push Payment (APP) scams. Perpetrators of APP scams that draw on social engineering techniques will adapt their methods in the light of CoP, meaning that such scams will not be eradicated. More widely, where CoP provides an effective obstruction, perpetrators are likely to move to committing other types of fraud. In the light of these observations, we recommend that the PSR considers CoP in the context of other, complementary initiatives – both from a policy and an implementation perspective.

Nevertheless, we support the PSR's desire for CoP to be implemented quickly. We agree that giving a direction in relation to receiving and responding to CoP requests will drive the necessary network effect and help ensure that CoP is widely available. However, we consider that the case for regulatory intervention via a direction in relation to sending CoP requests is weaker, and we are not supportive of such an approach.

We believe that enabling PSPs to develop sending propositions (which could potentially be CoP combined with other innovative solutions) on their own timelines will be a more effective way of achieving the PSR's objectives. Particularly given that it will enable an iterative, test and learn development approach, which will maximise the likelihood of success and usability. We expect competition forces (and potentially mandating the contingent reimbursement model) to help drive the development of sending capabilities when responding and receiving capabilities are in place.

If the PSR is minded to issue one or more directions, we recommend that when setting deadlines it balances speed of delivery against enabling the industry to implement robust propositions that meet customer needs.

The proposed April 2019 deadline for receiving and responding to requests is challenging, but LBG is on track to meet it for the majority of its customer accounts. We recognise though that there are wider challenges for the industry – particularly for PSPs that intend to utilise third party providers for their CoP provision. We understand that there is not yet an off the shelf CoP solution available in the marketplace.

Regarding sending CoP requests, we believe the proposed deadline of July 2019 is undesirable because it won't allow sufficient time to implement a robust and effective service. From a technical perspective, LBG is aiming to meet the deadline for most FPS and CHAPS payments via digital channels for retail and small business customers across our core brands, subject to the caveats we have referenced in our response. However, we are concerned there will be insufficient time to prepare customers for this change to the payments journey, and we note the risk of introducing unnecessary friction. For example, we understand that, across the industry, name matching rates are not yet at acceptable levels in test conditions. These must be improved ahead of any 'big bang' implementation to ensure customer trust and buy-in.

We have suggested alternative approaches to setting deadlines for any directions in our response to question nine. These focus on setting staggered deadlines that take account of the customer and channel type, as well as potentially payments volumes and values. We also note the Netherlands' CoP equivalent, where implementation was delivered using a phased approach. More widely, we recommend that the PSR ensures that any deadlines it sets align with the outputs of Pay.UK, which is developing the industry standards and guidelines for CoP.

As noted, we also recommend that the PSR considers CoP in its policymaking alongside other relevant initiatives, such as the contingent reimbursement model (CRM) and secure customer authentication (SCA). Mandating the CRM would provide additional protection for customers that are subject to APP scams. It would also provide PSPs with the flexibility to determine how best to protect customers in the context of their individual business models and risk appetites. We provided our thoughts on this in response to CP17/2. We are keen to collaborate with the PSR and other relevant bodies to address the feasibility of this.

Finally, we believe that CoP implementation would benefit from coordination that enables CoP implementation to dovetail with other relevant initiatives. A coordinated approach would bring the greatest overall benefits to customers and PSPs. It would also enable PSPs to prepare customers and communicate with them holistically about the various enhancements to their payments journey.

## Response to Consultation Questions

**1. IS GIVING DIRECTIONS UNDER SECTION 54 OF FSBRA TO PSPS REQUIRING THEM TO INTRODUCE COP THE RIGHT APPROACH TO SECURING OUR OBJECTIVES, IN PARTICULAR TO REDUCE SIGNIFICANTLY LOSSES AND HARM FROM APP SCAMS AND ACCIDENTALLY MISDIRECTED PAYMENTS AS SOON AS POSSIBLE? ARE THERE OTHER APPROACHES THAT WOULD LEAD TO THE SAME OUTCOMES THAT WE SHOULD CONSIDER, AND, IF SO, WHAT ARE THEY? DO YOU HAVE ANY OTHER COMMENTS ON THE ISSUES RAISED ABOVE?**

- 1.1 Yes, Lloyds Banking Group (LBG) is supportive in principle of giving a direction to PSPs under section 54 of FSBRA to introduce CoP. There is a need to accelerate implementation of CoP across the industry, which will help to enable the network effect that is required to make CoP a success.
- 1.2 We believe CoP will function as a valuable tool for many customers and provide them with peace of mind when sending payments. However, we are mindful that CoP will not provide a full solution to APP scams and accidentally misdirected payments.
- 1.3 We recommend that any direction from the PSR applies only to receiving and responding to CoP requests. A direction mandating that PSPs receive and respond to requests should help to drive the necessary network effect. However, we are not persuaded that giving a direction to send CoP requests will be the most effective way of achieving the PSR's objectives – we expand on this in our response to question eight.
- 1.4 We suggest that consideration be given to how CoP interacts with other relevant initiatives such as the Contingent Reimbursement Model (CRM) and secure customer authentication. Finally, we consider there is a need for coordination to aid orderly CoP implementation, and ensure there is read across to other relevant initiatives.
- 1.5 Lastly, if the PSR is minded to give directions, it would be helpful if any reporting requirements for PSPs are set out at the outset.

**2. ASSUMING DIRECTIONS IN RESPECT OF FPS AND CHAPS ARE GIVEN, ARE THERE ANY TYPES OF PSP THAT SHOULD NOT BE GIVEN THE DIRECTIONS? WHAT IS THE BASIS FOR YOUR VIEW, PARTICULARLY HAVING REGARD TO THE LIKELIHOOD OF ACHIEVING THE BENEFITS OF COP?**

- 2.1 LBG believes that any direction to receive and respond to CoP requests should be articulated as applying to PSPs that receive FPS and / or CHAPS payments on behalf of their customers. Likewise, any direction to send CoP requests should apply to PSPs that send FPS and / or CHAPS payments on behalf of their customers. Setting out any directions in such terms would enable applicability based on functionality. So the directions would apply to direct and indirect payment schemes participants. It could also capture third parties such as payment initiation service providers; but this would need to be as and when the service is extended to cover them in line with Pay.UK's phased approach.
- 2.2 Consideration could be given to exempting PSPs in some circumstances. For example, where their FPS and / or CHAPS payments volumes and / or values fall below a defined threshold

and are projected by the PSP to continue to do so. This would ensure that PSPs that undertake FPS and CHAPS payments on an exceptions basis only are not affected disproportionately by any direction. Another suggestion is to exempt PSPs that only enable first party payments. That is, where funds can only be returned to the account they were sent from.

3. **SHOULD THE SAME PSPS BE SUBJECT TO A REQUIREMENT TO RESPOND TO A COP REQUEST AS THOSE THAT ARE REQUIRED TO SEND A REQUEST?**

3.1 In LBG's view, the criteria for application of the requirements should be based on whether PSPs send or receive FPS and CHAPS payments, as outlined in our response to question two.

4. **DO YOU THINK THAT WE SHOULD CONSIDER GIVING DIRECTIONS IN RELATION BOTH TO FPS AND CHAPS TRANSACTIONS? IF YOU BELIEVE THAT WE SHOULD CONSIDER GIVING DIRECTIONS IN RELATION TO ONLY ONE OF THESE PAYMENT SYSTEMS, OR MORE THAN FPS AND CHAPS, PLEASE SET OUT WHY. ARE THERE ANY OTHER ISSUES THAT WE SHOULD CONSIDER WHEN DECIDING WHICH PAYMENT SYSTEMS SHOULD BE IN SCOPE?**

4.1 LBG supports in principle any directions applying to both FPS and CHAPS. However, we have identified that sending requests via CHAPS is likely to present a wider range of technical challenges compared with sending requests via FPS. CHAPS requests are lower volume and are likely to require workaround solutions for some channels.

5. **SHOULD THE DIRECTIONS APPLY TO ALL PAYMENT CHANNELS THAT AN FPS OR CHAPS PAYMENT CAN BE INITIATED FROM? SHOULD A COP REQUEST ONLY APPLY WHEN A NEW PAYMENT MANDATE IS BEING SET UP OR CHANGED?**

5.1 LBG believes consideration should be given to applying any directions to digital channels only – at least in the first instance. That is, the directions should apply to payments that are sent via online banking and mobile devices. Applying any directions to digital channels will capture the majority of payments that are the product of APP scams or are accidentally misdirected. In our view, for many PSPs there will be an aspiration to embed CoP across all channels, but this could require a staggered timeline.

5.2 Alongside CoP, we suggest further consideration is also given to mandating the CRM. Mandating the CRM would provide protection for customers that are victims of APP scams that are carried out via non-digital channels. That is, PSPs would be liable for refunding losses incurred by customers that are victims of APP fraud where CoP was not available. It would then be for each PSP to determine the costs and benefits of implementing CoP across all or some of its channels when compared with the costs of refunding customers in line

with the provisions in the CRM. We recognise that mandating the CRM might not be straightforward and we are keen to assist with resolving this.

- 5.3 In addition, we note that the involvement of PSP staff in payment transactions via non-digital channels, where they are trained to recognise APP scams, is likely to provide some extra protection for customers when compared to payments sent via digital channels.
- 5.4 Lastly, we recommend that CoP should only apply when a new payment mandate is being set up or changed – this is where CoP will add the most value to the payments journey. Applying CoP to existing payment mandates is likely to introduce unnecessary friction into the customer payments journey. For example, an existing payee mandate set up using a nickname or other reference would not produce a match. The friction that would arise when a payment is made to an existing payee could cause customers to distrust the value that CoP will bring when payment mandates are set up or changed.

## 6. **HOW SHOULD ANY DIRECTIONS DEAL WITH THE POTENTIAL FOR PEOPLE TO OPT OUT OF THE COP PROCESS?**

- 6.1 In order to ensure that the coverage of CoP can be as wide as possible, enhancing its effectiveness and benefit to both payers and payees, LBG believes that an opt-out should only be available to payees in a limited range of cases where that customer's circumstances fall within the scope of pre-defined set of criteria developed by each PSP. Criteria should be set in accordance with the general law and appropriate Pay.UK guidelines. In view of this, LBG does not currently feel that there would be any particular requirement for directions to be put in place specifically to deal with how customers can opt out.

## 7. **SHOULD ANY DIRECTIONS COVER THE SENDING OF MONEY FROM BOTH INDIVIDUAL AND BUSINESS ACCOUNTS?**

- 7.1 LBG recommends that any directions cover the sending of money from both individual and small business accounts – at least in the first instance. In respect of larger corporate customers, consideration should be given to Pay.UK's planned exemption of bulk files. We also suggest that, for these customers, CoP should be optional and be able to be offered on a commercial basis.

## 8. **SHOULD THE DIRECTIONS SEPARATE OUT RESPONDING TO COP REQUESTS FROM BEING ABLE TO SEND COP REQUESTS? SHOULD DIRECTIONS COVER BOTH SENDING AND RESPONDING?**

- 8.1 LBG agrees that any directions should separate out responding to CoP requests from being able to send CoP requests.
- 8.2 As noted in our response to question one, our view is that responding to CoP requests is vital in order to achieve the necessary network effect. In the light of this, we support the proposal to mandate receiving CoP requests.

- 8.3 We do not support the PSR giving a direction in relation to sending because we do not believe it will be an effective approach to driving high quality implementation of sending capabilities across the industry.
- 8.4 We recommend that the PSR allows PSPs to set their own delivery timelines. This will enable PSPs to make use of agile methodology – that is, continuous design improvement and testing based on rapid feedback and change. It will also enable PSPs to approach sending CoP requests as a propositional differentiator – potentially combining CoP with other innovative solutions that will help reduce APP fraud and accidentally misdirected payments.
9. **DO YOU AGREE WITH THE DEADLINES FOR THE INTRODUCTION OF COP? IF YOU DO NOT AGREE, PLEASE SET OUT WHY YOU CONSIDER DIFFERENT DATES WOULD BE MORE APPROPRIATE AND YOUR VIEW OF THE IMPACT THAT WOULD HAVE ON THE COSTS AND BENEFITS OF COP. IF THE DATES ARE NOT CONSIDERED ACHIEVABLE, PLEASE GIVE REASONS AND ALTERNATIVE DATES THAT YOU CONSIDER ACHIEVABLE AND THE REASONS WHY.**
- 9.1 LBG is supportive of the need for urgency in implementing CoP. However, we are concerned that the proposed deadlines are not achievable for the industry – particularly in relation to sending requests. We suggest the following factors are taken into consideration when determining any deadlines. As noted, we are not supportive of a direction that mandates sending requests, but if the PSR is minded to do this then we suggest that the following factors are taken into consideration when determining deadlines.
- 9.2 We believe there is a trade-off between implementing at speed and ensuring a robust, effective service that delivers in line with customer expectations. From a technical perspective, we are aiming to meet the proposed deadline of April 2019 for receiving requests for most customer accounts. We are aiming to meet the proposed deadline of July 2019 for sending requests for most FPS and CHAPS payments via digital channels for retail and small business customers across our core brands. However, we have identified issues around scalability, and there are a number of design issues outstanding (for example, in relation to opt-outs).
- 9.3 We are concerned that in meeting the proposed deadlines there is a significant risk that we do not meet the PSR’s goal of delivering a robust and user-friendly service – both for our customers and those of other PSPs. In turn, given the network effect, other PSPs might not be able to deliver an effective service for our customers. In order to implement CoP, there are various common rules and guidelines that each PSP must align with. These are produced by Pay.UK, and some elements require further consideration. The Pay.UK rules and guidelines must be ready and available to all PSPs to enable the necessary systems testing and development.
- 9.4 We are also concerned that deadlines of April and July 2019 are unlikely to provide enough time to undertake adequate test and learn programmes. Again, particularly in relation to sending requests, which presents the widest range of technical challenges. We note that CoP implementation relies on application programming interface (API) technology, which has not previously been used at this scale within the UK banking industry.
- 9.5 Launching a CoP service for all retail and small business customers that has not been fully tested risks failing to live up to customers’ expectations, causing misunderstandings and potentially resulting in a long term lack of trust and buy-in to the concept. For example, if matching rates have not reached an acceptable level, this could lead to customers contacting their PSP for advice ahead of sending a payment to a new payee. Some

customers that are particularly risk averse might in some circumstances feel they cannot proceed with a payment even when they have not been told conclusively that the names do not match.

- 9.6 In respect of smaller PSPs, we understand many plan to buy in CoP services from external vendors instead of developing their own in house. To date we understand that no third party vendors have yet launched a CoP product. Therefore we expect that smaller PSPs that intend to buy in CoP services will find the proposed deadlines particularly challenging.
- 9.7 In addition to the technical considerations, there is a significant risk that, by aligning to these deadlines, it will be more challenging for PSPs to implement effective customer awareness and education campaigns. That is, campaigns that prepare customers for CoP as well as the other initiatives in this area such as CRM and strong customer authentication.
- 9.8 A further consideration is that the proposed deadlines would make it more challenging for PSPs to address any necessary updates to customer terms and conditions in the clearest and most efficient manner way. We note there is a requirement to provide 60 days' notice of account changes of this type.

#### *Alternative approaches to setting deadlines*

- 9.9 There are various approaches that could be taken to setting deadlines, and given the many variables we do not have one preferred deadline or set of deadlines. Consideration could be given to staggered deadlines for implementing CoP based on functionality. For example, we understand that the Netherlands undertook a phased approach over two years, with their equivalent of CoP beginning with the service generating a message only if the payee's name was not a match with the keyed in name. Generating additional messages (for example stating whether there was a match or close match) was delivered over later releases.
- 9.10 Staggered deadlines for sending CoP requests could also prioritise retail and small business customers and digital channels ahead of a wider roll out. We also suggest that consideration is given to examining the read across from CoP to other initiatives, including CRM and strong customer authentication, and developing timelines that take account of all of these.

Finally, staggered deadlines for sending requests could apply to PSPs depending on their FPS and CHAPS payments volumes and values. Shorter deadlines could apply to PSPs that process high volumes and values, with longer deadlines applying to PSPs that process lower volumes and values. We note though the risk that longer deadlines for smaller PSPs could have the effect of diverting APP scams to smaller PSPs, which would need further consideration.

## **10. ARE THERE ANY ALTERNATIVE APPROACHES THAT WE SHOULD CONSIDER INSTEAD OF GIVING DIRECTIONS TO PSPS AS SET OUT IN THIS DOCUMENT?**

- 10.1 LBG notes that, as set out in in our response to question one, consideration should be given to how CoP interacts with other relevant initiatives.
- 10.2 We also consider there is a role for coordination to ensure orderly CoP implementation, and ensure there is read across to other relevant initiatives such as CRM and strong customer authentication.
- 10.3 More widely, we believe that, where there is a network effect, as there is in relation to responding to CoP requests, mandating via the payments schemes – such as providing a

direction to FPS and CHAPS – could be the most effective means of securing robust and timely implementation. In the absence of a central solution, coordination to assist PSP compliance with any direction deadline would be helpful.

**11. IS OUR ASSESSMENT OF THE BENEFITS THE RIGHT ONE? IF YOU DO NOT AGREE, PLEASE SET OUT WHAT YOU CONSIDER WOULD BE MORE APPROPRIATE AND YOUR VIEW OF THE IMPACT THAT WOULD HAVE.**

11.1 LBG agrees strongly with the PSR that CoP is the right thing to implement and will deliver benefits when it is implemented effectively – particularly in relation to reducing some types of APP scams and accidentally misdirected payments.

11.2 We also agree that CoP will deliver benefits that are difficult to quantify, such as in relation to improved trust in electronic payment systems and an improved customer experience. It is also possible that the number of false positives generated via existing fraud prevention strategies will decrease, reducing inconvenience to customers. However, the delivery of these benefits is dependent on high quality implementation.

11.3 We believe the benefits of reducing APP scams are likely to have been over-estimated given the likelihood that perpetrators of some scams will adapt their approaches to take account of CoP. We expect this to play out in two key ways. Firstly, perpetrators that utilise social engineering techniques to commit APP fraud are likely to adapt their techniques so that customers do not register the implications of a mismatched CoP result. Secondly, where types of APP fraud are limited by the implementation of CoP, we expect perpetrators to devise alternative approaches to acquire customer funds.

**12. IS OUR ASSESSMENT OF THE COSTS THE RIGHT ONE? IF YOU DO NOT AGREE, PLEASE SET OUT WHAT YOU CONSIDER WOULD BE MORE APPROPRIATE AND YOUR VIEW OF THE IMPACT THAT WOULD HAVE.**

12.1 LBG believes that the costs are likely to have been underestimated. Some types of costs are missing from the assessment, such as the cost of reissuing customer terms and conditions specifically for CoP where a reissue has not already been scheduled. We have provided some cost estimates in our response to the PSR's s.81 request that relates to CoP costs.

12.2 The costs are also likely to be higher if CoP is not implemented effectively. For example, the costs of providing customer support, as well as less tangible costs relating to lack of take-up and reputational impact.

**13. IS OUR ASSESSMENT OF THE TRADE-OFF BETWEEN COSTS AND BENEFITS THE RIGHT ONE? IF YOU DO NOT AGREE, PLEASE SET OUT WHAT YOU CONSIDER WOULD BE MORE APPROPRIATE AND YOUR VIEW OF THE IMPACT THAT WOULD HAVE.**

13.1 LBG considers that the benefits of CoP in preventing APP fraud have been overstated, therefore we believe the net benefits are likely to be lower than the estimates. We are not though in a position to expand on this.

14. **WHAT IS YOUR VIEW ON THE IMPACT OF THE PROPOSED DATES IN OUR APPROACH TO THE TRADE-OFF BETWEEN COSTS AND BENEFITS. DO YOU CONSIDER THAT IMPOSING APRIL AND JULY DEADLINES IMPACTS EITHER THE COSTS OR BENEFITS OF IMPLEMENTING COP RELATIVE TO A LATER IMPLEMENTATION DATE – FOR EXAMPLE, 2020 OR LATER?**

14.1 LBG believes the impact of the proposed dates is likely to be different than that envisaged by the PSR. The comparison between implementation in 2019 and 2020 or later appears to be based on an assumption that there are no barriers to high quality implementation across the industry in 2019. Given the concerns we have identified and set out in our response to question nine, we believe the benefits of a 2019 date are likely to have been overestimated.

15. **DO YOU HAVE ANY COMMENTS ON OUR ASSESSMENT OF THE IMPACTS OF THE DIRECTIONS WE ARE CONSIDERING ON PROTECTED GROUPS OR VULNERABLE CONSUMERS? DO YOU HAVE ANY EVIDENCE THAT WILL ASSIST THE PSR IN CONSIDERING EQUALITY ISSUES, AND IN PARTICULAR COMPLYING WITH ITS PUBLIC EQUALITY DUTY, IN DECIDING WHETHER TO GIVE DIRECTIONS AND CONSIDERING ALTERNATIVES?**

15.1 LBG agrees with the PSR's assessment on the impacts of the potential directions on protected groups and customers in vulnerable circumstances and that, overall, the service will have a positive impact. We have supported Pay.UK's engagement with consumer groups and independent research when developing the rules, standards and guidance for CoP. We look forward to continuing this engagement to ensure the needs of these protected and vulnerable groups are met when implementing the CoP solution.

# Member of the public

**To:** [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)  
**Subject:** Consumer feedback to "Confirmation of Payee" consultation.

---

I wished to feed back on the above consultation as a consumer.

The proposals do not suggest that there will be an absolute categorical block on a payment being able to be made if the name details on the recipient account do not come close to matching the actual name on the account. It seems that a user can override any match failure and still make the payment anyway.

This action should not be allowed as the social engineering skills of fraudsters will adapt to trick vulnerable people into making the payment anyway with all kinds of excuses as to why the name doesn't match, at which point they will still have no right to redress and recompense for the loss from their bank - rendering this whole exercise a waste of time. This will invite cynicism as to the banking sector's reasons to avoiding making compensation payments, rather than a genuine desire to all but eliminate push payment fraud from the banking system by adopting the tightest constraints - which they could have done if so agreed by / instructed by the Payment Systems Regulator.

The payment should be totally blocked if the name doesn't come close to matching, with the stated outcome that the payee must go back to the recipient to obtain their account's exact name for the payment to be successfully made again at a future time.

This will almost certainly cause a sizeable number of rejected payments initially as people get used to this new system, but the number of failures could be reduced if there is widespread and simple to understand bespoke messaging communicated directly to all account holders by their bank. This should be by means of a personalised posted letter stating in their account's specific case what name they have to tell payees to use in the future - much like the advice given to customers when their IBAN was changed when many banks separated their retail and investment banking divisions last year. This notification could be accompanied by timely TV, radio, print and online advertising paid for by the banking industry members as a whole in proportion to their size - like the FCA has taken out widespread advertising when it comes to generating awareness of next year's PPI claim submission deadline.

It won't take long for such a tightly controlled system to settle down, but the benefits to society would be well worth the short term inconvenience for some account holders who did not get or understand the message of what they need to do to make a payment from whenever the new system starts.

[I have not now or ever worked in the banking sector, have not now or ever worked in consumer affairs, and have never been defrauded by push payment fraud - I just wish the views of a consumer who this change is meant to benefit be heard in the development process.]



# National Trading Standards (NTS)

Chairman: Lord Harris  
National Trading Standards  
Sylvan Court  
Sylvan Way  
Southfields Business Park  
Basildon  
Essex  
SS 15 6TH



Email contact via  
nationaltradingstandards@actso.org.uk

APP Scams Policy Team  
Payment Systems Regulator  
12 Endeavour Square  
Stratford  
London  
E20 1JN

(sent by email)

14 December 2018

Dear Sir/Madam,

### **Consultation on general directions for the implementation of Confirmation of Payee**

Thank you for the opportunity to respond to the PSR consultation on Confirmation of Payee. I am writing on behalf of National Trading Standards (NTS). I know that colleagues in the NTS Scams Team, Louise Baxter and Melissa Dring, have been engaging closely with you on this through the work of the APP Scams Steering Group, and we wanted to submit a formal NTS response.

We believe that Confirmation of Payee is one of a number of tools that the banks can and should introduce to help prevent APP fraud. As you are aware, fraud is now recognised as the most prevalent crime in the UK and criminals are developing ever more sophisticated techniques to steal people's savings. Although financial institutions make a distinction between fraud (denoting unauthorised transactions) and scams (authorised transactions), NTS believes that the division made by financial institutions between fraud and scams is an artificial one that is incomprehensible to victims. Further we believe that distinguishing between fraud and scams has allowed 'scams' to be viewed as less serious, downplaying the impact on victims and resulting in weaker public and private action to prevent and tackle them. Our policy is that **Scams are Fraud and Fraud is a Crime**. Accordingly, the terms fraud and scams are used interchangeably in this response.

The National Trading Standards (NTS) Scams Team focuses on mail, telephone and doorstep fraud. Our data shows that the average victim is 75 and often lives alone. Victims lose an average of £1,000, but older victims suffer more, losing £5,000 on average, not to mention the impact on physical and mental health. We have examples of victims who have lost their life savings, their houses, and their independence. The evidence suggests that victims of scams are twice as likely to go into a care home or die in the two years following the crime compared to their non-victim peers.

NTS therefore welcomes the rising awareness of authorised push payment scams and understanding of the impact on victims among financial institutions. Confirmation of Payee (CoP) could help prevent some of

these frauds by alerting potential victims that the account they have been instructed to send money to does not belong to the person they expect. NTS supports the use of general directions by the PSR to enforce a timely introduction of CoP across all financial institutions. The design of CoP means that it needs to have uniform and widespread take up to be effective and enforcement by the regulator seems to be the best option for this given the current delays in implementation.

Moreover, public understanding of this process is limited. Many customers believe that the banks already cross-check account names and are surprised to find that this is not the case. Given the press attention around the introduction of CoP, there is already confusion around timelines for its implementation and some customers may believe that it is already in place. This may put them at greater risk of scams since they believe that this layer of protection is already in operation.

Finally, CoP is a key component of the contingent reimbursement model being developed by the APP Scams Steering Group. For the voluntary code to function properly, it is important that take up of CoP is widespread across financial institutions so that they can meet their obligations as sending and receiving banks. These are all reasons to support the adoption of CoP as soon as possible across the industry. NTS is disappointed that progress to date has been slow, and while we understand that changes to bank systems and technologies take time, technical solutions now exist and need to be implemented as soon as possible to protect customers.

On the details of the general directions, NTS believes these should cover as many PSPs and payment types as possible and we support the PSR proposal for it to cover FPS and CHAPS initially. We cannot envisage a disadvantage of applying it to all transactions to ensure payments details have not changed in between transactions, although a risk-based system where CoP was only used on changed or new payment details would also be acceptable as long as this is communicated properly to customers and they understand which payments are checked.

Both business and personal accounts should be included in the general directions, otherwise there will be little value in preventing scams as criminals will use whichever account type is not covered to move money. We are not sure why individuals or businesses should be able to opt-out and are concerned about this being used by criminals to prevent potential victims from checking that payment details match what they have been told. The misuse of CoP to find out account names should be minimal if the system is well designed to prevent this. We would suggest that while an opt-out may be appropriate for individuals in exceptional cases it is unlikely to be appropriate for businesses. We support the deadlines set out in the consultation and the intention to introduce CoP as soon as possible. The general direction should not prevent PSPs from implementing CoP earlier if they are able to do so.

NTS therefore supports the use of general directions by the PSR to enforce the implementation of CoP. This measure will prevent accidentally misdirected payments where customers enter the wrong details for an intended payee and will also prevent some of the more unsophisticated APP scams where a customer is tricked into changing payee details so that their payment goes to a criminal instead of a genuine payee. However, the PSR should not overestimate the effectiveness of CoP in preventing APP fraud. In many cases these scams involve sophisticated social engineering where the victim is tricked into trusting the criminal completely. As such it is likely that in many cases the victim could be persuaded that there was a reason for sending money to an account in a different name than the one they would expect or coached to ignore the CoP check altogether. It is well known that criminals practising fraud change their methods quickly to keep ahead of the latest developments in prevention, and as such we should expect that criminals will find ways to work around the restrictions of CoP. However, it will make the payment environment more hostile to criminals and increase the difficulty of defrauding victims and should be adopted as soon as possible.

Finally, we would like to suggest that if general directions are used to hasten the implementation of CoP, then the PSR should also consider using general directions to enforce take up of some or all aspects of the contingent reimbursement model for APP scams. Like CoP, the voluntary code will be most effective if it is adopted by the majority of PSPs in a consistent manner. Since the code aims to raise standards in prevention and detection of fraud across the industry, it is likely to do more to reduce harm from APP fraud in the long term and will have a larger impact on victims by ensuring they are reimbursed where they could not have prevented the fraud.

[REDACTED]

[REDACTED]

[REDACTED]

# National Westminster Bank PLC

## **CP 18/4**

# **Consultation on general directions on implementing Confirmation of Payee**

## **National Westminster Bank plc response**

**January 2019**

## Introduction

NatWest<sup>1</sup> fully supports the introduction of Confirmation of Payee (CoP) and agrees this will support the objective of providing further protection for customers from fraudulent activity.

We also consider it essential for there to be a consistent adoption of CoP by Account Servicing PSPs in a defined but achievable time period. Industry is working closely with Pay.UK to encourage it to take on the role to facilitate the creation of this 'network' effect, essential for a solution such as CoP which is intended to become an integrated part of the customer payment journey. This is currently not agreed and our view is that, if this were not to change, industry would need to consider how this might be resolved to ensure an effective launch of the new service.

As the first of the overlay services which Pay.UK is leading, its model to encourage competitive industry delivery by supporting development of the rules and standards has been welcomed. However, the CoP support materials have only now reached the stage where industry and technical providers can begin fully to develop their compliant and robust solutions with any certainty. This will take time, as will solution testing at scale, combined with individual PSP activity to achieve mass adoption and use for CoP's formal go-live date.

A key aspect of CoP that will require sufficient time for testing and potentially adaptation before CoP is introduced, are the name matching algorithms. These must be robust before live running, to ensure that customers continue to enjoy integrated and easy to use payment journeys.

An ancillary issue is the overlap between CoP requirements and elements of the Contingent Reimbursement Model (CRM) Code, also to be introduced in 2019, and greater clarity is required for PSPs on aspects such as liability and phasing. It will be important for this to happen before CoP is live. PSR should also be aware of the additional activity PSPs will have, to adhere to the CRM code standards and potentially to adapt procedures to support complaints to the FOS against them as a receiving PSP by a paying customer.

The specific CoP development and delivery issues pale into insignificance however against industry's full and complex mandatory change delivery programme for 2019, spanning Brexit, Open Banking and PSD2/RTS SCA. This is stretching resource capability across payments, technical and project specialisms and risks sub-optimal delivery and potential unintended consequences.

Regulatory focus on PSPs, both from European and UK regulators on the importance of Information and Communication Technology (ICT) risks and operational resilience has considerably increased in 2018 and NatWest is very conscious of its obligations in this regard.

We would urge the PSR when considering this and other PSP /industry responses to recognise these factors and consult with other parties before making its decision on CoP.

## Why are we consulting on directions?

---

<sup>1</sup> NatWest means National Westminster Bank plc responding for itself and its affiliates and subsidiaries. These cover The Royal Bank of Scotland plc, Coutts and Company and Ulster Bank Limited. In addition this response covers London and Gibraltar branch customers of The Royal Bank of Scotland International Limited in scope for CoP.

**Question 1 - Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

We understand the PSR's rationale for proposing to mandate participants to develop the capability to receive and respond to CoP requests, as this could help to support a reduction in certain APP scam fraud types impacting consumers (as defined in the CRM Code), and remove many accidental payment errors. However we believe the introduction of the CRM Code already incentivises PSPs to introduce a capability to send CoP requests at the earliest date they can to support their customers.

That said, we acknowledge that such an incentive may not lead to a well-phased, at scale roll out of the new service, leading potentially to a patchy and non-uniform service for customers, and the potential displacement of fraud to those PSPs not yet ready to offer the service. It may also see further targeting of mule account recruitment, where accounts operate as genuine accounts, until they are exploited for criminal purposes.

Our conclusion is therefore that any direction given must be proportionate in the PSPs it applies to and also recognise the emerging industry's proposed phased introduction of CoP. This is focussed on customers in scope of the CRM code, the digital channels via which the majority of APP scams are perpetrated and where CoP can play a part in their prevention, and the most impacted payment type used by consumers i.e. Faster Payments.

The use of CHAPS by consumers for payments is limited and often made as a bank-assisted payment. In addition, the Faster Payments transaction limit is expected to increase further in 2019, to a level where it will make it increasingly unlikely that CHAPS payments will be used for retail payments. This could potentially support holding back from giving a direction to CHAPS participants. This must be set against the often higher amounts of maliciously misdirected CHAPS payments, where the monetary loss may have a greater detriment.

We are aware too that during 2019, the FOS will take into account the adoption by PSPs of the CRM Code standards, and where these are not implemented, may require the PSP to contribute to any resultant loss by the customer. Our view is that for a technical industry delivery, it would be disproportionate if the FOS were to find a PSP at fault for not delivering CoP where it was unable to do so, and particularly before an agreed industry date to have done so.

We would add - and here we speak both for NatWest and include the views of our indirect PSPs - that industry already has a full and complex mandatory change delivery programme. This is creating overload on both payments and technical resource within PSPs and thus across industry as a whole. This is particularly onerous for smaller PSPs for example, with fewer resources, not operating with a unique sort code, and also less likely to be involved in Open Banking. [REDACTED]

We also note HM Treasury's recent acknowledgement of the significant changes occurring in the payments sector, which are limiting business capacity for implementation in the short to medium-term. We are aware of concerns too in Open Banking of their ability to support CoP API delivery in the timescale proposed.

Once PSR has considered PSP responses to this consultation, we strongly suggest that before making its decision on whether to take action, it engages with other regulators to ensure an

holistic view of the regulatory demands on industry. This may inform the setting of realistic and achievable implementation guidelines for CoP. For avoidance of any doubt, we do not believe that deliveries in April (respond to other PSPs) and July (deal with responses from other PSPs) are achievable. If this leads to mandatory directions on PSPs, then we believe that these will need to be proportionately applied.

## **The proposed scope of the directions**

### **Question 2 Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

Ideally, regardless of whether directions are given, all types of PSP should ideally be able to respond to a CoP request. Otherwise our expectation is that fraudsters will exploit this gap and open more accounts with non-participating PSPs. Recent articles have noted that pre-paid card accounts are increasingly being used by fraudsters, because of the ease with which they can be obtained.

We are aware that it will potentially be more onerous for smaller PSPs with for example, fewer resources, operating without a unique sort code, not an ASPSP, and less likely to be involved in Open Banking, to be able to comply with a CoP direction as easily as direct or directly connected PSPs, or perhaps larger agency PSPs.

To offset this, the emerging vendor market may be able to develop and support a multi-user CoP service, or larger PSPs to consider how they might support their indirect PSPs on a commercial basis. Additional development time to achieve this would need to be considered in any timescales for implementation directions, particularly as larger PSPs will need to prioritise their own compliance over the development of additional commercial services.

Our conclusion is that any direction should not be made mandatory for indirect Participants to offer CoP to their customers wishing to make payments in the same timescale as for direct and/or Open Banking enabled PSPs. We are aware that many indirect PSPs, with full online account services, consider that they need to provide a CoP service, to protect their customers and to mitigate fraud.

### **Question 3 - Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

Being capable of responding to a CoP request is the most critical element of the CoP service and the most challenging aspect of technical delivery for the receiving PSP.

Unless commercial solutions emerge that provide an outsourced CoP decisioning and responding service, a direction is likely to disproportionately impact some smaller PSPs.

As outlined above, we believe the PSR needs to consider this carefully.

### **Question 4 - Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

Whilst of the view that directions may not be essential, given the CRM code incentivises PSPs to introduce CoP, we believe there should be the same treatment of both FPS and CHAPS.

We acknowledge that although fewer payments pass through the CHAPS system, the values of these payments are considerably higher, including when made by consumers. We also believe that without it, there may be a migration of fraud to the CHAPS system.

**Question 5 - Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

As the PSR will be aware from other industry sources, the vast majority of electronic inter-bank payments are now made digitally, by both personal and all types of business customer.

As above, industry, including NatWest, is considering a phased approach by customer type, the most affected channel and the payment type most used by those customers.

[REDACTED] The losses for non-personal customers – are fewer in number but on average of considerably higher value and as such, we want again to mitigate potential fraud migration.

We continue to offer assisted payments to customers in branch and through our telephony channels. Their volumes continue to fall and fraud attempts, because of the person to person interaction, are much lower. We would therefore urge PSR not to extend any direction scope to these channels and to permit PSPs to consider reviewing how best to support customers making payments this way, in line with improved communication and where appropriate, warning messages.

On when a CoP request is applied, we agree that it should be when a new payment mandate is being set up or changed. We also believe that PSPs may want to check customer payment mandates not used say for 6/12 months, when the customer comes to make a further payment. We anticipate this frequency gap being set according to the PSP's risk appetite as opposed to a fixed 'rule'. The re-check may in time become an integrated part of digital payment services, allowing customers to be more in control.

**Question 6 - How should any directions deal with the potential for people to opt out of the CoP process?**

In our view, whilst we expect from wider publicity and our own customer communications that CoP will be a well-subscribed service, there will remain people who for identity protection need to opt out to protect their identity. This will need consistent management by PSPs to agree criteria aligned to identity protections.

Where an account cannot be reached for a legitimate personal protection reason, we do not believe that the customer, or their account providing PSP, should be liable under the CRM code standards.

How this can be managed under any direction, if our view is supported by other PSPs, will need to be considered by PSR, but a confirmed exemption from the direction (and a parallel

condition in the CRM code standards to support this) seem potential ways to deal with this situation.

Industry as whole supports limited opt-out of accounts for CoP checks for customers where a higher level of support is required. Given the nature of CoP, we believe all PSPs must make clear the benefits of the service and why opting out can only be considered if protection is required. This will require a reasonably uniform industry approach to be adopted and we would hope that UK Finance and other trade bodies may be able to co-ordinate industry activity here.

[REDACTED]

For business customers, short term opt-out may be needed for certain types of account where the convention is not to pay the account holder but the person or business for which the money is due. These include:

- businesses which provide undisclosed invoice discounting where the organisation using their service is provided with an account to which the funds are paid;
- solicitor and accountants that offer 're' accounts for named clients for transactions such as property purchase, trusts or acting as an insolvency practitioner; and
- businesses where the trading name is more familiar to the end user than the formal company name

In all the above instances, name matching solutions have not as yet been tested, and there are potentially other naming conventions where an absence of testing might lead to overly high no-match levels, causing end user detriment.

### **Question 7 - Should any directions cover the sending of money from both individual and business accounts?**

If directions are given, we believe it is important that their early focus is on consumers as defined in the CRM code, where such end users also use consumer channels to make their payments.

[REDACTED]

We support the delivery of CoP to business customers, but as PSR will be aware, the majority of business payments are made using Bacs, via bulk submission. How a business will make CoP requests alongside Bacs direct submissions is still to be considered by industry, in engagement with business users. As such we do not believe that business accounts should be covered by an early direction, except possibly for payments that are single and attended i.e. not bulk submission.

### **The rationale for our timeframe**

### **Question 8 - Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

Having a direction to respond to CoP requests, and with a date set, by which a good number of PSPs in its scope are able to provide a response, will assist achieving better service penetration.

We do not believe that there is as strong a case for giving directions on sending payments, as PSPs are already incentivised to offer this through the introduction of the CRM code.

In our view, it should also be possible, subject to there being a critical mass of PSPs able to receive and respond to CoP requests, for perhaps smaller volume or non ASPSPs to send requests to CoP-ready participants to protect their customers against scams. This will allow earlier benefits to be achieved.

**Question 9 - Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

NatWest does not agree with the proposed PSR dates for the implementation of CoP either to receive requests or to respond to them.

Our reasons on April 2019 being an unrealistic timescale to receive CoP requests are set out below and are also referred to in our answers above:

1. Need for PSPs and vendors to develop technical name matching capability that allows sufficiently high levels of realistic name matching that causes friction to a new payment only where necessary. Vendors have until recently received only limited information on CoP, but will under new arrangements agreed with Pay.UK be able to receive full CoP documentation in early 2019. The industry solution implemented in the Netherlands included an extended testing period to ensure this. We understand from other potential vendors that they would also recommend this, given the wide range of UK name types. In addition, names input by customers on existing payments refer not to the name of the person to be paid but e.g. to a family relationship such as Dad or the purpose, say, Pet Insurance. This will require customer education to help improve name input to overcome future matching errors.
2. Need to ensure critical mass of PSPs capable of both sending and receiving at the start, with others to come online progressively after them, to ensure confidence in the early service and little opportunity for fraud to migrate from PSP to PSP.
3. Wider busy regulatory programme deliverables already scheduled for that time, which include: Open Banking, PSD2 dedicated API interface / exemption from screen scraping, PSD secure customer authentication, the industry change freeze in case of a hard Brexit either side of the 29th March as well as [REDACTED]

We believe the date for receiving and responding to requests can only be agreed once industry is clearer on what is possible. Our expectation, given current state of overall preparedness, and the current absence of a plan for industry co-ordination, is that Q4/2019 is the earliest feasible date by which adequate mass capability is likely to be achieved, with early phase roll-out running to perhaps mid-2020.

On send capability, this is for each individual PSP to determine based on development and regulatory activity. [REDACTED]

**Alternative approaches**

**Question 10 - Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

We believe that there are some benefits to giving directions on an ability to respond to requests, but for sending payments are of the view that there are sufficient competitive and industry pressures without the need for reinforcement via directions.

The emerging alternative is the combination of the CRM code incentives and the separate FCA action to allow complaints to the FOS against the receiving bank both for APP scams, and under PSD2 obligations for accidental misdirected payments. This should drive more consistent behaviour by receiving PSPs to support payment recovery.

**Cost Benefit Analysis**

**Question 11 - Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

We agree with the financial benefit assumptions on the amount of CoP mitigated APP scam losses. As indicated above, we do not believe that PSPs, irrespective of whether a direction is set, are capable of delivering CoP to a timescale that will support these levels of mitigation.

Additionally, our view is that there will be fewer losses attributable to accidentally misdirected payments, covering payments sent to the wrong account or wrong payee. [REDACTED] of all our customer misdirected payments are to an incorrect account/ sort code. If other PSPs' customer errors of this type are at a similar level, this could drive considerable customer benefit.

In summary, more benefits may be achieved, and in the abstract, if delivery to PSR's predicated timescale were possible, this might achieve the 2019 net benefit stated. We do however fundamentally disagree with the feasibility of industry 2019 delivery being sufficiently broad to be capable of achieving such net benefits.

To comment on the Assumption variables used in Table 2, our current view tends towards higher annual APP scam growth than 5%, given the existing trend is higher. We also believe that the prevention rate from CoP alone will not be this high, unless PSR's assumption factors in the likely higher prevention of accidentally misdirected payment errors. Without more consistent adoption by the wider PSP community of improvement measures, prevention rates will not we believe increase to the level assumed.

**Question 12 - Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

As PSR is aware, NatWest provided its indicative delivery costs, as then known. These were at [REDACTED]

On customer education, this is included in our internal budget, but we may also be asked to contribute to potential industry communications. We expect customer education to be ongoing rather than a single year expense e.g. reminders for existing customers and a CoP introduction for new customers as part of online set up.

On annual running costs, we do not expect these to be high and thus the £20m figure seems reasonable as an indicative industry cost, together with the separate spend assumption on customer awareness communication.

**Question 13 - Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

While we believe that an extended implementation may increase total industry costs/reduce benefits achieved, we agree a net benefit will remain from a reduction (if not complete elimination) of APP scams and misdirected payments. This is particularly so for APP scams which will be supported by other industry initiatives.

While casual fraudsters may be deterred, industry will need to remain on alert to the threat of increased serious and organised crime activity which seeks to circumvent CoP controls in more creative ways. Social engineering in particular may be enhanced to convince end users to authorise payments.

**Question 14 - What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits? Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

Our costs of delivery are based on delivering to a timescale we can achieve, and on phasing delivery with other regulatory and internal developments. To deliver to PSR's proposed dates is not feasible for us, for reasons stated earlier; nor we believe for many other PSPs. In this sense, both cost and benefits will be deferred. However, the wider CRM code standards can be implemented, including online messages and warnings, so benefits may still be achieved.

If CoP implementation were left until say early 2020, costs are unlikely to change except for inflation based increases, but implementation could be expected to include more PSPs and bed in more smoothly for more customer types following longer testing.

As such, benefits, although deferred, would quickly be achieved and thus lead to a minimal difference. This would particularly be so if the wider CRM standard improvement by PSPs and greater customer awareness are achieved.

## **Equality Impact Assessment**

**Question 15 - Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

We agree with PSR'S paragraph 8.3 which states that there is potential for CoP to 'present a greater risk of poor outcomes to some consumers with protected characteristics'. We also consider that PSPs should consider how to minimise additional friction for all customers from the introduction by CoP.

We are aware from industry-sponsored customer research, in connection with the mitigation of accidentally misdirected payments, that cognitive load e.g. too much information and intrusive messages can affect all customers when setting up a payment. This impact is potentially greater on customers with certain characteristics.

Where a close or a negative match response is received, this may result in certain customers aborting their electronic payment and transitioning to a more familiar physical payment.

----- end of response -----

# Nationwide Building Society

## Consultation on General Directions on implementing Confirmation of Payee: Nationwide Building Society Response

Q1 Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?

We see enabling a payer to check the name associated with the account they are paying as very important and have been supportive of Confirmation of Payee (CoP) since its inception. In our September 2017 Payment Strategy Forum consultation response, we wrote *“Yes, we would wish to participate in the Confirmation of Payee service to offer our members greater confidence in who they are paying and help to prevent.... scams.”*

We recognise that the passing of General Directions could drive the ubiquity which will help to address the detriments of accidentally and maliciously misdirected payments and promote a consistent customer experience. Payers’ experience and faith in CoP could be dented if and when they try to check a payee on the first few attempts a response is not possible due to non-participation of a payee PSP.

However, in addition to the PSR’s aim of delivering CoP in a timely, safe and secure manner, we believe that priority should also be given to a reliable and co-ordinated delivery. We can see the potential for end-user detriment if consistency of payer experience is compromised in order to achieve delivery by April and July 2019.

We appreciate the need not to move at the pace of the slowest so are supportive of the setting of deadlines – however, we would challenge the achievability of those detailed in the consultation. We discuss involvement of PISPs in our response to Question 2, our thoughts on the implementation deadlines in question 9 and possible alternative approaches in our response to question 10 below.

Taking a wider industry perspective, there are issues on the timing and scope of the proposed directions that need to be assessed. Nationwide and other members have contributed to UK Finance’s response to this consultation and these macro-level issues include the timing of other mandatory deliveries of 2019 including Open Banking and PSD2 Regulatory Technical Standards. Individual firms engaged in these programmes face contention and, as a whole, the industry may need to evaluate its priorities to create a roadmap for 2019 that complies with regulation but also maximises the value for end users, including victims of APP Scams.

As well as their timing, the scope of these directions will be a key consideration given we need to create the greatest value to end users, especially consumers, as rapidly as possible. There are elements of CoP that can be deployed more easily than others, and for some PSPs there may be challenges that lead to unintended consequences of increased exposure to financial crime – for example if they are highly dependent on vendor delivery, perhaps operating their current accounts via a head office collection account model.

Other factors that influence towards a successful deployment of CoP in the UK include testing, communications and governance. Each of these is important to get right in 2019, and perhaps testing is an area we would particularly stress as we’re very keen not to undermine the benefit that

end users derive from the UK's world leading near real time payments, whilst making them as safe as possible. As Nationwide has noted previously in dialogue with the PSR, we are concerned at the unintended detriments that may arise should there be 'excessive' negative responses to CoP requests. With this in mind, we're keen to support the development of matching capabilities and their reciprocal testing, and optimise fully the outcomes they yield.

Q2 Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?

In principle, for Confirmation of Payee to achieve the desired level of protection for our members, we believe that all PSPs, including new PSPs, would need to participate. We also recognise the risk mentioned in the consultation that non-participation could result in a migration of fraud to those PSPs without a CoP capability.

For smaller firms and new entrants, delivery of CoP must not be uneconomic. The development of third party vendors to meet some requirements could help but this should be factored into implementation plans. We would ask for this to be considered in the timing of the implementation of CoP for these players.

Q3 Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?

If General Directions are issued we believe that:

- Logically, PISPs that are not also ASPSPs should only be required to send a request.
- All ASPSPs should be required to send and respond to a CoP request.

Going forward, further consideration will be needed for investment firms for whom the ability to respond to a CoP request could deliver customer benefits

Q4 Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?

We believe directions should be given for both Faster Payment and CHAPS transactions as:

- Not least, the former represents the significant majority of volumes of misdirected payments/APP scams, and the latter the highest potential value of individual transactions.
- Customers make misdirected payments and, as recognised in the Contingent Reimbursement Model, suffer APP scams on both payment types.
- There is a risk that if CoP is only required in relation to one payment type APP scams will migrate to the other.

CoP rules and standards have been designed to operate with both payment types. In fact, it is designed to be payment type agnostic. Therefore, CoP could also be used to enable Direct Credit payments to customers (e.g. for benefits, salaries etc).

Q5 Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?

We believe that the choice of payment channel should be left to the Payer PSP. The liability position for non-provision is clear within the Contingent Reimbursement Model (CRM) and again the economic and practical effectiveness of mandating this for all channels and all PSPs needs to be understood.

We would agree that CoP should be used on new beneficiary set up or when the beneficiary details are changed. This mirrors the utilisation of the “trusted beneficiary” exemption in article 12 of Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Open Standards of Communication (SCA-RTS). Where strong customer authentication has been performed for the initiation of an electronic payment, and the payer has established the payee as a trusted beneficiary, PSPs have the option of executing future electronic payments to this beneficiary without the application of SCA. Importantly, where the payer amends the list of trusted beneficiaries, broadly equivalent to the changing of a payment mandate, SCA must be applied again. But again, we believe that a decision about when a CoP check is conducted should be a choice for the Payer PSP as this may be in the competitive space.

In mapping customer journeys, we have considered the question of whether customers who have switched accounts (with their mandates) should be requested to perform a CoP on the first use of this beneficiary mandate with the new PSP. This is an area in which we would seek guidance – there are technical limitations in being able to identify skeleton mandates and/or a view of mandates that have been paid without issue. The industry has worked to ensure that switching accounts should be a seamless process to encourage competition. We are conscious therefore, that we would not want to create a disincentive to CASS use for some customers by creating more friction in the switch. However, we are also keen to ensure that customers are protected from APP scams and PSP liability is effectively managed, given that there is no process for confirming whether CoP was performed and that effective warnings were given to the payer by their previous PSP.

Under the Contingent Reimbursement Model, there is therefore a strong incentive on PSPs to apply CoP to payments from switched accounts. The aims of both CASS and CoP need to be aligned.

#### Q6 How should any directions deal with the potential for people to opt out of the CoP process?

This provision is already part of the CoP solution. In mandating its implementation, the directions are in effect already providing for the potential for people to opt out.

We recognise the importance of protecting individuals whose information should not be disclosed as part of a CoP request. We would also want to ensure that this provision is not exploited by scammers.

Therefore, the directions must accommodate this potential – i.e. their wording should not make it mandatory that all payees participate. If possible, we would encourage guidance to Payee PSPs that they must act with care in allowing people to ‘opt out’.

To ensure a smooth and consistent implementation of CoP, guidance on the parameters regarding the application of the ‘opt-outs’ provisions offered by ASPSPs would be beneficial. The criteria under which a payee is deemed eligible to be opted out and any evidentiary considerations should be clearly defined. This will give a clear benefit in terms of consistency of the COP service and its ubiquity.

#### Q7 Should any directions cover the sending of money from both individual and business accounts?

Yes, as both are vulnerable to APP scams as recognised in the draft CRM's coverage of micro-businesses.

But we believe businesses should have an internal payment process with safeguards against APP fraud risk as per our recent consultation response on the CRM. And, for many larger businesses their operating model for processing payments in bulk may not align with the 'peer to peer' nature of the CoP solution, but this needs to be explored further as there may be ways in which CoP might be useful in setting up the individual payment mandates within bulk submissions.

[Q8 Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?](#)

Directions should cover both sending and responding - as the consultation highlights in paragraph 3.13 there is little point in a CoP service which only enables one side of a request to be satisfied.

In separating the directions for sending and responding to CoP requests, the PSR recognises that delivering a respond capability will not be dependent on channel, process, training and other changes necessary for firms to implement the request functionality and therefore, theoretically respond could be delivered to a different timescale.

The directions might be structured in such a way to reasonably enable partial adoption for players for whom sending or responding may be their only necessary participation in CoP. The directions should be easily divisible - enabling this contingency for non-account holding PSPs, but at the same time the incentive on major PSPs to both receive and send CoP requests will help address the bulk of the detriment we have identified within the UK market.

[Q9 Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.](#)

As stated in response to question 1, in addition to the PSR's aim of delivering CoP in a timely, safe, and secure manner, we believe that priority should also be given to a reliable and co-ordinated delivery. We are still working through the costs and implementation implications of adopting CoP as the solution takes shape, but we do not feel it is possible to deliver COP in an effective and safe way to the proposed dates. To ensure we deliver COP in a manner consistent with the PSR's stated aims, we would propose that a revised timeline be considered.

The timeline as currently proposed raises concerns in relation to limited opportunity for testing and risk mitigation, availability of viable vendor solutions for those PSPs that might wish to use them and a lack of centrally coordinated implementation/communication support. These, as well as further points made below, present real challenges to CoP's effectiveness, and therefore the likelihood of achieving the benefits envisaged by the PSR if they are not factored into realistic implementation scheduling.

A critical consideration is that the CRM and underlying measures such as CoP are required to be implemented at the same time as the industry is required to deliver other significant regulatory change such as Open Banking and Strong Customer Authentication. This joint requirement presents a challenge as PSPs payments change agendas are full and the same resources and expertise are needed to deliver both. It is not as simple as putting more funding and other resources in place as expertise and experience with internal systems also needs to be developed. This is further

compounded by the concentration of business readiness activity necessary in the face of an uncertain Brexit.

Our other considerations include:

- Although much work has been done, the Pay.UK rulebook/guidelines will not be finalised until the beginning of 2019.
- Furthermore, should the PSR implement General Directions as an output of this consultation, timescale complexity increases as we await confirmation and how this interacts with further publications from the APP Steering Group and Pay.UK.
- Although, CoP appears on the face of it to be a simple solution to deliver, it has many complexities – such as data privacy, matching standards, customer protection and liabilities - which have needed to be worked through at an industry level to develop the core rules and these need to be interpreted for application in-house in order to provide a robust service for our members.
- Offering CoP will require significant development in our channels and clarity of the solution is necessary to understand how the proposition could be adapted for mediated channels and back office processes.
- Operational processes will need to be reviewed to support queries from payers and payees. Development of the matching capability, testing of the proposition, staff training, and customer communication all need to be factored into this change process.
- Member education and awareness will need to be developed and delivered.
- A process through which we could enable customers at risk to opt out will need to be implemented.
- We may need to amend and notify customers of changes to our Ts&Cs and Fair Processing Notice, which will influence and impact the planned schedule of contractual changes lined up for 2019.
- A coordinated approach is required to implement CoP across participating PSPs, including communications, implementation planning and testing.

Please also see our response to Question 2.

Given the constraints we have documented, specifically the payments transformation schedule in 2019 and resource capacity, a strategic decision would need to be made, potentially impacting our compliance to Open Banking and Strong Customer Authentication regulation. We therefore advise that these important regulatory requirements and dates are taken into account for the purposes of the General Directions for CoP.

Broadly, Nationwide's position on the implementation timeline aligns with the position UK Finance is reporting on behalf of its members and we call out factors influencing our readiness that are common across our peers. However, we can validate this from the perspective of our own ongoing project activity which is progressing as rapidly as possible but operates, so far, without the degree of solution definition from the centre that is needed for the level of design, build and testing we should aim for. We are also progressing independently in building our technical solutions but in common with others, we anticipate vendors may play a valuable role in the near future. However, at this stage, vendor offerings are largely undeveloped and partial, with perhaps some of the most valuable benefits being in 'augmenting' the CoP service by enhanced matching protocols for example.

[Q10 Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?](#)

The obvious answer here would be to allow adoption of CoP at the pace of the market – incentivised by the implementation of the voluntary CRM which includes finalised dates for when CoP would need to be considered with regards to determining liability for sending and receiving Firms.

For the longer term, we suggested another alternative in our CRM consultation response, we wrote *“we feel the New Payments Architecture being developed by Pay.UK should include transactional security in its scope, leveraging the potential benefits of ISO 20022 messaging standards and potentially enabling name validation on the actual transactions in flight before funds are available to withdraw.”*

[Q11 Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.](#)

We believe the PSRs identification of the benefits to be mostly correct and broadly agree with the data sources quoted in their collation, notwithstanding our points below.

Although we are working with industry to make CoP effective, it is difficult to comment on some of the assumptions in the benefits analysis. Until CoP is in place, we will not know how many customers continue with payments despite receiving a negative or ‘match not possible’ response. This will partially be determined by the implementation of the final solution, participation of payee PSPs (hence the importance of co-ordinated implementation), customer behaviour and the efforts of fraudsters to frustrate the barriers put in place by CoP (e.g. by social engineering). The benefits stated in the first year do look ambitious.

An assumption should be included that the benefits dwindle over time as scammers adapt and find other ways to defraud customers via methods where CoP is not effective. Whilst this doesn’t challenge the assertion that CoP could help prevent 90% of APP scams where the name entered does not match the account details, it does acknowledge that the efforts of fraudsters is likely to increasingly focus on activities that avoid CoP detection, or indeed that they are likely to increase their activity in order to maintain the same level of profit. For this reason, a 90% prevention rate does not necessarily equate to a 90% reduction in losses.

We believe CoP will be most effective as part of a layered set of measures including those currently under consideration by the APP Steering Group, UK Finance and Pay.UK. Again, as other measures come on stream it will be more difficult to comment on the effect of CoP alone.

We would suggest that the statements made under point 7.1 are revised to include the inherent benefits related to losses avoided due to the prevention of accidentally misdirected payments. The Credit Payment Recovery process is a largely successful tool for resolving these types of misdirected payments, but we are aware that losses do still occur, be that for customers directly, or firms who reimburse under Bank Error. We would recommend that the PSR consult with Pay.UK to understand the extent of these losses across the industry based on their cumulative reporting statistics.

In addition to those stated, other benefits could include internal savings on operational costs for PSPs involved in the processing of APP scams and accidentally misdirected payments.

To expand on our response to question 9 above, without consideration of realistic implementation timelines, a possible phased delivery and appropriately tested development of technical standards we feel CoP’s effectiveness would be compromised and potentially undermine confidence in near real-time push payments rather than inspire trust. In other words, we feel there is a positive cost: benefit advantage in delivering a well-developed and tested capability later in 2019.

Q12 Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

As we said above, we are still considering our final costs for CoP however, we believe that the estimated industry cost involved in implementing CoP (£200m) is low if this is to cover all PSPs participating in CHAPS and FPS (direct and indirect). Of particular note should be the outcome of question 5. Adoption across all channels, if mandated by the directions, will drive significant cost for PSPs.

There is a need to agree the objectives of the CoP communications prior to selecting the most appropriate communication methods and budget. Nationwide is working with the industry to drive forward those conversations.

Q13 Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

We would challenge the stated reach of counterfactual (C1) – “...assumes that without the proposed directions, CoP would not be available to the majority of consumers without regulatory intervention.” Given that the CRM requires CoP, and the Steering Group (plus others) have committed to implementing it, this will encompass a large percentage of payments made/payers in the UK. The benefit of mandating COP is therefore less than stated in the document.

It's important to recognise the theoretical origins of a ubiquitous CoP solution within the UK's payments industry pre-dates the foundation of the Payments Strategy Forum – but the detailed design and Open Banking infrastructure is only now emerging and becoming available for the type of peer to peer, decentralised version that the UK has opted to pursue. It's possible other routes to CoP delivery, such as centralised repositories akin to the UK Paym model and used by other international implementations, may have yielded a different deployment profile – but there are inherent pros and cons in these different approaches.

Q14 What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?

The proposed deadlines provide limited opportunity for the development of viable vendor solutions, proven maturity of name matching capabilities and could lead to increased costs and fewer benefits than envisaged for end users than if a later implementation was accepted.

Our response to Question 9 mentioned the lack of centrally coordinated implementation support - challenging the delivery of an effective proposition. Poor implementation caused by unrealistic timelines would introduce extended/duplicate costs for PSPs (not to mention sustained APP losses as CoP's effectiveness suffers).

At present, there are few vendor solutions available to PSPs, and even the most developed of these still face the challenge of the limited time in which to amend their services to match the Pay.UK solution rules and PSPs requirements. With inadequate opportunity to test and improve upon their processes, further challenge to CoP outcomes is likely as a result of immature name matching

algorithms. Further, vendor capacity to onboard multiple PSPs in relatively short succession will prove extremely difficult.

Q15 Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?

We should seek to ensure that individuals in vulnerable circumstances feel assured that CoP provides an additional level of protection to their payment journeys. Accessible communication and education is important here - there will likely be populations of people who may find it difficult to engage with CoP due to the added friction – though we do agree with the PSR’s view that this is necessary and reasonable given the benefits.

Further to our response to Question 6, sufficient consideration will need to be given in advance of implementation to the opt-out process, its eligibility parameters and PSP guidance on its application so as to adequately protect those individuals whose circumstances mean they may wish to ‘opt out’ of the service.

# Open Banking Implementation Entity

**Payment Systems Regulator Consultation on General Directions  
on Implementing Confirmation of Payee CP18/4**

**Open Banking Implementation Entity Response**

**4 January 2019**

1. The Confirmation of Payee (CoP) service will provide payment service users with a new mechanism that gives greater assurance that their payments are directed to the intended recipient and act as a barrier to Authorised Push Payment fraud. This is a welcome development that will deliver significant benefits and we are supportive of the PSR's aims to ensure that it can be implemented quickly and uniformly across the market.

## Introduction to Open Banking

2. The Open Banking Implementation Entity (OBIE) was established by the CMA following a very extensive analysis of the Retail Banking market, which found that a lack of competition was contributing to a failure of the market that has a particularly profound effect on certain groups of consumers, particularly overdraft users. The CMA concluded that the sector was not as innovative or competitive as it should be, and the complexity of charging structures makes it extremely difficult for even the most sophisticated consumers to assess whether they can get better value from other providers or products.
3. The CMA recognised that Application Programming Interfaces (APIs) could transform the financial services sector by enabling the sharing of account data that can power new innovative products and digital applications which are being developed by the vibrant FinTech community. OBIE was created to enable this innovation, and the initial component of its mandate was delivered in January 2018, consisting of APIs, data structures and security architectures that will make it easy and safe for customers to take control of their financial data and share it with organisations other than their own bank and enables developers to harness technology that allows them to do so.
4. The governance, composition and budget of the Implementation Entity were agreed by the CMA. It is led by an independent Implementation Trustee, with decisions taken by the Implementation Entity Steering Group (IESG), comprised of a wide spectrum of stakeholders including representatives of consumers and SMEs. Transparency and extensive consultation with a diverse range of key stakeholders is the cornerstone of the decision-making process.
5. Our vision is to give people real control over their finances, so they can securely and effortlessly move, manage and make more of their money and we are working to create a dynamic and sustainable market for new financial services, easily accessed through consumers' everyday devices. In doing so we want to put consumers in the driving seat by giving them complete control over their financial data, confident that their data will only ever be used with their express and informed consent.
6. A new phase of work is also underway to add measures to improve the customer experience when using Open Banking services, in particular services accessed through mobile apps, which reflects a desire of OBIE to focus extensively on the functionality that matters most to customers. To this end OBIE published Customer Experience Guidelines in September 2018 that sets out how the Open Banking Standards should be implemented to ensure an optimal customer experience that conforms to the requirements of PSD2. The Customer Experience Guidelines are critical components of the Standards and were created in close

consultation with the financial services and technology sectors, underpinned by a wide range of independent research. This has given valuable insight into how to ensure that security, trust, speed, transparency and control are all evident and effective throughout the customer journey. We intend to develop the Customer Experience Guidelines over time as the Open Banking functionality and supporting standards evolve.

## Open Banking's role in the Delivery of Confirmation of Payee

7. COP aims to improve the payment process for customers initiating payments by introducing a process allowing the payer's PSP to send a CoP request to the payee's Account Servicing Payment Service Provider (ASPSP) using an API, which will include the account reference details provided by the payer. The payee's ASPSP will then be able to match the details provided against their own account database and respond with the outcome of the verification request, again using an API. It is expected that payment initiation service providers (PISPs), third party aggregators and other third-party solutions will also provide various payment options which also rely on an API.
8. Given that the CoP architecture is reliant on an API infrastructure, OBIE was requested by Pay.UK to develop the CoP API specifications, given our competence in this field and the criticality of the Open Banking Directory, which all of the CMA9 retail banks are enrolled in. An added benefit is that the solution aligns closely to the existing suite of APIs that have been developed and are managed by OBIE, ensuring a high degree of consistency and interoperability with the existing Open Banking API framework.
9. The Open Banking Directory is a trust platform that has a record of all registered participants, which they can use to enable safe and secure connectivity within the ecosystem. OBIE has established rigorous registration and monitoring processes to ensure that participants are authorised to undertake the requested activity and they are who they say they are. The Directory can support a number of API based services, which require participants to make calls on API endpoints. In the end to end customer journey for CoP, the payer's PSP will perform a directory look up to determine the payee's ASPSP API endpoint and by virtue of this the ASPSP can be confident that it is responding to a legitimate request by an authorised participant.
10. OBIE is confident in the resilience of the Open Banking Directory. Its distributed design ensures that it is not a single point of failure.

## Scope of the Proposed General Directions

11. OBIE recognises the importance of customer protection within a customer journey and is supportive of the introduction of CoP together with the contingent reimbursement model (CRM) that will contribute to a consistent and robust approach to reducing authorised push payment (APP) fraud, ultimately leading to better customer protection and safer payments. The utility of CoP will be enhanced if it is widely available and the proposed general directions are an appropriate mechanism to ensure that delivery is co-ordinated, and implementation is timely.

12. It is unclear whether the intention of the PSR is to bring PISPs within the scope of the proposed general directions. The consultation document uses a broad definition of PSP, which suggests that this is potentially the case. However, while the consultation makes explicit reference to direct and indirect PSPs (defined as having contractual arrangements with another PSP enabling it access to the payment scheme), this definition would not extend to PISPs which by virtue of PSD2 do not require contractual relationships with the ASPSP. In addition, because PISPs are not actively involved in the settlement of payment transactions there is no need for them to be members of Pay.UK. However, our working assumption is that PISPs will be required to contract with Pay.UK for the CoP service. This does appear to impose unique obligation on PISPs active in the UK that are not applicable in other European markets and there is some ambiguity as to how this will work in practice for those PSPs which are supervised by a Competent Authority other than the FCA. This is an issue that will require some further clarification, possibly in the Open Banking Enrolment and Customer Experience Guidelines.
13. There is, of course, an overlap between CoP and the CRM particularly as the PSR has identified that use of the CoP will be an important determinant as to whether the PSP has met the required standard of care by providing appropriate prevention tools to payers. In this context we note that the PSR's position in relation to the development of the CRM is that the code should apply to PISPs who have control over preventing and responding to APP scams.<sup>1</sup>
14. We note that the FCA has recently made policy changes intended to provide victims of APP fraud (where they are eligible complainants) with access to dispute resolution through the Financial Ombudsman Service for complaints against payment service providers (PSPs) relating to the alleged fraud. Our interpretation is that PISP initiated payments are covered in the new definition of APP fraud.
15. The market for PISP services is currently at an early stage of development, but we expect to see innovative products emerge in the course of 2019 as the final components of the PSD2 legislative package enter into force. It would assist existing and potential market participants if the regulatory intention in relation to both CoP and the CRM was set out transparently and comprehensively. We are keen to engage with the PSR in more detail on this issue so that any obligations are clearly articulated in various Open Banking documents that set out the implementation requirements for both PISPs and ASPSPs in an Open Banking/CoP journey
16. Phase 1 of the Pay.UK CoP delivery is focused on ASPSPs, enabling facilitation of CoP requests and responses between ASPSP participants. A second phase of work (Phase 2) is planned to enable the development of new standards and messaging that will allow PISPs and, technical service providers (TSPs) to make CoP requests and present the response to their customers. Some initial consideration has been given to the possible design of this, but considerably more work will be required to evaluate and define the supporting standards. It is estimated that this work will complete in Q4 2019.
17. We will continue to work closely with Pay.UK to define the requirement and scope of Phase 2 deliverables. In particular, the extension of CoP to incorporate PISP payment journeys will potentially require the development

---

<sup>1</sup> PSR Authorised push payment scams : Outcome of consultation on the development of a contingent reimbursement model Feb 2018 para 3.73

of a new series of APIs to support the additional communication between the PISP that initiates the payment and the payee's ASPSP, which will validate and respond to the CoF call. In the absence of some form of additional messaging with the PISP, it will be unaware of the outcome of the CoP call and whether it is necessary for the payer to take additional steps (one of which may be to amend the payment instruction to reflect the correct account name. This will require careful consideration to ensure that the process flow is fully transparent to the PISP and that they can support the payment process.

18. In addition, it is currently undecided as to whether CoP should be required for all PISP payments. An important use case for Open Banking will be the development of PISP solutions that will help online retailers reduce the costs associated with the acceptance of conventional card payments. This will require the PISP to have an established relationship with the retailer and consequently the TPP will be able to accurately populate the settlement account details of the retailer, reducing the risk of APP fraud and misdirected payments. In these circumstances CoP is unlikely to provide any additional protection and indeed the added steps may introduce unnecessary friction, which makes PISP payments less attractive for users. Card transactions do not fall within the scope of CoP.
19. PISPs who offer CoP functionality to customers will be required to comply with the service rules and standards set by Pay.UK. The commercial framework and rules for PISP participants are yet to be developed and will be considered in the context of the Phase 2 development.
20. The PSR should ensure that:
  - a) the timing of the directions is fully aligned to the COP delivery programme, in a phased approach reflecting the fact that the scope of CoP will extend on completion of Phase 2;
  - b) the scope of any direction takes account of the complexity of certain PISP journeys;
  - c) the need for PISPs to enter into some form of commercial agreement with Pay.UK and the implications of this on PISPs which are regulated by a European Competent Authority other than the FCA;
  - d) that sufficient time is allowed to enable OBIE to revise existing Customer Experience Guidelines that set out optimal customer journeys ;and
  - e) that the application of the liability model under the CRM is also suitably phased to take account of the overall programme delivery schedule to ensure that liability is not imposed on firms until they have the capability to provide CoP functionality.

## Timeframe for the Proposed General Directions

21. OBIE believes that the proposed timescale for PSPs to be capable of receiving and responding to CoP requests by 1 April 2019 is ambitious because although the technical specifications for the CoP service are available there are still a considerable number of issues in relation to the contractual arrangements, including the liabilities of the various participants, yet to be agreed. Participants could not be expected to commit to the use of the service until this is satisfactorily resolved.
22. OBIE is confident that the Directory is sufficiently scalable to accommodate the 300-600 ASPSPs that are likely to participate in the CoP service. However, on-boarding this number of participants by 1 April 2019 would potentially present some logistical challenges. A phased approach as set out above would enable effective

orderly management of the on-boarding process. We note that a number of significant ASPSPs, notably the CMA9, are already participating in the Directory at present and have API capability. However, on boarding the larger number of ASPSPs some of whom are presumably planning to implement their API capability in line with the timetable set out under PSD2 is likely to be problematic for those firms. The precise nature of the enrolment process is still under discussion between Pay.UK and OBIE and consequently it is currently difficult to accurately estimate the time required to enrol participants. This will require further and more detailed consideration.

23. OBIE considers that it would be good practice to adopt the same approach that we use for implementation of new or revised standards that gives participants a 6-month lead time from the publication of the standard, and supporting Customer Experience Guidelines, so that participants can plan ahead and build to this plan. The objective of this is ultimately to ensure that change is delivered consistently and to ensure the stability and resilience of the underlying systems.
24. In addition, OBIE has usefully adopted a managed roll out over the course of six weeks to enable participants the opportunity to systematically test the system in a controlled way to provide the necessary assurance that the system is stable, fully secure and ready for use by customers. Testing initially takes place in a non-live environment and then progressively in the live systems under controlled circumstances – to ensure the integrity of the service. We commend this approach and recommend that the PSR factors in a similar approach and timings into the proposed delivery schedule for CoP.

## Potential Issues Arising from the General Directions

25. As previously noted, the CoP proposition is closely related to complementary work to implement the CRM voluntary code. We note that the draft CRM voluntary code specifically requires the sending firm to take reasonable steps to prevent APP fraud, where on a risk-based assessment it identifies APP fraud risk. This includes a requirement to take reasonable steps to provide 'effective warnings' to customers.
26. There is likely to be some tension between the PSD2 regulatory obligations on ASPSPs not to create obstacles in Open Banking customer journeys, while providing effective warnings to customers in instances where there is a genuine risk of APP fraud. In our view the draft CRM code is clear, warnings should only be shown in instances when there is an identified APP fraud risk, based on objective risk-based criteria. As such, these warnings should not appear by default for all new payments including those initiated via a PISP to a new payee, especially as most PISP initiated payments, particularly at the outset, will be made to new payees.
27. If ASPSPs adopt a blanket approach where a warning is provided for all payment journeys by default, we believe this will have a particularly unfavourable impact on PISPs, limiting competition within the payment industry, decreasing adoption of PISP services by customers and resulting in a poor outcome for innovation and customer choice. This is potentially inconsistent with the PSD2 framework (including the RTS and EBA Guidelines). It is critical that the overarching regulatory approach supports the wider objectives of PSD2, which are to promote innovation and competition within the payments industry whilst at the same time mitigating fraud.

# Ordo

## **PSR Consultation on general directions on implementing Confirmation of Payee (paper CP18/4)**

20 December 2018

Response from Ordo (the trading name of The Smart Request Company Ltd)  
Submission to [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)

REDACTED version for PUBLICATION

*The following information is the property of Ordo, the trading name of The Smart Request Company Ltd (“Ordo”) and is provided to the PSR for the purposes of our response to the above consultation only.*

*The information is only to be used in connection with Confirmation of Payee, it is not to be used for any other purpose.*

*The commission of any unauthorised act in relation to the information may result in civil or criminal actions being taken by Ordo in relation to this matter. Any licences issued by the Copyright Licensing Agency Limited do not extend to this matter. All opinions and forecasts contained herein are the opinions of Ordo and are made in good faith at the time of writing.*

**Who we are:**

We are Ordo, the trading name of The Smart Request Company Ltd. We are an early stage fintech start-up and TPP.

The five founding directors incorporated the business as a new venture earlier this year, having previously worked together in the Faster Payments Scheme, driving new competition in banking and payments and transforming access to the Systemically Important payment system. Whilst we were the leadership team at Faster Payments, we instigated bringing on new challenger banks and other PSPs such as Monzo, Starling, Atom, ClearBank and Transferwise. The team were awarded the Payments and Cards Awards Industry Achievement Award in 2017 by their payments industry peers for their work to allow Transferwise and its customers direct access to the Faster Payments System.

Following our time at Faster Payments, we set up The Smart Request Company Ltd, trading as Ordo, in the spring of this year.

Ordo's company purpose is:

to improve financial wellbeing of individuals, businesses, social enterprises, charities, community groups and the public sector by helping them to be more in control of their finances. We do this by:

- enabling payers to securely and simply see what they've been asked to pay, trust who's asking, and then choose how and when they make or don't make payments;
- enabling billers to securely, simply and cost effectively provide information to, and request payments from, their customers without having to gather, store and protect payers' private financial information; and
- enabling billers to understand the status of their payment requests and receive settlement irrevocably and without delay from their customers, directly into their bank accounts.

We are leveraging our collective experience in payments, technology, consumer markets and regulation to achieve this.

***Our view and what we think a secure payments future should look like:***

We are creating a better way to request and make payments with a new, secure end-to-end competitive digital payments overlay service. We believe the solution we are building is an important part of the strategic long-term solution which will afford all payers, be they individual consumers or businesses of any size, the confidence and assurance that their payment has gone to the intended destination.

If every payment begins with a request from the biller concerned (which could be a consumer or a business), this significantly lessens the likelihood of a payment going to the wrong destination. A biller's request for payment will contain the account details for the biller [redacted], and these are neither revealed to, nor can they be changed by, the payer. The receiving (of the request for payment) potential payer will then only choose to pay the request if they recognise the biller, what the requested payment is for and if it is for the correct amount.

[Redacted] The payer will be notified that they received a request for payment, which will contain the biller name. [Redacted]

*At the date of writing, Our comments regarding scope of CoP are made without the benefit of access to the detailed CoP specifications/requirements. As an aspiring PISP, rather than an existing ASPSP, we have so far not been granted access to Pay.UK's documents. It is possible therefore that we may have misunderstood the precise scope of CoP.*

*The CoP Service and rules need to ensure that:*

*Where a third party provider (TPP) includes in a Payment Instruction for their customer an account title that is the same as, for example, what is shown on a person's debit card or cheque book, the CoP process must result in a perfect match and the process for the end user to complete a payment must be seamless and frictionless.*

*All of the account titles that an ASPSP uses to describe its customer must result in a perfect match from the CoP service. This should cover: cheque book name, debit card name and the account name provided via any push payments.*

*Where the provided account title is only a close match, and the payer has to manually accept the match, Open Banking must inform the TPP that the payer had to validate and accept the played back title to allow this to be investigated, improved and amended if relevant.*

***At the point of launch of CoP it is vital that all these requirements can be met for TPPs initiating payments via Open Banking. Failure to provide these will prevent the TPP delivering a comparable level of service as an ASPSP and would mean that the TPP was not operating on a level playing field compared to an ASPSP. This would be anti-competitive, prevent the objectives of PSD2 being realised and must not be permitted by regulators.***

This is particularly relevant to our service as [Redacted] the payer will have received a digital request from the biller [Redacted] [which] include[s] its receiving account details [Redacted]

To address the consultation questions which are relevant to us specifically:

**1. Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and if so, what are they? Do you have any other comments on the issues raised above?**

The approach of giving directions is not without risk. It could enable ASPSPs to behave in such a way that means they comply with directions but is effectively anti-competitive enabling them to discriminate or exclude TPPs. Any regulatory mandate and/or directions given must be technology neutral. Adequate consultation with all parties that are individually affected by any directions is essential.

We believe our request for payment service provides a fuller, richer and more comprehensive package of security and assurance than Confirmation of Payee alone, as explained above. [Redacted]

*As at the date of writing,* In the absence of sight of standards and any rules (see comment above), we would urge the PSR to ensure that CoP does not prevent other long-term strategic solutions being created that may serve the market, and solve the problem, more comprehensively.

**2. Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? .....**

Excluding certain types of ASPSP, typically smaller ones, may lead to those organisations being targeted by fraudsters. Ultimately this could distort the market as customers may decide to only bank with larger ASPSPs, thereby conflicting with the long-stated desire to increase competition in the current account market

**3. Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

**4. Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions?.....**

We note that the proposed solution excludes other forms of push payment such as Bacs Direct Credits; has the likelihood that fraudsters will change their vector of attack to such services been considered?

**5. Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

Our service will provide [Redacted] a payer with certainty every time.

If only applied to CHAPS and FPS 'Single Immediate Payments' fraudsters could encourage victims to set up Standing Order and 'future dated' transactions ('set it up now, to pay me tomorrow/next week'). Unless these are in scope of CoP, with the Payer having the ability to check the payee account name, end users will not benefit.

**6. How should any direction deal with the potential for people to opt out of the CoP process?**

Billers and payers will sign up for our service whereby proactively making the decision to pay using a more secure and smart end-to-end solution [Redacted]. This model largely reflects how people exchange information and buy services in today's digital, online and mobile world, eg messaging services such as WhatsApp, music and TV streaming services such as Netflix and Spotify, and picture sharing services such as Pinterest all require a proactive sign up.

[Redacted]

Any directions should not prevent a user, whether opted in or out of CoP, participating in any other kind of service that delivers the same assurance or more.

**7. Should any directions cover the sending of money from both individual and business accounts?**

Our service will provide [Redacted] certainty every time. We have anecdotal evidence that SMEs suffer widespread fraud attacks when emailing invoices to customers for payment. Not only will our service ensure the correct SME biller is paid, but it will provide a channel for SMEs to send their invoices in a safe and secure environment.

**8. Should the directions separate out responding to CoP requests from being able to send CoP requests?.....**

**9. Do you agree with the [1 April 2019 for responding, and 1 July 2019 for sending] deadlines for the introduction of CoP?....**

**10. Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

As outlined above, our request for payment service will be an end-to-end secure digital service [Redacted]. We believe that our solution, therefore, is the strategic, long-term, richer solution that will provide the UK with the next progression in the UK's already advanced payments system. [Redacted] where there is a match between who the payer is wanting to pay and the destination account title, the checks an ASPSP conducts must be frictionless for the payer, otherwise this will impede adoption and undermine the UK's opportunity to lead the way in the next revolution of making payments easier with greater security.

Excluding business or consumer accounts will leave an opportunity for fraud.

Article 74 of the Payment System Regulations 2009 refers to liabilities on PSPs around incorrect account numbers. It is this that has enabled ASPSPs to not validate account name and number. Has the PSR considered this, and/or potentially raised with the FCA?

***Incorrect unique identifiers***

***74.—(1) Where a payment order is executed in accordance with the unique identifier, the payment order is deemed to have been correctly executed by each payment service provider involved in executing the payment order with respect to the payee specified by the unique identifier.***

***(2) Where the unique identifier provided by the payment service user is incorrect, the payment service provider is not liable under regulation 75 or 76 for non-execution or defective execution of the payment transaction, but the payment service provider—***

*(a) must make reasonable efforts to recover the funds involved in the payment transaction;  
and*

*(b) may, if agreed in the framework contract, charge the payment service user for any such recovery.*

*(3) Where the payment service user provides information additional to that specified in regulation 36(2)(a) or paragraph 2(b) of Schedule 4, the payment service provider is liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.*

- 11. Is our assessment of the benefits the right one?....**
- 12. Is our assessment of the costs the rights one?.....**
- 13. Is our assessment of the trade-off between costs and benefits the right one?.....**
- 14. What is your view of the impact of the proposed dates in our approach to the trade off between costs and benefits?....**
- 15. Equality impact assessment.**

We are a commercial company building a competitive solution for the payments ecosystem. The information above remains the property of Ordo, the trading name of The Smart Request Company Ltd.

# Santander UK, plc

**PSR Consultation on general directions on implementing Confirmation of Payee****Response from Santander UK, plc****Overview**

1. Santander UK (hereafter Santander) welcomes the opportunity to input into the PSR's consultation on general directions on implementing Confirmation of Payee (CoP).
2. Santander supports, and has provided input to, the UK Finance response to this paper. However, we wish to emphasise a number of points below.
3. Please note that we do not consent to the publication of this response, either in whole or in part, without prior discussion. We would be happy to discuss our comments with the PSR and can be contacted at [REDACTED] to arrange or with any further queries.

**Summary of key points****1. Implementation Timescales**

4. Santander welcomes the introduction of Confirmation of Payee, recognising the value and added protection it could bring to the market. Key to the success of CoP will be market-wide adoption; a Direction could help to achieve this.
5. However, for the implementation of CoP to be successful and deliver the best possible, and most consistent, customer outcomes, the proposed implementation timescales must be reasonable and realistic. The current proposed timescales are extremely challenging, particularly as these are on top of the existing demands already facing firms as a result of Open Banking and PSD2. Moreover, a period of testing is also critical – Open Banking is a relevant example that demonstrates whilst message standards can be written quickly, and the coding delivered to those specifications, a period of 'fine tuning' will be essential in a collaborative space to ensure the best outcome for customers.
6. Santander maintains that there is a clear link between 'regulatory flow' and the risks this can pose to financial institutions' operations. We consider that there needs to be better coordination and prioritising of regulatory mandates. To recognise the complexity of the payments roadmap faced during 2019, Santander would strongly support the creation of a coordinated timeline between the PSR, UK Finance and its members, Pay.UK and Open Banking.

## 2. Customer Impact & Engagement

7. We are mindful that there are considerable customer experience changes due to be implemented in 2019. In order for CoP to achieve on its objectives and instil transactional trust, a consistent, aligned and thought-through industry implementation is critical.
8. The PSR is considering a differentiated timeline for receiving and responding to, and sending, CoP requests. The Direction should only apply to the ability to receive and respond to CoP requests. This means, at minimum, firms need to comply with the request. This places the sending of requests in the competitive space for firms to consider account and payment type.
9. Consistency for customer experience may also play an important feature in the overall space. Whilst ensuring against competition issues, the various PSPs may need to establish some common behaviours; it would bring further risk to the model if some banks only accept “Yes” validated responses and reject all other customer requests; while others try to help customers by providing support, advice and fuzzy matching to better support the model.

## 3. Addressing Authorised Push Payment (APP) Fraud & the Contingent Reimbursement Model (CRM)

10. Santander agrees that a common and agreed, legally binding target is essential for the successful delivery of CoP. Without an aligned delivery and standard, the trust and integrity of the feature is reduced and will lead to a service that adds minimal value and accuracy for customers along with opportunities for fraudsters to manipulate a weak service. The implementation of this should be focused and prioritised based on the known risks from APP scams, with an agreed Minimum Viable Product (MVP) and scope fully defined by Pay.UK which enables participants to deliver to agreed timeframes. An adoption in H1 2019 will allow participants to further mitigate scam risks for customers and, therefore, reduce the financial impact caused by scams to customers in alignment with the CRM guidelines.
11. [...]
12. The PSR’s leadership in the payments space will be invaluable as there is a need for consistency – the aims of the CoP work needs to be considered alongside the aspirations of other change programmes. To use Open Banking as an example again: their customer journey from the TPP engagement looks to remove all friction, rather than supporting the gentle warning to customers of the risks behind scams and APP.

## 4. Conclusion

13. We support the introduction of CoP and recognise the benefit this could provide to both customers and the industry, but the delivery needs to be carefully considered, with testing a critical feature of delivery, and consistency is essential. We consider a more refined Direction as a helpful way to coordinate the market and ensure CoP works well for the entire ecosystem. Whilst we see the benefit and welcome the introduction of CoP, we believe the timescales need to be considered carefully given the volume of significant changes being delivered by the industry, and the scale of the firms required to introduce new processes and systems

needs to be managed carefully to ensure consistency and the customer experience is protected.

**[ENDS]**

# Secure Trust Bank

4 January 2019

Confirmation of Payee Consultation  
Payment Systems Regulator  
12 Endeavour Square  
London E20 1 JN

Sent via email to: [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)

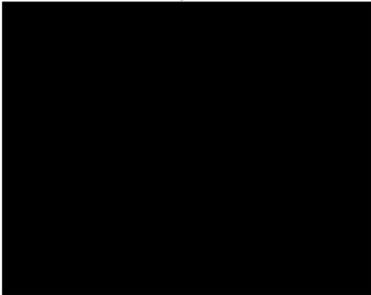
### **Secure Trust Bank Response to Consultation on general directions on implementing Confirmation of Payee**

We welcome the opportunity to respond to this consultation. Secure Trust Bank (“the Bank”) agrees that the Confirmation of Payment (CoP) service would reduce the incidence of authorised push payment scams (“APP scams”) and is supportive of its implementation. The Bank is not opposed to the issuance of directions under the Financial Services (Banking Reform) Act 2013 (FSBRA), requiring payment service providers (“PSPs”) using Faster Payment and CHAPS to send, receive, and respond to CoP requests. The Bank does, however, have the following key concerns regarding the proposals set out in the consultation:

- The Bank considers the timescales to be unrealistic. We agree that the CoP scheme is most effective if implemented widely. However, the small timeframe between closure of the consultation and proposed implementation dates does not give adequate time for firms such as the Bank, which operate on an agency banking basis in association with one of the major banks, to take the necessary steps to implement CoP.
- It is not clear to us how CoP will deal with instances where a payee will legitimately send money to an entity with a different name to that named on the receiving bank account. Examples include where trading names or styles are used in place of the legal entity, or where payments are made to different entities within a Group. The Bank considers that further clarity is required in this respect prior to implementation of CoP.
- It is also not clear to us how CoP will impact on invoice factoring and discounting arrangements. In these cases, payments will be initially directed from the customer to the firm from which it has procured services (“the Firm”), but under the factoring or discounting arrangement, those payments will then be routed to the provider of funding to the Firm under the arrangement (“the Funder”). It is generally the case that, in such circumstances, the Firm does not wish its customers to know that it is party to a factoring or discounting arrangement, as this could indicate financial weakness. They would not wish their customers to be making payments directly to the Funder for this reason. The Bank believes that further clarity is required on how such arrangements could continue under CoP.

Detailed responses to the questions follow. Please note that the Bank would prefer its responses to this consultation to remain confidential.

Yours sincerely



### Detailed responses to consultation

**Question 1: Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

The Bank is supportive of the introduction of CoP and is not opposed to the issuance of directions. It is, however, concerned about the proposed timescales.

In our opinion, giving direction to introduce CoP can only take place when the vast majority of the industry is ready. Given that this consultation is not due to close until early January with time then required to collate responses, we consider the timescales as set out to be unrealistic. The costs are not yet available for the service and companies such as the Bank agreed their 2019 budgets some time ago. It was only recently that our main banker talked to us about the action required on our Agency Sort Codes. The timescales therefore are unachievable from our perspective.

Clarity is required on issues such as trading styles/names as well as global indemnities and how the banks will then handle requests. Implementation before the fine detail is fully available could cause customers to lose confidence in the UK banking system.

**Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

The Bank's view is that customers are unlikely to understand the difference between direct/indirect settling participants for FPS/CHAPS, so excluding some of these types of PSP would make it difficult to identify who was in and who was out of the CoP scheme. Therefore, in order to provide customers with clarity that CoP covers all (ultimately) payment types, there should not be any exceptions/exclusions based on PSP type.

However, the costs of implementation need to be considered, as do firms' technical ability to link to CoP, with or without an aggregator. The non-inclusion of some PSPs may not adversely impact the likelihood of APP scams and frauds, as firms may have other controls in place to mitigate these risks, such as linkage of nominated accounts to savings accounts.

**Question 3: Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

In theory, the Bank considers that responders and requesters should be the same.

**Question 4: Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

FPS and CHAPS are both at risk payments from a fraud perspective, so in our view both should be in the scope of the directions.

As mentioned in responses to previous questions, it should be noted that there are times when the payee will send money to a place that has a different name to that of the end customer facing business (i.e. Group & trading style/name as against legal entity). The ability to deal with these types of facilities needs to be ascertained before CoP is launched.

**Question 5: Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

All payment channels should be considered in our view.

For CoP to be successful and ubiquitous it should be applied for any new mandate instruction or any change to an existing mandate, otherwise mandate changes will become one area for fraudsters to target.

Consideration should be given to how to treat payments where the payee account name has changed e.g. where an account may be in joint names but is amended to a single name. In this instance there should be a notification from the recipient PSP to the originating PSP.

**Question 6: How should any directions deal with the potential for people to opt out of the CoP process?**

Clarity is required on what the term “people” relates to in the question e.g. individual payer or PSP. If the term refers to an individual payer, then in our opinion, there should not be an option for people to opt out.

If there is an opt out available to PSPs then the message that is then subsequently relayed back to the originator is crucial. If there is a legitimate reason for an institution to opt out, then this should not be perceived as a negative position by customers or requesters. It also needs to be clear where the liability resides in the event of opt out.

**Question 7: Should any directions cover the sending of money from both individual and business accounts?**

As the intention of CoP is to reduce APP scams then handling individual accounts could be considered a higher priority than business accounts. However, the operational implications of a two stage roll out would need to be considered. It would need to be clarified whether sole traders and partnerships are treated as business accounts or individuals.

**Question 8: Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

In the Bank's opinion, it would make more sense for directions to cover both requests and responses. Separating could give more time to allow PSPs to embed the new process but the timescales are so short that even the July 2019 target date is unrealistic.

**Question 9: Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why**

Due to the extent of changes required and the need for Agency Banks to engage with aggregators, the Bank considers there to be insufficient time under current proposals to implement and test the necessary changes to introduce CoP within the deadlines currently proposed.

Mainstream banks have only recently been advising Agency Banks of the actions they will need to take and clarification is still required in many areas.

As many Agency Banks have not yet engaged an aggregator, timescales involved in securing a contract and then testing the new process are unachievable, as just securing a contract can take many months. With many Agency Banks likely to be using the same aggregators, there will inevitably be bottlenecks and delays.

In targeting the key areas of fraud risk first, the Bank would recommend a two phased approach whereby the larger PSP's with current account customers implement in a first tranche, with other lower risk PSP's to follow at a later date.

A more realistic deadline for the lower risk PSP's would be 18 months (i.e. Jun 2020) to allow sufficient time for all the practicalities to be worked out, to allow time for all Agency Banks to work with aggregators, and to allow budgets to be adjusted accordingly.

If this is to be successful then it must be implemented properly and not rushed through. Despite it having been talked about for some time, certain of the finer details remain unclear, for example, how will global indemnities or trading styles/names be considered by banks as opposed to just legal entity names. Customers do make payments to trading styles and this is not always held alongside a bank account, but such payments must not and should not be rejected.

**Question 10: Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

We do not have an alternative response and are not opposed to the issuance of directions, subject to appropriate timescales and our views on implementation approach as set out in the response to Question 9.

**Question 11: Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

The benefits appear to be predicated on the assumption that, currently, one of the parties has not met their duty of care in processing payments. In the majority of instances this is not the case. As a business we do not experience many incoming payments that are not destined for us, but those we do cost us in time of investigation required to return funds quickly and efficiently.

**Question 12: Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

The costs will vary dependent on how each PSP operates, but the engagement of an aggregator for example will be an ongoing cost that is difficult to determine at this moment. As many PSPs will already have effective fraud processes in places, making these changes will deliver little long term benefit.

**Question 13: Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

The Bank has no further comment in respect of this question.

**Question 14: What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits? Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

The Bank has no further comment in respect of this question.

**Question 15: Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

The Bank is not certain that the directions will have a significant positive impact on vulnerable customers, because scammers are likely to flex in response to the change and find ways around it. This is particularly the case if these customers become liable rather than the bank, if they fall victim to a scammer finding such a way to circumnavigate CoP.

**Additional comments:**

Key issues such as invoice discounting / factoring accounts have not been considered and remain unresolved. For such accounts, invoice payments will be collected by a firm other than that to which they are addressed, due to the factoring / discounting arrangement. Such arrangements are likely to be compromised if CoP in its current form is implemented.

From an operational perspective the introduction of CoP may result in unnecessary additional customer communication to the payee if PSPs are not able to accommodate different trading styles.

# Societe Generale

# Consultation on general directions on implementing Confirmation of Payee

## Why are we consulting on directions?

### Question 1

Is giving directions under section 54 of FSBR to PSPs requiring them to introduce CoP the right approach to securing our objectives, to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?

### Answer

Giving direction is the only viable action available as without clear and unambiguous instructions, to which all PSP's must adhere, then PSP's will simply act in their own interests and ignore the issue of Authorised Push Payment (APP) fraud. They will do this by deciding not to invest in the CoP service on the basis that under The Payment Services Regulations 2017 (PSR 2017) they have zero liability for transactions that a customer has properly and correctly authorised.

The CoP service is a development that puts the interests of customers first by delivering a service that is entirely to their benefit and for this reason CoP as both an anti APP fraud initiative and a customer centric solution should be uniformly adopted by PSP's.

Furthermore, the universal adoption of CoP by all PSP's will ensure that a level playing field is maintained throughout the entire payment services market, which will benefit all retail, business and commercial banking customers. If adoption of CoP is not universal, then those organisations that have a significant retail and business banking activity will gain an unfair advantage in the commercial banking market through the simple extension of the CoP service developed for the retail market at minimal cost. If it were to be decided that the adoption of CoP by a PSP is a commercial (i.e. discretionary) decision, then such an approach would be anti-competitive and distort the payment services market, contrary to the objective of having a properly functioning and competitive marketplace in payment services for all customers.

## The proposed scope of the directions

### Question 2

Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?

### Answer

The target is to identify 3<sup>rd</sup> party beneficiaries from their account details and for PSP's this means that it is 3<sup>rd</sup> party payments which are of interest. It would follow then to apply the same exceptions for bodies and transactions exempted under Regulation 3 and Schedule 1, Part 2 of The Payment Services Regulations 2017 in order that where a PSP exclusively settles internal transactions within their organisation and/or bilateral transactions (such as securities/market settlements) with known counterparties, then such PSP's would be exempted as there is no 3<sup>rd</sup> party beneficiary involved in their transactions and using CoP would not add value.

### Question 3

## Consultation on general directions on implementing Confirmation of Payee

Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?

### Answer

Yes, the community of PSP's should be obliged to respond to CoP request's as any gaps in the service will undermine its credibility, destroy confidence in its ability to deter APP fraud and reduce the value of CoP. As the service is specifically designed to benefit customers and not PSP's then all PSP's should be required to provide a response as this will meet the objective of delivering both a positive confirmation and a degree of reassurance to the customer initiating the payment, whilst also demonstrating the value of the service.

### Question 4

Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?

### Answer

The requirements for CoP apply to the capture of beneficiary party information, which can occur before the settlement routing is chosen, and so the service must be universally adopted by any PSP that settles 3<sup>rd</sup> party payments via either CHAPS and/or FPS, as both schemes support the settlement of 3<sup>rd</sup> party payments.

Customers should also be given the reassurance that they are receiving the same level of protection whether the funds are to be settled via CHAPS or FPS as irrespective of which scheme used to settle their instructions the outcome should be the same.

If CHAPS were to be excluded from the scope of CoP, then the customer perception would quite rightly be that CHAPS is a less secure scheme than FPS even though CHAPS and FPS provide an equivalent service.

As an organisation it would be impossible for SG to treat transactions destined for settlement via CHAPS any different to those destined for settlement via FPS, the reason for this is that the beneficiary party must be created in our online banking channel prior to the capture of a payment instruction and determination of the settlement routing only occurs during execution of the payment instruction.

### Question 5

Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?

### Answer

Validation via a CoP requests is only necessary when beneficiary party details are being created or modified. Once validated any stored beneficiary party details can be used without the need for a further CoP request. Any modification of stored details should result in a further CoP request to validate the modified information.

### Question 6

## Consultation on general directions on implementing Confirmation of Payee

How should any directions deal with the potential for people to opt out of the CoP process?

### Answer

Providing the ability for people to opt out of the CoP service is of highly questionable value. Any gaps in the CoP service will undermine its effectiveness and destroy value and considering that the beneficiary party will have already provided their account details to the remitting party then I see no practical reason why they should then choose to opt out of the CoP step in the payment initiation process. If someone wishes to receive a payment from a 3<sup>rd</sup> party, then they must participate in the CoP service.

### Question 7

Should any directions cover the sending of money from both individual and business accounts?

### Answer

APP fraud is endemic in the business and commercial banking market and the deployment of the CoP service will greatly assist businesses of all sizes in combatting the threat of APP fraud. The CoP service must be applied to the entire payment services market as APP fraud poses the same degree of risk to all customers whether they are retail, business or commercial. The later phases extending the CoP service to support an offline/bulk validation service covering salary and bulk payments is essential as CoP will clearly be a powerful tool for companies to use in combatting the rise of APP fraud.

## The rationale for our timeframe

### Question 8

Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?

### Answer

Any directions should cover both sending and responding. CoP must be viewed as a single service that should be universally adopted to avoid creating gaps that will undermine credibility and destroy value. If an organisation were to make a commercial decision regarding their level of participation (or not), then this would create a two-tier structure creating distortion in the payment services market and hand an unfair competitive advantage to full participants.

### Question 9

Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.

### Answer

The deadlines included in the consultation are very short, and as we are not participants in the UK Open Banking implementation then it is highly unlikely that we would be able to meet them. The workload for 2019 is already very high with the focus being the implementation of the European Open Banking and SCA/RTS requirements and so we would unlikely be unable to implement CoP

## Consultation on general directions on implementing Confirmation of Payee

before September 2019. Another complication in determining our workload is that the UK Open Banking implementation currently deviates from the European model and as a result the CMA9 have been handed a competitive advantage over other PSP's with regards to the implementation of CoP.

### Alternative approaches

#### Question 10

Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?

#### Answer

CoP is unique in that it is designed around the needs of customers as opposed to the needs of the financial services industry and as a concept it will provide customers with visibility and an opportunity to avoid APP fraud. If there was an effective alternative to combatting APP fraud then it would already have been identified and proposed, but at this time there isn't, and the results are that APP fraud is endemic.

Whilst currently there is no effective alternative to CoP, the RTGS renewal and NPA projects do offer an opportunity to incorporate the use of a mask/label containing legally verifiable information such as LEI's for corporate entities or passport, NI or tax identifiers for individual persons and this would also effectively tie an account to an entity/person.

### Cost Benefit Analysis

#### Question 11

Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

#### Answer

I believe that the losses attributable to APP frauds are a significant underestimated as they do not include the losses being incurred by commercial organisations. Also, if CoP is not universally adopted then the erosion of benefits will be significantly higher as customers will lose faith in the service.

#### Question 12

Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

#### Answer

The universal adoption of CoP will create a competitive market for aggregators to offer a service and allow PSP's to make a competitive choice regarding the architecture of their implementation of CoP. This will have a positive effect on costs for smaller PSP's.

#### Question 13

## Consultation on general directions on implementing Confirmation of Payee

Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.

### Answer

No comment to make

### Question 14

What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?

### Answer

The deadline is challenging, but CoP should absolutely be implemented in 2019, but possibly in line with Open Banking SCA/RTS requirements?

## Equality Impact Assessment

### Question 15

Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and complying with its public equality duty, in deciding whether to give directions and considering alternatives?

### Answer

No comment to make

# SWIFT



# **SWIFT's response to the Payment Systems Regulator's Consultation on general directions on implementing Confirmation of Payee**

**SWIFT**

**04 January 2019**

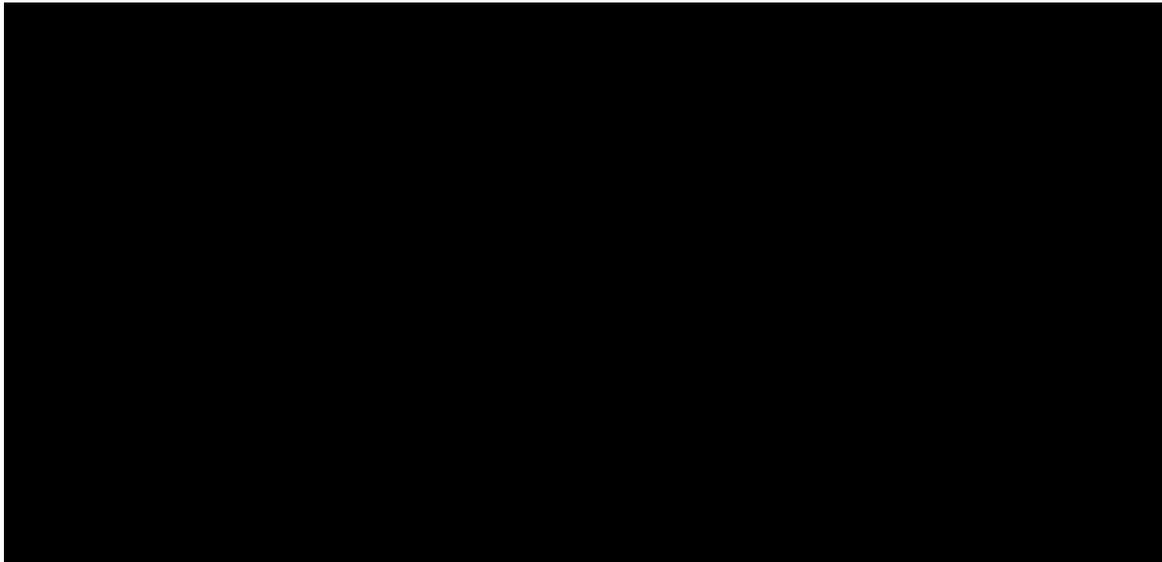
**Confidentiality: Public**

SWIFT thanks the Payment Systems Regulator for the opportunity to provide comments on the Consultation on general directions on implementing Confirmation of Payee.

SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholders, comprising more than 2,000 financial institutions. We connect more than 11,000 institutions in more than 200 countries and territories.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response, please do not hesitate to let us know.



## Chapter 4: The proposed scope of the directions

### **SWIFT comments:**

SWIFT believes that Confirmation of Payee (CoP) will be most successful if it is introduced widely, to ensure it is available to verify a payee's details for any transaction. As a result, the greater the number of PSPs sending and responding to requests, the greater the chance that CoP's benefits will be widely felt.

As developed by the Forum and then Pay.UK (with industry participation), the current specification of CoP does not require CoP solutions to be provided for all transactions. In the current proposal on which the PSR seeks views and evidence, it excludes from scope any transactions to which the current specifications do not apply. These include transactions where the payment is not routed by sort code and account number, i.e. where a payment will be routed via IBANs or BICs.

As IBANs and BICs are used in the CHAPS payment system the above would automatically exclude all CHAPS payments. We don't believe this is the intention, as previously CHAPS was explicitly included within the scope of CoP. We therefore recommend this exclusion be removed or further clarified.

In addition we note a UK IBAN includes the sort code and account number which therefore makes their exclusion difficult to understand. We suggest IBANs are included as this would make the adoption for internationally submitted retail payments easier to accommodate at a later stage.

### **Other SWIFT considerations:**

For cross-border international payments SWIFT is developing a capability to check account validity. This service will allow the payer's bank to verify that the destination or beneficiary account at the beneficiary bank is correct. This will improve straight-through processing and reduce delays in international payments. Integration of this new service with existing and forthcoming domestic account-validation services will further increase the value for bank community customers globally. To ensure interoperability between various domestic and international solutions it is important internationally accepted business and technology standards are used when implementing such solutions. We believe the proposed Pay.UK implementation based on Open Banking standards is a good example permitting such interoperability.

----- END OF DOCUMENT -----

# Transpact

**To:** [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)  
**Subject:** Response to CP18/4: Consultation on general directions on implementing Confirmation of Payee

---

Dear PSR,

I am writing with my firm's response to the PSR's consultation CP18/4: Consultation on general directions on implementing Confirmation of Payee (<https://www.psr.org.uk/sites/default/files/media/PDF/PSR-CP-18-4-consultation-general-directions-confirmation-of-payee.pdf>).

My firm's comments are as follows:

- a. We do not understand why the proposed orders that the PSR proposes includes FPS and CHAPS payments, but not BACS credit payments.  
BACS credit payments are fully included in Pay.UK's Confirmation of Payee (CoP) solution and operation, and it seems destructive to CoP (by allowing a huge BACS credit loophole) to allow BACS credit payments to be able to avoid mandatory CoP inclusion.

All that will occur if BACS is not included in the PSR's direction is that fraudsters will shift to instructing vulnerable victims to set up payments to them by BACS (which includes setting up Standing Orders) and APP Fraud (Authorised Push Payment Fraud) will continue unabated.

Fraud prevention is only as good as the weakest link in that prevention, and leaving a fraud doorway wide open by not including BACS will drive a 'Coach and Horses' through the ability of CoP to prevent APP fraud.

Please, please reconsider, and extend the direction/order to BACS credit payments.

- b. Given the epidemic scale of APP fraud in the UK, we do not believe that the implementation of CoP can come quickly enough.  
We would like the PSR to actively encourage (but not mandate) PSPs and banks to implement CoP to their customers where they can between 1 April 2019 and 1 July 2019, and not wait for the July 2019 deadline.

It is clear that banks and PSPs have had ample time to plan to implement CoP by April 2019, and are able to do so if they wish (although they will grumble, and make strong representation to delay).

Large banks do not wish to implement CoP, and have been dragging their heels for at least three years to try and push the start of CoP into the long-grass, and if the PSR listens to the large banks' excuses at this time then the large banks will never be ready to actually begin CoP (as those excuses will always be pertinent).

But it is also clear that the deadline of April 2019 to respond to CoP requests is easily within the grasp of large banks if they choose to cooperate, and it is not technologically difficult for them to easily achieve this date (although it will be expensive for them).

So the PSR should strongly resist the vehement representations from the large banks

trying to push off the April 2019 deadline.

Such protests are not technologically based, nor data based, but purely down to reluctance and cost. That is why the PSR's intervention is so important.

c. Question 1) -

We believe the PSR would be correct in giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP, in order to secure the PSR's objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible.

In fact, not to do so would be a significant failure by the PSR, and would be viewed historically in perpetuity as a significant mistake.

There are no other comparable approaches that the PSR can take that will bring CoP to market, as any other approach will provide banks and PSPs with a reason or excuse not to implement CoP for as long as possible.

Every month's delay to CoP impacts tens of thousands of additional UK consumers and businesses, often with life-changing (and sometime life-ending) negative consequences.

For other factors related to Question 1) – Please also see a) and b) above.

d. 4.2 of the consultation mentions payments routed by IBANs or BICs.

Since GB IBANs are simply an account number and a sort-code concatenated with extra check-digits, it is important for the PSR's direction to explicitly state that a GB IBAN is within scope of the PSR's direction.

Otherwise, the direction could be easily sidestepped just by quoting a GB IBAN instead of the identical sortcode and account number.

e. All payments to a payee with a unique sortcode and account number must be within scope.

This must be so, even if the payee's bank makes outbound payments through a HOCA account.

The PSR's direction must be drawn up with this in mind.

To illustrate, if you take a pseudo-bank PSP such as Tide.co or Revolut.com as an example (and there are many others), these own their own sort code – and are certainly within Phase 1 of CoP, as their clients' accounts are addressable with a bank account number and a sortcode (payments can be made directly to such accounts, by quoting their unique sortcode and account number).

However, these ASPSPs also use a sponsor's HOCA (all outgoing payments, for example, are made through the sponsor's HOCA).

Such accounts and ASPSPs must be included within the PSR's direction, as they are within Phase 1 of CoP and there is no reason to not include them in the PSR's direction (omitting them would allow largescale fraud – see f) below).

f. Question 2) -

It is critical that for CoP to be effective, all ASPSPs must be mandatory participants in CoP's introduction.

To allow any tranche of ASPSPs not to have to participate will simply allow fraudster to

work around and circumvent the critical fraud-reduction of CoP.

There is no reason that any ASPSP of any size or complexity should not be forced to join – small players do not have a significant cost to implement as they have agile IT systems (and CoP is simply an API call and response technologically), and large legacy players have a critical need to ensure their customers are safeguarded and treated fairly due to their large customer size and excessive current APP fraud levels (and to reduce their own money-laundering of the results of APP Fraud, which also results from lack of CoP).

See also a) and e) above, and h) below.

- g. Question 3) AND Question 8) -  
Phase 1 of CoP does not include PISPs – only ASPSPs.

All ASPSPs must be included in the requirement to both send and respond to CoP requests.

As soon as CoP is capable of taking requests from PISPs in Phase 2 of CoP, then PISPs must be mandated from that point by the PSR to also make CoP requests (although the PSR should give thought in such a circumstance, where a payer customer is creating a new payee through a PISP, as to whether it is the PISP or the payer's ASPSP who is required under the PSR's direction to make the CoP request. We actually believe it would be preferable if it were the Payer's ASPSP and not the PISP, but this may be deemed to interfere in the PISP handling the paying customers journey in contravention of the Payment Services Regulations 2017).

- h. Since CoP is a separate and distinct overlay service to FPS and CHAPS, it makes no sense to exclude Indirect participants from the direction.  
Whether a PSP is a direct or indirect participant makes absolutely no difference to their CoP participation, and it is critical for both to be included in the direction.  
If not, fraud will not be reduced by the introduction of CoP, and fraudsters will simply move to the many indirect participant PSPs.

- i. Question 4) AND Question 5)

See a) above.

CoP should be introduced for a FPS and CHAPS and BACS (credits).

All channels should be in scope.

And it is important in the PSR's direction that it be recognised that one-off payments that are not made to existing payee mandates have an implicit payment mandate being set-up. This should be stated explicitly in the direction, to prevent a loophole being introduced which would otherwise allow such payments without CoP to be mistakenly outside the direction.

- j. Question 7) -  
CoP has been designed for both business and personal accounts (both at the payer and the payee end).  
There is no reason not to mandate for both types of account, and not to do so would

permit fraudsters to continue to defraud both.

It is imperative that both types of accounts (business and personal) are included within the direction.

k. Question 9) -

ASPSPs have known about the CoP draft deadline for a significant time – it has been discussed in the industry since the PSR first proposed the mandatory introduction of CoP (and for some years before that, since the inception of the PSF).

Further, all ASPSPs are technologically and datawise capable of meeting the proposed timelines, if they wish.

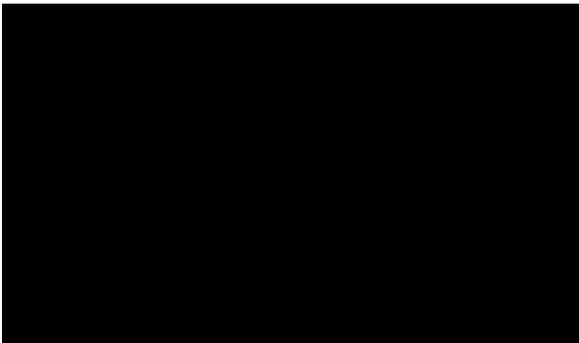
There are ASPSPs which will declare to the PSR that they will not be ready – but whatever date the PSR proposes, those ASPSPs will provide high-level similar responses and provide convincing but bogus reasons as to why they will not be ready.

The truth is those ASPSPs fear CoP, and will never be ready to introduce it unless the PSR issues its direction – only then will those ASPSPs be ready.

l. Question 10) -

There are no alternatives to the PSR's direction that will reduce the current epidemic of APP Fraud.

Please let us know if you require any clarification or further information.



TSB Ltd



**TSB Ltd Response to:**

**PSR Consultation on general directions on  
Implementing Confirmation of Payee  
(November 2018 – CP 18/4)**

**January 2019**



## Table of Contents

Table of Contents.....	2
Executive Summary.....	3
TSB Response to Individual Questions.....	4
Question 1:.....	4
Question 2:.....	6
Question 3:.....	7
Question 4:.....	7
Question 5:.....	8
Question 6:.....	9
Question 7:.....	10
Question 8:.....	10
Question 9:.....	10
Question 10:.....	13
Question 11:.....	13
Question 12:.....	14
Question 13:.....	15
Question 14:.....	15
Question 15:.....	16



## Executive Summary

TSB supports the implementation of Confirmation of Payee (CoP) at pace to improve end-user protection against fraud and misdirected payments and is committed to ensuring that the service is delivered safely and effectively to our customers and the wider industry.

TSB is also supportive of the principle of giving directions to PSPs, requiring them to introduce CoP, as this will provide certainty to the market through a legally binding and common target and allow greater industry alignment, a controlled implementation and the maximisation of benefits to customers.

TSB are concerned, however, that implementing changes to the proposed timelines would be extremely challenging (if not unachievable) due to insufficient industry capacity for change as well as concerns over the scope and readiness of key supporting industry capabilities (standards, infrastructure, co-ordination and vendor readiness). Delivering against the proposed timelines could therefore result in an inconsistent and unreliable experience for the customer, undermining user trust and potentially limiting the effectiveness of CoP.

TSB also are concerned that proposed plans could also have an adverse effect on competition and innovation by disproportionately impacting the capacity and quality of smaller PSPs, during a time of significant regulatory, mandatory and industry change for PSPs.

While TSB are largely in agreement with the nature of costs and benefits proposed by the PSR, we believe that the PSR's cost-benefit analysis is overly positive and does not take account of some key assumptions and incremental costs implied in an effective delivery of CoP. TSB would also question whether the cost-benefit trade-off applies equally to all PSPs and payments types/channels/users.

TSB therefore suggest that, to support a more robust and effective implementation, deliver improved customer outcomes and achieve an appropriate trade-off of costs and benefits, consideration is given to a credible and realistic, phased approach for implementation. Such a phased approach would follow the principle of allowing for the most significant sources of detriment to be tackled first and would allow for a period of industry stability, co-ordination and testing. For instance, the phased approach could:

- focus on FPS transactions in the first instance, followed by CHAPS at a later date;
- focus on direct participants first, but that the timeline for subsequent inclusion of all PSPs remains as short as possible;
- focus on online and mobile payment channels first;
- focus on individual and SME accounts first; and
- limit the direction (in the first instance) to the ability for PSPs to receive and respond to CoP requests



## TSB Response to Individual Questions

### Question 1:

**Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

TSB is supportive of increased protection of customers from the risks of APP Fraud and misdirected payments. Consequently, TSB is supportive of the proposed Confirmation of Payee (CoP) service and its potential to address these risks and is committed to ensuring that the service is delivered safely and effectively to our customers and the wider industry.

TSB supports the principle of giving directions to PSPs, requiring them to introduce CoP, as this will provide certainty to the market through a legally binding and common target and allow greater industry alignment, a controlled implementation and the maximisation of benefits to customers.

However, the scope and timeframes of any direction need to be credible and realistic to allow effective implementation that avoids customer detriment and disruption and does not unintentionally shift fraud risk & liability to other channels, payments types or participants.

TSB does not believe the currently proposed timeframes are achievable based on a number of factors:

#### 1) Industry Change Capacity

The current level of regulatory/mandatory and industry change and consequent demands on UK PSPs is significant and, as a result, the capacity and capability of both TSB and the wider industry to implement a new regulatory mandate in the first half of 2019 is extremely limited – this is particularly true for smaller PSPs.

The demands of PSD2 (particularly for firms outside the Competition and Markets Authority Retail Banking Market Investigation Order, such as TSB, who are currently implementing PSD2 requirements at pace, but at a later stage than the CMA9), delays to the roll out of the Image Clearing Service (ICS), and the Structural Reform requirements for TSB are all forecast to consume significant resource within TSB through to the end of H1 2019.

In addition, TSB would like to ensure that capacity is left for PSPs to be able to make the changes that are required ahead of and following the UK's exit from the European Union, which may vary depending on the terms of the UK's departure. In line with this, TSB would also ask the PSR to note the ongoing consideration of industry change freeze periods on/around the 29<sup>th</sup> March exit date

#### 2) Implementation Risks Relating to Stability & Availability of CoP Standards

The standards developed by Pay.UK are critical in ensuring a consistent implementation and customer experience. However, TSB do not currently believe that the standards are sufficiently stable or comprehensive to allow for an effective implementation of CoP. The current rules and guidelines are insufficiently detailed, and do not resolve a number of outstanding questions on scope/coverage, making it difficult for PSPs and vendors to build and deliver solutions that are fit for purpose and consistently applied to/by the market.

As a result, there is a risk of introducing a solution that lacks the necessary ubiquity, reliability or quality and could cause alarm and distress for customers which may hinder adoption/usage and realisation of the benefits.



Furthermore, the availability of the standards remains an area of industry concern with differential flow of information to indirect participants and vendors inhibiting industry development.

TSB also understand that the ICO is yet to provide final agreement (to Pay.UK) regarding the compliance of the proposed standards/solution against GDPR requirements.

### 3) **Vendor Availability & Procurement**

Leading on from the ambiguity of the rules and guidelines, vendors remain in the early stage of their solution development with many still in the process of building out solutions and/or running Proof of Concepts to test their solutions (e.g. for example, TSB is engaged with one vendor who are running a Proof-of-Concept which is not due to complete until mid/late February with no committed dates for a live service).

The lack of clarity around the matching rules and mechanisms makes it difficult to build and offer a fully developed (compliant) solution, thereby limiting the competitiveness of the market.

Furthermore, the capacity of the vendor community to support market-wide adoption of CoP remain unclear and there is a risk that smaller PSPs may be disadvantaged (commercially or operationally) if vendors are unable to support their needs in a timely and effective fashion.

While TSB has yet to make a decision on the use of vendors to meet our CoP aspirations/obligations, the selection, due diligence and onboarding of any potential vendor would be extremely challenging to achieve within the proposed timescales, particularly given the sensitivity and security requirements of any information/data sharing agreements required and the potential liability models arising from the use of a CoP service.

### 4) **Industry (OBIE) Readiness**

Key requirements for the proposed API-based architecture remain insufficiently mature to support an effective implementation.

For example, the ability of and terms of usage for smaller PSPs and/or vendors to gain access to the Open Banking Directory (for the sole purpose of supporting CoP) is currently constrained and the impact of any future changes to the Directory (including but not limited to the switchover to eIDAS certificates) remains unclear. It is also unclear as to the level of resource availability within OBIE to support CoP development given the demands of PSD2 delivery during 2019.

It is also worth noting that the longer-term ownership/governance/liability/funding of OBIE remains uncertain and there is a risk of creating a dependency on market infrastructure that may not fully align to the needs of CoP and the wider payments industry in the long-term.

### 5) **Industry Co-ordination & Testing**

Whilst a direction may be helpful in providing certainty to the market, giving all PSPs a legally binding and common target and will provide the momentum and pace needed, further consideration needs to be given to understand how industry co-ordination will be managed and delivered, including a focus on industry testing and co-ordinated rollouts (particularly if the delivery is phased). There is currently no central point of industry co-ordination around delivery of CoP and no process for addressing any exceptions, issues (e.g. high-level of no/partial-match or service unavailability) or concerns in a consistent and transparent manner across the industry.

In the absence of central co-ordination, there is a risk that implementations will be inconsistent, network issues are not identified and resolved, unintended risks and consequences emerge, and customer confusion and detriment would result.



It is important that a period of industry testing is enabled before the service is delivered to end users. This will help to ensure that the matching algorithms can be appropriately tested, and industry-wide performance be assessed before launch. This is particularly vital when the customer experience of a TSB customer will be largely dependent on the accuracy and performance of other PSPs CoP services.

TSB acknowledge the ongoing discussions between UK Finance and Pay.UK regarding this matter but would draw attention to the managed rollout activity of both the ICS programme and Open Banking as recent examples of the value and importance of industry co-ordination.

### **Proposal for a Phased Approach**

TSB believe that the use of a direction should be limited (in the first instance) to the ability for PSPs to receive and respond to CoP requests. This would ensure the necessary ubiquity and coverage of the service to allow for an effective and consistent customer experience.

The ability to send requests could therefore become an innovation & competitive matter for banks themselves to determine which accounts and which types of payment are suited to a confirmation of payee request. This would also allow for a period for the industry and individual PSPs to ensure that the CoP responses are sufficiently stable/consistent and effective before directly exposing the service to customers. In time, the adoption of the Contingent Reimbursement Model will likely drive a commercial incentive for PSPs to introduce the 'send' capability (see Response to Q10). However, should this be delayed, or adoption becomes slow/inconsistent, then a further direction may be required to ensure ubiquitous adoption of the CoP service.

Consideration should also be given to a phasing of the direction across channels and payments types that allows for the most significant sources of detriment to be tackled first. However, this must be rigorously assessed against the risk of displacing the fraud and customer detriment to other payment environments.

In summary, if it is deemed necessary, a direction needs to be given that is achievable by all industry participants (PSPs and solution vendors) and minimises the risk of disruption to customers. A poor execution (lack of ubiquity, inconsistent implementation, false negatives/positives, etc), could encourage customers to 'dismiss' or lack trust in a CoP request therefore reducing its ongoing credibility and realisation of the proposed benefits.

PSPs need to be confident that the solution they deliver is fit for purpose and one that customers will trust and use. Furthermore, TSB and other PSPs will be dependent on the accurate and effective implementation of CoP across the industry. TSB, as well as other PSPs, will need to ensure a fully comprehensive solution is in place, with a consistent and reliable matching rate – failing to achieve this could leave PSPs with a negative reputation and could result in poor customer experiences.

TSB believe that any implementation date that falls ahead of the PSD2 RTS implementation timetable would introduce risks and challenges that would outweigh the benefits.

### **Question 2:**

**Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

TSB broadly supports giving directions to all PSPs sending or receiving FPS and/or CHAPS payments, as this will allow for ubiquity and consistency across the industry and maintain a level-playing field for all PSPs.

TSB agree that the direction should apply to those who are both direct and indirect participants of FPS and CHAPS but acknowledge, and are supportive of, the challenges faced by indirect



participants in implementing CoP (e.g. implementation capacity and lack of visibility around guidelines and rules from Pay.UK, vendor support, etc). With this mind, we would be supportive of consideration being given to a phased approach with an initial focus on direct participants, but that the timeline for subsequent inclusion of all PSPs remains as short as possible.

In the event of a phased approach, further consideration should be given to the impact on the out-of-scope PSPs (e.g. displacement of fraud risk/impact, reputational impact, etc) as well as the customer experience challenges driven by having a sub-set of PSPs that will not be CoP enabled (i.e. the guidelines need to explicitly clarify what is meant by 'account not reachable' and any clarification around exemption towards the CRM must be resolved beforehand).

### Question 3:

**Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

TSB believe that a direction should only apply, in the first instance, to a respond/receive request and therefore do not agree that the same PSPs should also be given a direction to send a request.

The ability to receive/respond to a request is the pre-requisite for market ubiquity and sending can be more a matter for innovative & competitive provision. It should be up to a PSPs to decide when/where they support a send request in line with their fraud/risk appetite (linked to the obligations arising from the proposed CRM) and approach to customer experience. The shifting of liability (under CRM) for institutions not implementing the send capability will likely provide a commercial driver for implementation provided the CRM is widely adopted and an effective process is delivered for the recovery of funds between participants under the liability model.

To allow for consistency and a controlled industry implementation any direction applied should be clear, consistent and easy to follow.

### Question 4:

**Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

TSB supports the proposal to apply directions to both FPS and CHAPS transactions in the first instance.

TSB currently supports FPS transactions across all channels (branch, telephony, internet/mobile), whereas CHAPS payments are currently only available in branch and are therefore keyed/entered by Bank Staff not the customer and are subject to additional charges and fraud checks. As such, the question of channel scope (Q5) is critical to the likely coverage of CoP within TSB.

TSB's view is that the main risk of APP fraud and misdirected payments is currently related to FPS payments. Therefore, TSB would be supportive of consideration being given to a potential phasing of directions to focus on FPS transactions in the first instance, followed by CHAPS at a later date.

TSB would also request clarity in any direction as to the scope of sub payment types covered. For example, within the scope of FPS transactions, would a direction apply to Forward-Dated Payments [FDPs] and Standing Orders [SOPs] in addition to Single Immediate Payments [SIPs]? There is a risk that for Forward-Dated Payments and Standing Order Payments, the asynchronous nature of these payments creates a time-lag between the mandate/instruction being created and the payment being processed.



Similarly, for CHAPS payments, it is important to differentiate the use of CHAPS for retail and wholesale purposes.

In the longer term, TSB would prefer to see regulation that is agnostic to payment type or providers broader coverage the consultation proposals. However, TSB would not support the inclusion of further payment types (beyond FPS & CHAPS) in any initial direction. PayM transactions already invoke a form of account name confirmation and other 'core' Sort-Code/Account Number push payment types (e.g. Bacs) involve significant further complexity which would make the introduction of Confirmation of Payee extremely challenging and likely see the costs outweigh the benefits.

TSB would also request guidance on whether CoP is expected to be applied (now or in the future) to push payments that are not addressed to Sort-Code/Account Number (SCAN) destinations? For example, a number of card (PAN-based) push-payments solutions are being brought to market (e.g. Visa Direct/Mastercard SEND) and multiple Fintech/overlay solutions exist that use alternative identifiers/proxies (email address/usernames/hashtags) for addressing.

Lastly, it is worth considering the challenges that could arise from applying CoP to certain account types. For example, HOCA accounts or Client Money Accounts whereby the account name returned by a CoP-service may not be directly attributable to the ultimate payee.

### Question 5:

**Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

Careful consideration needs to be undertaken to determine which channels the directions should apply to. TSB believe any proposed direction should apply to all payment channels (where possible) but subject to a phased implementation with online (internet) and mobile payments addressed in the first instance.

Failing to apply the direction to all channels could provide fraudsters with an opportunity to exploit those channels which are not in scope. However, this drives a consequent trade-off with the timelines for delivery. Applying CoP to all payment channels (as opposed to, say, online/mobile channels only) will increase the complexity of the delivery and, by consequence make any short-term deadline even more challenging.

At this stage, it is important to highlight the challenges in applying CoP to channels with no customer-facing graphical user interface (GUI) and the lack of rules, standards and clarification for 'human-intermediated' channels and customer experiences where a bank member of staff would likely be keying the payment instruction – e.g. branch/telephony. If the direction is to apply to all channels, then the Pay.UK rules & standards need to be further developed to address the requirements and complexity of these additional payment channels as the current standards only focus on digital and online platforms thus making it difficult to build a solution that will benefit customers across all payment channels. Furthermore, even within these additional channels there are customer experiences that are automated or semi-attended (e.g. IVR, branch self-service) which may require special consideration.

It should also be noted that application of CoP to payment-initiation channels where the PSP does not have full control of the user experience also create additional challenges. This is particularly important for the emerging Open Banking PISP customer journeys where PSPs have received clear guidance from the EBA & FCA to minimise 'obstacles' in the PSP-controlled elements of the user journeys. The current OBIE user-experience guidelines make no account of any CoP steps where a payment is made via a PISP (to either an existing or new mandate). Not applying CoP to this channel may create a risk of displacing fraud risk to a relatively immature channel and one where customer uncertainty



will be relatively high (in the near-term). Bearing in mind the limited (or costly) ability for a PSP to recover funds from PISPs in the event of fraud and the lack of clarity as to the application of the CRM to these emerging payment environments, this is an area of particular concern to TSB. Additionally, not applying CoP to these payment channels will create a non-level playing field between bank and third-party customer experiences which is contrary to the underlying principles of the PSD2 legislation. Additional guidance in this area is requested as a matter of urgency.

Furthermore, it would be useful to understand what considerations, if any, have been taken to address new and emerging channels that are not yet mainstream (e.g. voice, chatbot), but where application of CoP may be challenging. Although this may not apply to an initial phase of directions, TSB would request further thought be given to alternate channels that CoP could potentially apply to and how the industry would migrate to cover these additional channels.

As stated previously, TSB believes that it should be at the discretion of the sending Bank to decide whether to apply CoP to a new/changed and/or existing mandate (e.g. as a “step-up” mechanism where there is heightened risk of fraud). As noted above, TSB believe it is important to keep this aspect of CoP competitive.

TSB would welcome further clarification on the approach to apply CoP to mandates already in existence before the introduction of CoP. There is a risk that any public communication of a fixed date for the launch of CoP (e.g. through directions or otherwise) may drive fraudsters to register accounts and target customers to create mandates ahead of the deadline thereby taking these accounts out-of-scope from the proposed approach to CoP.

In addition, payments made to existing mandates (from both before/after any implementation date for CoP) would still fall under the scope of the Contingent Reimbursement Model and it is unclear whether a PSP would have met its duty-of-care should CoP not be applied in these circumstances (as is proposed). TSB would suggest that consideration be given to a periodic or step-up approach (based on time and/or transactions volumes/values) be considered for ongoing CoP checks to ensure that CoP remains an effective mechanism for preventing fraud and misdirected payments. That said, TSB acknowledges that the more widespread application of CoP to existing mandates (e.g. on first payment to a given mandate following the introduction of the CoP service or on a periodic basis) would drive increased friction to payment journeys, and could result in poor customer experiences, higher opt-out responses and an increase in abandoned transactions.

## Question 6:

### **How should any directions deal with the potential for people to opt out of the CoP process?**

An opt out from the Confirmation of Payee service (for either send and/or respond capability) would likely be desirable for certain customer types (e.g. where there is a need to protect their identity) or certain types of transaction, but the terms under which the customer exercised that right should be made clear. This needs to be considered carefully and the legal basis understood so that there is consistent implementation and the impacts can be appropriately assessed.

TSB believes that further consideration needs to be given to how specific groups of customers, (vulnerable, disabled, those with speech/learning difficulties), could opt out of the CoP process where deemed necessary. The current guidelines do not consider the opt out process in enough detail and we understand that Pay.UK are awaiting clarification from the ICO on whether the standards are GDPR compliant and would require any opt-out allowance from a data protection perspective.

TSB is also aware of industry payment usage (e.g. in large corporates using ERP systems, Direct Corporate Access or host-to-host systems) where FPS/CHAPS transactions are created and submitted in bulk/batch files for automated processing and where application of CoP may not be desirable or achievable.



It is also important that, should an opt out process become available for CoP, the consequent implications for liability under the CRM model are also clarified (i.e. would a bank be deemed to have met its duty of care if it offers a CoP service and a customer subsequently opts out?)

### Question 7:

#### **Should any directions cover the sending of money from both individual and business accounts?**

TSB believe that the CoP service and any associated directions should be focused on individual accounts in the first instance.

The consultation is unclear as to the definition of business accounts. Application of CoP to business accounts drives incremental challenges in name-matching for the respond capability (e.g. trading names, multi-party account names, corporate structures, etc) which largely increase in complexity with the size of the business.

Furthermore, as noted above, TSB is also aware of additional complexity in applying the send capability to certain business payment usage (e.g. in large corporates using ERP systems, Direct Corporate Access or host-to-host systems) where FPS/CHAPS transactions are created and submitted in bulk/batch files for automated processing.

TSB believe that application of CoP to SME accounts should be considered. TSB operates a SME-focused offering to sole trader and multi-director businesses. Application of CoP to these customer types would be more challenging than for individual accounts, but TSB believe that these challenges can be addressed. However, a short-timeframe direction would likely increase the risk associated with the range of coverage and accuracy of these account/customer types.

TSB believe that application to all business accounts would be desirable but acknowledge that this drives significant additional complexity (subject to detailed definition of Business accounts) and would suggest that the cost-benefit analysis of applying CoP to large corporates requires further investigation to assess the relevant trade-offs.

### Question 8:

#### **Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

As above, TSB believes that the direction should only apply to the ability to receive and respond to CoP requests. This places the sending requests in the innovation & competitive space and will give PSPs the option to send a request when they deem appropriate.

### Question 9:

#### **Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

Whilst TSB fully understand that for a customer to benefit from this service CoP must be widely introduced by PSPs, TSB believe the PSR's proposed timescales are not achievable. There are several reasons to support this view, this is also reiterated in Q1:



1) **Industry Change Capacity**

The current level of regulatory/mandatory and industry change and consequent demands on UK PSPs is significant and, as a result, the capacity and capability of both TSB and the wider industry to implement a new regulatory mandate in the first half of 2019 is extremely limited – this is particularly true for smaller PSPs.

The demands of PSD2 (particularly for firms outside the Competition and Markets Authority Retail Banking Market Investigation Order, such as TSB, who are currently implementing PSD2 requirements at pace, but at a later stage than the CMA9), delays to the roll out of the Image Clearing Service (ICS), and the Structural Reform requirements for TSB are all forecast to consume significant resource within TSB through to the end of H1 2019.

In addition, TSB would like to ensure that capacity is left for PSPs to be able to make the changes that are required ahead of and following the UK's exit from the European Union, which may vary depending on the terms of the UK's departure. In line with this, TSB would also ask the PSR to note the ongoing consideration of industry change freeze periods on/around the 29<sup>th</sup> March exit date

2) **Implementation Risks Relating to Stability & Availability of CoP Standards**

The standards developed by Pay.UK are critical in ensuring a consistent implementation and customer experience. However, TSB do not currently believe that the standards are sufficiently stable or comprehensive to allow for an effective implementation of CoP. The current rules and guidelines are insufficiently detailed, and do not resolve a number of outstanding questions on scope/coverage, making it difficult for PSPs and vendors to build and deliver solutions that are fit for purpose and consistently applied to/by the market.

As a result, there is a risk of introducing a solution that lacks the necessary ubiquity, reliability or quality and could cause alarm and distress for customers which may hinder adoption/usage and realisation of the benefits.

Furthermore, the availability of the standards remains an area of industry concern with differential flow of information to indirect participants and vendors inhibiting industry development.

TSB also understand that the ICO is yet to provide final agreement (to Pay.UK) regarding the compliance of the proposed standards/solution against GDPR requirements.

3) **Vendor Availability & Procurement**

Leading on from the ambiguity of the rules and guidelines, vendors remain in the early stage of their solution development with many still in the process of building out solutions and/or running Proof of Concepts to test their solutions (e.g. for example, TSB is engaged with one vendor who are running a Proof-of-Concept which is not due to complete until mid/late February with no committed dates for a live service).

The lack of clarity around the matching rules and mechanisms makes it difficult to build and offer a fully developed (compliant) solution, thereby limiting the competitiveness of the market.

Furthermore, the capacity of the vendor community to support market-wide adoption of CoP remain unclear and there is a risk that smaller PSPs may be disadvantaged (commercially or operationally) if vendors are unable to support their needs in a timely and effective fashion.

While TSB has yet to make a decision on the use of vendors to meet our CoP aspirations/obligations, the selection, due diligence and onboarding of any potential vendor would be extremely challenging to achieve within the proposed timescales, particularly given the sensitivity and security requirements of any information/data sharing agreements required and the potential liability models arising from the use of a CoP service.



#### 4) **Industry (OBIE) Readiness**

Key requirements for the proposed API-based architecture remain insufficiently mature to support an effective implementation.

For example, the ability of and terms of usage for smaller PSPs and/or vendors to gain access to the Open Banking Directory (for the sole purpose of supporting CoP) is currently constrained and the impact of any future changes to the Directory (including but not limited to the switchover to eIDAS certificates) remains unclear. It is also unclear as to the level of resource availability within OBIE to support CoP development given the demands of PSD2 delivery during 2019.

It is also worth noting that the longer-term ownership/governance/liability/funding of OBIE remains uncertain and there is a risk of creating a dependency on market infrastructure that may not fully align to the needs of CoP and the wider payments industry in the long-term.

#### 5) **Industry Co-ordination & Testing**

Whilst a direction may be helpful in providing certainty to the market, giving all PSPs a legally binding and common target and will provide the momentum and pace needed, further consideration needs to be given to understand how industry co-ordination will be managed and delivered, including a focus on industry testing and co-ordinated rollouts (particularly if the delivery is phased). There is currently no central point of industry co-ordination around delivery of CoP and no process for addressing any exceptions, issues (e.g. high-level of no/partial-match or service unavailability) or concerns in a consistent and transparent manner across the industry.

In the absence of central co-ordination, there is a risk that implementations will be inconsistent, network issues are not identified and resolved, unintended risks and consequences emerge, and customer confusion and detriment would result.

It is important that a period of industry testing is enabled before the service is delivered to end users. This will help to ensure that the matching algorithms can be appropriately tested, and industry-wide performance be assessed before launch. This is particularly vital when the customer experience of a TSB customer will be largely dependent on the accuracy and performance of other PSPs CoP services.

TSB acknowledge the ongoing discussions between UK Finance and Pay.UK regarding this matter but would draw attention to the managed rollout activity of both the ICS programme and Open Banking as recent examples of the value and importance of industry co-ordination.

As noted above, TSB believe that a phased approach to any directions would be preferable and that any implementation date that falls ahead of the PSD2 RTS implementation timelines would introduce risk and challenges that would outweigh the benefits.

However, without a clearly defined scope (payment types, channels, customer types) it is challenging for TSB to suggest an alternative date as the scale of the implementation, and associated cost-benefit analysis, would vary significantly.

TSB acknowledges that any delay to the implementation of CoP would create further risk of customer detriment from APP Fraud and misdirected payments. However, CoP is just one of a number of initiatives seeking to address these customer detriments and TSB considers that an earlier date would create undue costs and risks that would not be acceptable and may create additional risks of increased fraud through customer uncertainty and/or lack of customer adoption.



### Question 10:

**Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

TSB are supportive and understand that a direction to PSPs provides a helpful way to co-ordinate the market.

However, we would recommend consideration of alternative approaches that may also drive the required outcomes:

- 1) The PSR provide a phased approach to the direction to PSPs, initially focused on the respond and receive aspect of CoP, but with a timeline that is realistic and achievable, leaving the introduction of send capability to the innovation & competitive domain
- 2) The industry (e.g. through Pay.UK) could adopt a more pro-active approach to industry co-ordination and seek to set (non-regulated) deadlines for implementation
- 3) The implementation of CoP could be more closely tied to the delivery of the New Payments Architecture (NPA Core) to allow for greater efficiency of planning, co-ordination and delivery
- 4) The adoption of CoP could be left entirely in the innovation & competitive domain and the adoption of the CRM would act as a commercial driver for implementing CoP\*.

The combination of options 2&4 would be similar to the approach adopted by payment card schemes in driving the adoption of EMV and 3D-Secure in recent years where scheme transition dates and liability shifts have been effective in achieving (near) ubiquitous usage.

\*As CoP is a key requirement of the CRM model, failing to implement this could leave PSPs liable to reimburse victims of APP fraud. PSPs will be classed as failing to provide a 'duty of care' without offering CoP so this could be the driver needed by Banks to implement a solution. It is important to note that is only a consideration and is dependent on the outcome of the final code due to be released in Q1 2019.

### Question 11:

**Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

TSB does not believe that the level of benefits assumed by the PSR would be realised – either in total or within the timescales assumed.

The benefits proposed are contingent on effective, well-co-ordinated and ubiquitous delivery of CoP. As noted above, there are challenges and risks arising from the implementation that would need to be addressed, otherwise they could reduce the impact of the service in the initial months/years.

The level of benefits proposed is dependent on the ultimate scope and coverage of a CoP implementation – it is not clear what assumptions have been made in respect of the different variables raised by the questions in this consultation. For example:

- The value of APP (Malicious Redirection) Fraud assumed includes a proportion of fraud that is related to Bacs/International payments that are currently out of scope for the service designed by Pay.UK (TSB believe this to be c.£20m of the £93.9m total).
- The proposed exclusion of payments to existing mandates as well as any potential reduction in the scope of participants/payment types/channels/customers will likely further reduce the level of benefits achieved

In addition, the analysis does not take account of any technical and behavioural learning/development on the part of participants, vendors, users and fraudsters that may limit the impact of the service – both initially and over time:



- There may be technical implementation issues associated with participant/vendor delivery that may limit the early impact of the service, for example, algorithm learning. Consequently it will be a number of months before the service becomes fully effective
- The impact of CoP is also dependent on customer behavioural change. It is currently unclear to what extent (scope and/or timing) customers will refine their approach to inputting account names or the extent to which customers may choose to ignore a no/partial match response (based on lack of education/awareness or poor-matching on behalf of the receiving PSP). This risk would be further exacerbated by an ineffective industry implementation of CoP that may result in poor customer experiences
- It is well-known that fraud is not a static threat. Fraudsters will likely initially be impacted by the introduction of CoP, but it is likely that they will adapt and a proportion of the APP fraud under consideration will remain or be displaced to other environments

As a result, TSB believe that both the total and addressable value of the benefits in the PSR analysis is overstated, a 90% reduction is not realistic and the timing of the benefits realisation is overly aggressive

Alongside the fraud-reduction benefits, TSB acknowledges and agree with the proposed qualitative benefits, but would also note that these may be offset by the incremental friction associated with the introduction of CoP.

As regards mis-directed payments, TSB agree that the benefits are likely to be substantially smaller. The assumption that all misdirected funds are returned to the payer may not be true in all cases and CoP will likely only address a subset of these payments as mis-directed payments includes both CPR (Credit Payment Recovery) cases where the customer has made an error as well as BER (Bank Error Recovery) cases which will not be addressed by CoP. Furthermore, the ability for a customer to override the CoP response (e.g. for a no/partial match) will likely result in some level of continued mis-directed payments.

### Question 12:

**Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

At this stage TSB is yet to make any firm decisions on our approach to implementing CoP and are therefore unable to estimate the specific costs of implementing CoP. We are currently running or participating in a number of proof-of-concept solutions (both internal and external), but have yet to initiate or size a specific CoP implementation.

It should be noted that our ability to appropriately assess the implementation costs for CoP is further limited by the lack of a clear scope for the service (payments types/channels/customers) as well as the lack of available vendor solutions/costs.

The overall level of industry costs proposed in the PSR's cost-benefit analysis (£6-15m for a large PSP & total industry costs of £200m capital expenditure/£20m p.a. running costs) appear to be directionally correct. However, the scope and timing of any directions (including phasing if required) may influence both the scale and timing of these costs.

TSB would also expect that a reduction in APP fraud and misdirected payments would reduce existing operating costs, but this may be offset by additional costs for operating within the CRM (e.g. dispute management and recovery of funds under any liability shift).

TSB agree that campaigns for customer/staff education and awareness are important and would expect to incur costs accordingly. However, in line with our preference for industry co-ordination, we would expect that industry-level communication may also seek to address these needs. We would suggest that CASS does not provide the most appropriate comparator as (although available to the



whole market) is an “opt-in” service and therefore has different education and awareness needs. It would perhaps be prudent to consider the costs associated with other whole industry/opt-out solutions (e.g. the introduction of CHIP & PIN) to provide alternative data points.

### Question 13:

**Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

TSB believes that there are several variables that will have an impact on the trade-off between costs and benefits:

- 1) The timing, scope and effectiveness of industry implementation for CoP will have significant impact on the trade-off between the proposed costs and benefits
- 2) TSB broadly agree that CoP will help reduce APP Fraud. However, there is a risk that fraudsters will adapt their behaviour and displace fraud to other payment types or channels. Consideration and thought needs to be given as to how this risk can be mitigated.
- 3) There will likely be some phasing of the assumed benefits based on any phasing of implementation as well as the learning of participants, vendors, customers and fraudsters
- 4) There is a risk that the costs and benefits may not apply equally to all PSPs. For smaller PSPs, there is a risk that the costs if implementation and ongoing operation of CoP exceeds the additional liabilities that would be incurred in the event that CoP is not applied. However, the associated implementation of the CRM (and included liability shifts) may further affect this trade off.
- 5) The costs and benefits may not apply equally to all channels/payment types/customers
- 6) The qualitative impacts are hard to assess. CoP will drive increased confidence and trust in payments and reduce the emotional stress of fraud and misdirected payments. However, the introduction of CoP will also drive additional friction into payment journeys and this may push customers towards alternative payment types that lack the protection intended to be provided by CoP.
- 7) Communication and an effective implementation to our customers is extremely important, if the communication isn't right, there is the risk of driving unwanted customer behaviour

In summary, there are a number of factors that could impact the benefits and costs of CoP. Further consideration needs to be undertaken to understand the implied trade-offs.

### Question 14:

**What is your view on the impact of the proposed dates in our approach to the trade off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

TSB believe that implementation of CoP within the timelines suggested will likely result in higher costs (based on the uncertainty of scope and rules/standards as well as the limited availability of resources and 3<sup>rd</sup> party solutions) and a reduction to the near-term benefits resulting from the risk of incomplete market coverage and poor customer experiences.

In TSB's view, delaying implementation is likely to lead to an improved cost-benefit position, although we acknowledge that this would result in ongoing customer detriment in relation to APP Fraud.



Question 15:

**Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

At this stage, TSB has not been able to fully consider the impact to our protected groups and vulnerable customers or whether the current rules/standards sufficiently address these issues.

# UK Finance



## UK Finance response to the PSR's consultation on general directions on implementing Confirmation of Payee

4th January 2019

### Introduction

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we help drive forward positive change to enhance standards, support customers and promote innovation.

We welcome the opportunity to respond to the Payment Systems Regulator's (PSR) consultation on general directions on implementing confirmation of payee (CoP) and we would welcome the opportunity to discuss it with the PSR.

**Question 1** *Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?*

Our members support the introduction of CoP to help protect customers from authorised push payment (APP) scams and misdirected payments. The banking and finance industry is committed to making CoP a success and providing customers with the best possible experience.

A Direction could help provide certainty to the market giving all payment service providers (PSPs) a legally binding and common target – but the timeframes need to be credible and realistic to allow effective implementation and co-ordination that avoids any disruption to customers and does not unintentionally shift fraud risk, for example, to smaller firms.

The timelines currently envisaged are simply not achievable – given the demands on firms resulting from implementation of the Competition and Markets Authority's (CMA) Retail Banking Market Investigation Order 2017, the revised Payment Services Directive (PSD2), the IT freezes associated with the UK's anticipated withdrawal from the European Union on 29 March and several other industry programmes of a legal, regulatory or mandatory nature. They also do not take account of the critical dependency for many firms on vendor solutions. The capacity and capability in firms to implement a new regulatory mandate in the first half of 2019 is, in consequence, extremely limited.

Most PSPs would not be able to meet a short notice legal mandate to implement CoP. The mandate is even more challenging for firms currently implementing PSD2 requirements at pace but at a later stage than the nine subject to the requirements for open application programming interface (API) standards and data sharing in Part 2 of the CMA Order (the CMA9).

The result would be only a few firms implementing CoP, creating confusion amongst customers and a long tail of firms going live, thereby squeezing the ubiquity necessary to deliver CoP's benefits and risking customer adoption.

We would suggest the PSR work with us, our members, Pay.UK and the Open Banking Implementation Entity (OBIE) to create a timeline that ensures effective implementation without delay and allows implementation to be co-ordinated and fully tested. If necessary, implementation could be phased in a way that focusses on delivering the best possible customer outcome where the customer detriment is most apparent. We provide an outline implementation proposal below.

Co-ordination is essential to implement a new service at pace that will impact all consumers and businesses. It is needed to ensure that all PSPs – both direct and indirect participants – are informed, network issues identified and resolved, and implementations properly tested. It is also critical to ensuring that unintended risks and consequences are identified, for example, to mitigate any adverse impacts on confidential invoice discounting facilities used by around 25,000 of the UK's largest firms necessary to ensure their access to working capital. These currently rely on confidential account names that the payer could not know.

The Direction and timeline should be predicated on the following:

- A final and stable set of specifications, rules and guidelines (with the basic standards and logic, against which PSPs can establish their matching evaluation). There is a particular concern that indirect participants have not yet received all the information they need, for example, the terms and conditions for joining the Open Banking Directory for CoP only;
- The ability to receive and respond to CoP requests. The ability to send requests would therefore become a competitive matter for PSPs themselves to determine which accounts and which types of payment are suited to a confirmation of payee request (although some have made the case for both receive/respond and send to create greater ubiquity);
- The availability of vendor solutions with sufficient bandwidth to accommodate multiple implementations across the PSP community and time for firms to undertake due diligence on proposed solutions and on board a supplier. Smaller institutions have stressed this point to us throughout our discussions on responding to the consultation;
- Access to the Open Banking Directory for all PSPs caught within the scope of the Direction and clarity about the terms under which the Directory is used for CoP only. At the time of writing, the terms and conditions for joining the Directory for CoP purposes only are not available;
- Placing all PSPs under a legal obligation to implement CoP puts the Open Banking Directory at the heart of the UK's payments infrastructure. All PSPs would depend on it to offer a CoP service and manage their liabilities under the Contingent Reimbursement Model (CRM). The regulatory authorities will need to consider whether the existing governance, liability and funding arrangements are sufficiently robust;
- Implementation support and co-ordination so that there is industry wide visibility on firm's approaches;
- If necessary, a phased approach that tackles the most significant sources of detriment first and recognises that the receipt and response to a CoP request is necessary for all PSPs whereas sending is a more competitive matter;
- A testing plan that identifies implementation risks and allows for them to be mitigated. There is a particular concern in the industry around the volume of false negatives (no matches and close matches for correctly inputted payments) and the impact on the use of the Faster Payments Service (FPS), including abandoned payments, if an unacceptably high volume of false negatives emerges. There is also a concern about uncertainty over the response speed to a CoP message and that vendor solutions are still in development that will augment and optimise the matching process;

- A managed roll-out of at least six months from the date at which there is confirmed availability of final specifications, rules and guidelines and enrolment on the Open Banking Directory<sup>1</sup>. The rollout would steadily increase the volume of CoP API calls and allows any risk around no match/close match volumes to be measured and assessed. The Open Banking APIs were introduced through managed roll-out to help de-risk the implementation. For some firms with a critical dependency on vendor solutions, a narrow window will be very challenging and does not allow for a diligent procurement and on-boarding process;
- The development of customer communication tools and a realistic marketing approach which explain the changes and encourage a behavioural change in the way customers make digital payments to include the accurate input of the account holder name (thereby increasing the verified payments); and
- Central co-ordination support is essential to effective implementation without unnecessary delay. The absence of a central utility – other than the Open Banking Directory – does not obviate the need to co-ordinate network aspects of the implementation.

The timeline also needs to take account of the implementation requirements already resulting from the CMA Order on open banking and PSD2. These mandates and the proposed Direction draw on the same implementation capability – which is already overstretched, particularly in smaller firms.

Many firms have said to us that they will not therefore be ready to receive and respond to CoP requests until Q4 2019, with some suggesting Q1 2020.

### **The proposed scope of the directions**

**Question 2** *Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?*

A level playing field for all PSPs is the best way manage fraud risk and avoid displacing the fraud risk (and liabilities under the CRM) to relatively late adopters.

**Question 3** *Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?*

All PSPs should be subject to the requirement to receive and respond to a CoP request. The speed at which a response is sent is critical to the success of CoP. We know from open banking that API response times can vary. A co-ordinated approach to testing will illuminate any concerns about response times and what is an acceptable standard.

**Question 4** *Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?*

The Direction should apply to both FPS and CHAPS transactions. But the main source of risk of detriment is FPS transactions, with relatively few CHAPS payments at risk of either APP scams or misdirection, although where these occur the value is higher. Some firms have suggested that the Direction is phased to apply to FPS first and then CHAPS in respect of a new payment mandate being set up or an existing mandate being changed. They have cited the additional protections that exist around CHAPS payments, the pre-validation tools available and the importance of differentiating the use of CHAPS for retail and wholesale payments.

---

<sup>1</sup> OBIE operates a rule that provides the CMA9 (who importantly have delivery teams in place) for at least a six month window from the publication of final specifications and guidelines to implementation. This window does not take account of the need to procure a vendor solution.

There is a danger of steering fraud towards the smaller PSPs who use Head Office Collections Accounts (HOCAs) as there will be no solution for this until Phase 2 (timing tbc and creating an anomaly with the proposed Direction). The consultation is also not explicit on whether PSPs using HOCAs for receiving CoP requests (e.g. many building societies) would also be out of scope for sending requests even if they send payments from their own sort code account numbers.

**Question 5** *Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?*

Yes, it should apply when a new payment mandate is set up or changed. Some of our members have suggested a phased implementation with online and mobile payments channels addressed in phase one.

There are some payment channels to which the Direction should not apply. The direction cannot apply to channels where there is no graphical user interface or where the customer does not communicate with a PSP employee unlike in branch or over the phone. In these circumstances the messaging to customers cannot be controlled. This would include channels like FPS direct corporate access and file input, host-to-host channels, SWIFT users and where a payment initiation service provider is involved. Although nothing should stop PSPs developing services for such channels should they wish to.

**Question 6** *How should any directions deal with the potential for people to opt out of the CoP process?*

An opt out to respond to CoP would be desirable for certain customer types (especially where there is a need to protect their identity) or certain types of transaction but the terms under which the customer exercised that right should be clear. This needs to be considered carefully and the legal basis understood so that there is a consistent approach.

Corporates should be given the possibility to opt out of CoP when sending payments to consumers, as CoP may not be linked to resource planning systems and they may not be in a position to handle the responses.

**Question 7** *Should any directions cover the sending of money from both individual and business accounts?*

Yes, but there will be some types of account where there is confidentiality – in these cases a work round needs to be designed.

The complexities in servicing accounts for large corporate clients and other financial institutions (FIs) also need to be taken into account.

On the sending side, most customers will send files and their PSP would not know if any payment within a file was “new” or recurring because this would be handled upstream by the customer in their own resource planning system. It is helpful to be clear this is a phase 2 issue where there is scope for third parties to enter the market and provide such services and offer solutions at payment set up level.

On the receiving side, it would be rare for large corporate customers to have payments that are fraudulent in nature directed towards them. The complexity for a PSP supporting large corporate clients is in providing a comfortable match that takes into account complex structures, trading names and aliases, for example, where they have purchased a company or are undertaking a divestment, and on behalf of structures. Additionally, there are virtual account propositions in the large corporate cash management space. Consideration should be given to exemptions for large corporate and FI customers.

### **The rationale for our timeframe**

**Question 8** *Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?*

The Direction should initially apply only to the ability to receive and respond to requests (although some have made the case for including both receive/respond and send in the Direction to create greater

ubiquity). This places the sending of requests in the competitive space. This could be monitored to ensure the population of “senders” develops in a balanced way. It also allows PSPs that are ready to send CoP requests ahead of others to receive a response.

**Question 9** *Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.*

We set out below (please see annex) an alternative implementation proposal that is designed to deliver the benefits of CoP at pace, in a way that maximises the opportunity for it to work well in the market. The impact on the real-world costs and benefits would be marginal since the cost benefit analysis makes unrealistic assumptions about go live implementation.

### **Alternative approaches**

**Question 10** *Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?*

We consider that a direction to PSPs provides a helpful way to co-ordinate the market in providing greater protection in the vast majority of transactions at risk of either misdirection or APP fraud.

For the reasons set out in this response, we would propose a more realistic timeline based on Q4 2019 to ensure CoP works well for customers, allows thorough implementation and testing and would not therefore require expensive re-work in the future.

### **Cost Benefit Analysis**

**Question 11** *Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.*

We do not believe CoP will have the impact level assumed in the cost benefit analysis.

The benefits case is predicated on the £93.9 million figure that is said to be the total value of malicious redirections scams in H1 2018. This includes over £20 million (Bacs and International payments) that is not in scope for the direction or the service designed by Pay.UK.

The analysis does not take account of any technical implementation issues that will limit the early impact of the service, for example, algorithm learning.

The initial impact of CoP will be quite high as fraudsters will not be used to the prevention tool and will need to adapt and change their tack to bypass the CoP messages. However, experience has proven that fraudsters will adapt to the changing landscape. The analysis does not appear to take account of displacement effects and the possibility that the impact of CoP could diminish over a period of time.

Clearly too the analysis will depend on the precise scope of the direction. It is not clear what assumptions have been made about the different possible variables raised by the questions in the consultation. A rapid implementation, with unintended consequences and poor customer experience, could reduce the benefits.

**Question 12** *Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.*

We have not gathered any evidence on the costs of implementing and running CoP, which will in any event vary according to the scope of the Direction.

**Question 13** *Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.*

The costs and benefits may not apply equally to all PSPs. For smaller PSPs there is the risk that the costs of implementation and ongoing operation of CoP exceeds the additional liabilities that would be incurred in the event CoP is not applied.

The costs and benefits may not apply equally to different channels. Some of our members have said the costs of applying CoP to telephony channels would exceed the benefits, given that most APP scams are online.

**Question 14** *What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposed April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?*

The costs of implementing CoP to the April and July deadlines would be materially higher, for example by compressing demand for vendor solutions into a shorter time window. If the timelines provide for a ubiquitous implementation and a good customer experience, the benefits are much more likely flow through.

If shorter timescales were to result in shorter testing cycles and increased false negatives, the customer demographic most at risk would be those vulnerable customers that are in most need of fraud protection and that will require the most education and guidance. Customers would also benefit significantly if PSPs align and simplify their communications toward a mutual date, as this is more likely to gain a positive response, less abandonment of transactions due to lack of confidence and fewer opt-outs in the longer term.

### **Equality Impact Assessment**

**Question 15** *Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?*

The current deadlines do not allow firms the opportunity to adequately consider the impacts on protected groups and vulnerable customers before the launch of the service or whether the rules and guidelines adequately cover these issues.

## Annex: UK Finance Implementation Schedule

Activity – Phase 1	Timing	Commentary
Individual and business accounts, FPS transactions, all PSPs, online and mobile transactions		
Pay.UK specifications, guidelines and rules	OBIE applies a six month rule between final sign off of specifications and implementation. During the development, specifications are open so firms can prepare their build against stable elements of the specifications.	Whilst published, the Pay.UK specifications, guidelines and rules have been subject to a non-disclosure agreement and many PSPs have not seen them. Some documents are still being updated with full baselining not happening until the end of January.
Open Banking Directory enrolment	OBIE should provide a timeline to enrol PSPs.	The terms and conditions for enrolling in the Open Banking Directory for CoP are not available yet.
Vendor solutions widely available	The PSR needs to take account of the availability of vendor solutions and orderly procurement.	Vendors have only had access the Pay.UK documents for a short time. Final vendor solutions are not present in the market at scale.
Vendor solutions – procurement		PSPs need time to undertake due diligence on vendor solutions, procure a solution and onboard the vendor.
Implementation build	OBIE applies a six month rule from the point at which documents are finalised to allow for implementation – with delivery teams already in place.	
Testing validation, self-attestation, accreditation of participants	In the Netherlands there was a three month non-customer facing testing phase alone.	<p>Effective implementation requires a network testing plan. Open Banking APIs were implemented through a managed roll-out, with providers' staff using the service in the first instance.</p> <p>Testing is required to gather: how a consumer would react to a <i>no</i> or <i>close match</i> response in practice; if the infrastructure, in the centre and within other PSPs, is resilient for the expected volumes; whether PSPs will be able to perform the matching in a sufficiently fast</p>

		time; and to assess the channel changes and customer messages that will be effective at getting the correct payee information from payers.
Co-ordinated and managed rollout		Volumes should be controlled to de-risk implementation
Internal (including front-line staff training) and customer communications		Work on communication materials can commence early in 2019
Customers communications and adaptations – protected and vulnerable customers		Work on communication materials can commence early in 2019
Go live	The PSR should consider the experience of the January 2018 deadline for Open Banking which led to a number of CMA9 firms placed under direction and re-working aspects of the implementation.	

# Ursa Finance

# Consultation on general directions on implementing Confirmation of Payee: Response

Ursa Finance

Dear sir or madam,

[REDACTED]. We're a new firm currently applying for a banking license, and have been working with the PRA and FCA to this end for ~18 months.

Thank you very much for consulting those with interest in the matter on the general directions on implementing Confirmation of Payee (CoP). We value the opportunity to respond to this consultation, and have laid out our responses to relevant questions included in your Consultation paper (Nov 2018) below.

Overall, we are very supportive of your directions regarding implementing CoP, and believe that this direction is an excellent way forward. We have a few areas of concern, largely around firms this direction applies to and implementation time, which we've detailed in our responses below. We have specifically only responded to questions which we have a unique perspective on, to ensure the best use of your time.

Please let me know if you have any questions or comments. We value your openness in allowing firms such as ourselves to participate in this process, and look forward to working with you in the future.

Sincerely,

[REDACTED]

## 1 ABOUT US

---

We want to take the opportunity to introduce ourselves to set the context for our responses below. Ursa Finance is a new applicant for a banking license in the UK. We've been working closely with the PRA and FCA for the past few months, and anticipate being granted authorisation with restrictions (AWR) in Q1/Q2 2019.

We have chosen to only respond to questions which are appropriate and for which we have relevant responses for – we hope this is not too much of an inconvenience.

## 2 RESPONSES TO QUESTIONS

---

**Question 1:** *Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?*

We agree that giving directions to PSPs to require them to introduce CoP is the right approach to secure your objectives. We feel this is important to establish at the outset – since our concerns do not apply to the end goal or general approach, but rather with the specific timelines required.

**Question 2:** *Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?*

We feel that initially, new banks, especially those without transactional banking services, ought to be excluded from both responding to a CoP request and sending CoP requests, or given an extended time-frame to comply with this direction. This is due to the high costs of introducing CoP, as well as the low benefits from including new banks. These benefits are particularly low when considering new banks who do not offer transactional banking services (current accounts etc), such as ourselves.

The costs for introducing CoP at such short notice is proving quite high for banking applicants such as ourselves. From initial quotations from third party solution providers, we understand that introducing CoP will more than double our anticipated implementation



costs for our payments system. As a new bank, this is particularly problematic. It adds to the barriers to entry that already exist in the banking industry, and make it more difficult for new entrants such as ourselves to start a new bank.

The benefits from including new banks in this directive are fairly low. When aggregating all banks such as ourselves (new banks not offering transactional banking services), the percent of transactions impacted, when compared to the total volume of UK transactions, would not be significant.

As a result, we believe that the overarching goals of CoP outlined in the consultation paper (set out in Section 2) will not be impacted significantly with this exclusion. Furthermore this exclusion need not be indefinite in length – new banks without transactional banking services simply ought to have a longer period of time to implement this direction.

**Question 9:** *Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.*

As mentioned above, we do not feel that this direction for the introduction of CoP allows for sufficient time to do so in a cost-effective manner for organisations such as ourselves. Due to the immediacy of the proposed dates (1 April 2019 and 1 July 2019), third party providers who we've spoken to are struggling to identify resources to implement this type of system, and are having to resort to charging quite steep implementation fees to assist in the prioritisation exercise.

Therefore, we suggest that new banks who do not offer transactional banking services are allowed a lengthier period of time to introduce CoP. Allowing 12 or 18 months after gaining an unrestricted banking license to introduce CoP would allow us and banks like us to safely implement this direction in a cost-effective manner, and have a negligible impact on the target benefit achieved.

# Virgin Money

APP Scams Policy Team  
Payment Systems Regulator  
12 Endeavour Square  
Stratford  
London  
E20 1JN

4<sup>th</sup> January 2019

Dear Sir/Madam

**Virgin Money response to the PSR consultation on general directions for the implementation of Confirmation of Payee**

Virgin Money welcomes the opportunity to respond to the PSR consultation “Consultation on general directions on implementing Confirmation of Payee”. We agree that APP scams are an increasingly serious problem confronting the sector and that without action such scams will most likely increase in scale, damaging consumer trust in electronic forms of payment.

Virgin Money is responding to this consultation as a direct participant of the BACS and CHAPS payment schemes, as distinct from the separate payments scheme memberships of CYBG.

Virgin Money supports introducing confirmation of payee (CoP) across the banking sector. We recognise that providing customers with more information around the recipient provides an additional tool that could reduce the harm associated with APP scams and misdirected payments.

Furthermore, we agree with the PSR that the more PSPs that offer CoP, the greater the benefits from its introduction. We would therefore support the goal of eventually requiring all PSPs to introduce CoP, whilst recognising that smaller PSPs will face specific challenges in doing so – potentially thereby justifying a differentiated timeline for implementation for such firms. We comment further below on both scope and timing.

We also recognise that CoP is just one tool alongside a number of other industry initiatives being introduced – these include, for example, the contingent reimbursement model and additional customer education measures. The variety of measures being introduced is a recognition of the complexity of the issue and that CoP in itself will not resolve all APP scams and is just part one of the solution.

### ***Scope, timing and the importance of consumer engagement***

Virgin Money would encourage the PSR to further consider some of the wider issues associated with the introduction of confirmation of payee. In particular, we would suggest further industry engagement and a clear plan to ensure that customers, businesses and other payments users are aware of the changes being made and what they need to do differently to what they do now (by being aware of the importance of the right payee name and providing the correct account name when requesting payments).

We have concerns that the current proposed timelines would allow little time for such communications to embed, especially given consumers are currently receiving a large amount of communications from PSPs with respect to PSD2 and upcoming authentication changes to their accounts. There is a further risk that the changes being made to strong customer authentication and CoP in parallel to customer's accounts could potentially discourage the use of electronic payments or lead to information overload for some consumers – particularly vulnerable consumers.

With respect to scope, Virgin Money would suggest the PSR considers prioritising online/mobile channels in the first instance to “test and learn” with this audience who will be able to more easily interact with the process of confirming a payee before rolling out to other face to face and telephony channels. The complexity of explaining the CoP process to customers in a branch or on a telephony channel is a lot higher than online and more work will be required by PSPs to ensure the user experience and communication is optimised for these channels.

We would also suggest prioritising those PSPs who make/receive the largest number of payments, recognising that the “network effect” means that smaller PSPs must ultimately be able to comply in order to reduce gaps in the service – this could be achieved, as suggested by the PSR, by mandating smaller PSPs to respond to requests but not be required to make requests in the first instance.

In terms of payment types, Virgin Money agrees that both Faster Payments and CHAPS should be in scope for CoP, given the current use of CHAPS for higher value consumer transactions and therefore transactions which are attractive for criminals to divert. Further consideration should be given to bulk BACS payments for businesses given that invoice fraud is perpetrated against business users and they may choose to pay invoices via bulk BACS payments.

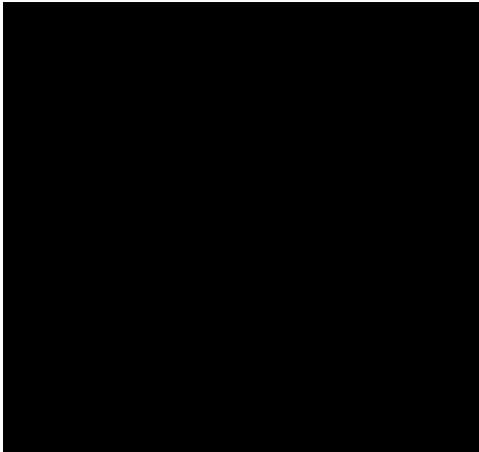
### ***Business engagement***

There are, however, a number of issues with confirmation of payee which could reduce confidence in electronic payments and therefore have wider effects on the economy. For example, issues around head office accounts (where an acct no/sort code collects for a number of organisations), businesses who hold their accounts in different names to their recognised trading names and inconsistencies in “fuzzy matching” due to the lack of centralised control and standards could all cause issues for consumers and businesses in both sending and receiving payments.

In particular, the impact on large collectors of payments (such as utility companies, credit card/mortgage companies, central/regional tax authorities, etc) could be significant as updates to bills, stationary, websites and communications may be required if their registered account names for collection of payments doesn't correspond to customer expectations. This could be especially significant where accounts are held in the name of a parent company which customers might not recognise vs the trading name the customer is familiar with (such as Centrica vs British Gas) or where a third party is collecting money on behalf of a recognised authority.

We would welcome further discussions with the PSR on any of the matters discussed above. Given the proposed timelines contained within the consultation, we would also appreciate a swift response from the PSR in terms of final timelines and scope for the industry activity.

Yours faithfully



Visa

## VISA

### Response to the Payment Systems Regulator's consultation on general directions on implementing Confirmation of Payee

#### 1 EXECUTIVE SUMMARY

- 1.1 Visa welcomes the opportunity to provide comments in relation to the 'general directions on implementing Confirmation of Payee' consultation published by the Payment Systems Regulator (PSR).<sup>1</sup>
- 1.2 Since the consultation by the PSR on a proposed 'contingent reimbursement model' (CRM) for UK interbank payments, progress has been made by interbank industry participants to increase customer protections against authorised push payment (APP) scams.
- 1.3 However, we recognise that there may be opportunities to improve protections for customers making payments over UK interbank systems, and we therefore welcome the consultation by the PSR on the timely implementation of 'Confirmation of Payee' for UK interbank payments.
- 1.4 It is important that any potential policy responses, such as Confirmation of Payee, are considered in the wider context of a competitive global payments market. As noted in our previous responses, global payment networks are at a different stage of maturity in terms of competition and security. Unlike the historic interbank market, global payment systems have strong incentives to deliver benefits to customers, which is demonstrated by extensive innovation that has led to inherent customer-focused features that provide support and protection. We therefore strongly agree that the proposed direction should be focused solely on UK interbank payments.
- 1.5 In addition, the Confirmation of Payee solution under discussion has been developed by Pay.UK with specific consideration for, and engagement with, the UK interbank market only. This does not reflect the additional complexities associated with global payment schemes, which frequently involve a higher number of parties and operate across different countries and regions throughout the world. This reinforces that it would not be appropriate for this particular solution to apply beyond FPS and CHAPS.

#### 2 COMPETITION IN CARD PAYMENTS

- 2.1 At Visa, our goal is to be the best way to pay and be paid for everyone. We do this by connecting the world through the most innovative, reliable and secure digital payments network that enables individuals, businesses and economies to thrive. Our layered approach to security and strong

---

<sup>1</sup> PSR, Consultation on general directions on implementing Confirmation of Payee, CP18/4, November 2018

customer protections, which have been delivered through a competitive market, have helped build and maintain trust in the Visa system over many years.

- 2.2 Competition has continued to intensify in payment systems globally, as industry participants seek to meet the changing needs of customers and merchants. This high level of competition has allowed - and encouraged - innovation to flourish across a range of new services that have enhanced protections for customers, such as authentication, fraud controls and advanced security measures that are now inherent in card payments. While the PSR may wish to apply prescribed solutions in the consolidated interbank space, extending these to other payment systems would have a detrimental impact on their ability to innovate and compete and, in turn, on the quality and choice of solutions being developed and delivered for customers.
- 2.3 The cards market is at an advanced state of maturity in relation to security and fraud minimisation, and has constantly evolved to keep pace with consumer behaviour and technology advancements. Visa has invested significantly in developing solutions that provide increased control and convenience to customers while improving security, in both the face-to-face environment (e.g. EMV chip, contactless technology, payment tokenisation) and in the e-commerce environment (e.g. 3-D Secure Verified by Visa, payment tokenisation). Visa Transaction Controls also allow customers to block or create alerts for selected types of transactions (such as cross-border or e-commerce transactions).
- 2.4 Innovation also underpins our approach to fraud prevention. Our recognised world-class fraud detection and cybersecurity capabilities have been used by banks and governments alike to help identify fraud and economic crime on a domestic, as well as global level. We frequently and proactively work with organisations on identifying fit-for-purpose fraud prevention mechanisms, support law enforcement agencies and lead global industry fraud prevention initiatives.
- 2.5 We have made three long-term investments that will underpin our innovative future – our Innovation Centres, Data Science Lab and Threat Intelligence Fusion Platform. Each of these provides us with the essential expertise and knowledge from which our experts build and continually improve the underpinning technology. These investments and centres are all in place today, delivering innovation to the market.
- 2.6 To encourage future innovation, continued competition is needed to bring customers further choice for more convenient and secure payments. As customers take up new services, payment system providers will be incentivised to enhance their overall offering (including security and customer protections) in order to gain customers. Flexibility is therefore required for providers to develop solutions tailored to particular payment types and customer needs.

### **3 A SOLUTION DESIGNED FOR THE UK INTERBANK MARKET**

- 3.1 The particular Confirmation of Payee solution under discussion has been developed solely for the UK interbank market, which is appropriate. It therefore does not take into consideration the

technical specifications that would be required for a similar solution to be implemented in a non-interbank scheme. Other payment systems operate based on different technology, infrastructure and rules, which are also at a more advanced state of maturity. In a number of cases, key risk-based features of card payments do not exist in the interbank space.

- 3.2 In addition to the innovations discussed above, card payments benefit from extensive in-built risk management and monitoring tools, such as risk-based authorisation. Our advanced fraud and risk capabilities are supported by the rich data set included in card-based transactions, which equips payment service providers with the information to make better-informed decisions.
- 3.3 Crucially, the Pay.UK solution has been developed for the UK market only. Global payment systems facilitate cross-border payments which frequently involve a much higher number of parties and intermediaries. Local, regional or global legal and regulatory changes require continual maintenance, and flexibility is also required to enable the ongoing development of global standards and controls specific to card payments.
- 3.4 The proposed interbank solution would not be effective or scalable across a global operation. Individual schemes vary in terms of size and geography, therefore solutions should be designed to reflect these characteristics and most effectively protect customers. We believe individual schemes are best placed to undertake this task, and that the specific work undertaken by Pay.UK should be limited to the specific market it was designed for.

#### **4 CARDS INHERENTLY PROVIDE CUSTOMER PROTECTIONS, AND VISA DIRECT OFFERS FURTHER CHOICE FOR SECURE PAYMENTS**

- 4.1 Card payments and networks inherently offer a range of support and protections to customers that are not associated with interbank payments. As previously mentioned, there is an extensive set of 'built in' capabilities in card payments such as authentication, fraud detection, customer protection and other security measures.
- 4.2 Our network supports customers looking to make and receive payments in a quick, convenient and secure manner, whether via traditional card payments or newer solutions such as Visa Direct<sup>2</sup>. [REDACTED]
- 4.3 All issuers, acquirers and money transfer operators<sup>3</sup> are vetted and approved by Visa and are then subject to extensive checks, obligations and responsibilities under the Visa scheme. Acquirers must perform due diligence on money transfer operators and ensure they comply with local laws and regulations, and issuers must undertake 'Know Your Customer' (KYC) checks on customers. [REDACTED]

#### **5 CONCLUSIONS**

---

<sup>2</sup> In **Appendix 1**, we include further detail on Visa Direct payments, in line with our response to CP17/2.

<sup>3</sup> The Visa Direct service is provided in partnership with carefully selected and vetted money transfer operators.

- 5.1 We understand and appreciate the PSR's desire to ensure the timely implementation of customer protections in the UK interbank payment system. However, competition in the broader global payments market has driven extensive investment and innovation in relation to customer protection and fraud prevention, which we are continuously enhancing in response to evolving technologies and customer needs. We therefore strongly agree that the proposed direction should be focused solely on UK interbank payments.
  
- 5.2 The particular Confirmation of Payee solution under discussion has been developed by Pay.UK with specific consideration for the UK interbank market only. It therefore does not reflect the complexities associated with global payment schemes and would not be appropriate to be applied beyond FPS and CHAPS.

## 6 APPENDIX 1: VISA DIRECT OFFERS CUSTOMERS DIRECT CHOICE

### A new way to send and receive payments

- 6.1 Visa Direct offers enhanced choice to customers looking to make and receive payments. In contrast to interbank payments, the service is provided in partnership with carefully selected Visa Direct money transfer operators.
- 6.2 In the Visa Direct model, money transfer operators initiate payments on behalf of customers on customers' request and all payments are processed by Visa quickly, conveniently and securely.
- 6.3 [REDACTED]
- 6.4 Visa Direct can be used by individuals to make P2P payments, and also by companies and public institutions for disbursements (e.g., insurance or benefit pay-outs).<sup>4</sup> Payments can be sent to eligible Visa debit, credit or pre-paid cards domestically or cross-border in accordance with the rules of the merchant's programme.

### Visa Direct controls and protections

- 6.5 Customers who send money using Visa Direct can expect fast, convenient, and secure payments that benefit from a layered approach to managing risk through our system level controls. This seeks to identify the source of fraudulent or malicious activity and prevent issues before they arise.
- 6.6 All issuers, acquirers and Visa Direct programmes are vetted and approved by Visa before being granted access to Visa's network. Acquirers must perform due diligence on money transfer operators and ensure they comply with local laws and regulations, while issuers have an obligation to undertake 'Know Your Customer' (KYC) checks on customers.
- 6.7 [REDACTED]
- 6.8 The overall aim of this layered approach is to minimise risks associated with Visa Direct payments and prevent opportunities for malicious interception and fraud, thereby lessening the need for recourse. In exceptional situations, for example when an error has occurred, customers have the opportunity to seek to reverse a transaction.
- 6.9 As a global payment network Visa is responsive to customer needs, risks and changes to its competitive environment. Preserving the security and trust that customers have in Visa is fundamental to our business model across payment types. We review and enhance our rules, controls and protections for our products on a regular basis. As with any new product, we closely

---

<sup>4</sup> In the case of disbursements, merchants make a payment from their own funding source to the recipient.

monitor payments made using Visa Direct and proactively update our controls as needed to protect the integrity of the Visa payment system.

Which?



Which?, 2 Marylebone Road, London, NW1 4DF  
 Date: 4 January 2019  
 Response by: Which?

## Consultation Response

### Payment Systems Regulator's consultation on general directions on implementing Confirmation of Payee

Which? welcomes the opportunity to respond to the Payment Systems Regulator's (PSR) consultation on general directions on implementing Confirmation of Payee. Which? strongly supports the PSR's proposals. We have long called for the widespread adoption of Confirmation of Payee by banks and other payment service providers to help detect and prevent authorised push payment scams. We have been disappointed that a voluntary approach has so far failed to introduce this much needed measure, so regulatory action is now required.

Payments made via Faster Payments and CHAPS are currently processed without checking whether the account name matches the account number. Confirmation of Payee will check whether the account name, which could be an individual or business, matches the customer's intended recipient before any money is transferred. If customers are provided with clear and reliable information and warnings, this measure could be particularly effective at tackling redirection scams, whereby the victim thinks they are paying a legitimate payee but are tricked into paying a malicious payee. It will also help to prevent accidentally misdirected payments.

Victims currently face losses of potentially life-changing amounts of money from authorised push payment scams. Whether a victim is reimbursed after a scam is dependent on the goodwill of their bank, or the success of attempts at repatriation. Most victims are therefore not reimbursed unless the sending and/or receiving firm decides it is at fault. Of the £92.9m lost by consumers from 31,510 cases of authorised push payment fraud in the first half of 2018, just £15.4m (16.6%) was returned to consumers.<sup>1</sup>

The PSR's latest modeling highlights that Confirmation of Payee has the potential to significantly reduce the incidence of maliciously redirected authorised push payment scams affecting consumers and businesses, by around £150m per year. This would significantly reduce the financial detriment suffered by victims of malicious redirection scams, which amounted to £93.9m for consumers and businesses in the first half of 2018,<sup>2</sup> or around £188m if this trend continued in the second half of 2018.

We agree that Confirmation of Payee will not prevent all malicious redirection authorised push payment scams. This is partly because Confirmation of Payee does not directly confirm the payee, as its title suggests, it only checks whether the name inputted by the customer matches

<sup>1</sup> UK Finance (2018), 2018 half year fraud update, p.19

<sup>2</sup> Of which, £27.2m was subsequently returned to consumers. UK Finance (2018), 2018 half year fraud update: Annexe

the one on the recipient's account. Scams are often highly sophisticated, and scammers will still find ways to convince victims that the account name is the payee they intend to pay. For example, by claiming that the business name on an account is different to the intended business' name because it is a related trading name, or by opening fraudulent accounts with names similar to legitimate businesses.

Nonetheless, Confirmation of Payee should make it harder for scammers to operate. It will also add an extra risk warning for customers and payment service providers to help them identify a scam. For customers, they may be told there is only a partial or negative match with their intended recipient name, which may alert them to a potential issue. For payment service providers, if their customer receives a negative match and tries to proceed with the payment then this should suggest a higher risk of the payment being a scam. Sending firms should therefore provide tailored warnings, and sending and receiving firms should subject any such payments and the accounts they are paid into to greater checks.

The draft contingent reimbursement code, which Which? is working with the PSR, industry and other consumer groups to help develop, aims to both reduce the occurrence of authorised push payment scams, and to reduce the impact of these crimes. The code makes clear that signatories to the code should implement Confirmation of Payee. However, it is at yet unclear which firms will sign up to the voluntary code.

Confirmation of Payee has been under consideration since at least as early as 2011 by the then Payments Council,<sup>3</sup> and later in 2015 by Payments UK.<sup>4</sup> Even now that Pay.UK has published the technical standards for firms to implement Confirmation of Payee, it remains unclear which firms would even choose to offer the service. To meet the PSR's aim to introduce Confirmation of Payee without unnecessary delay, and with widespread and quick adoption, a continued voluntary approach is therefore unlikely to be effective.

Which? recommends that the PSR's general directions should:

- **Require all payment service providers using Faster Payments and CHAPs to both respond to and send Confirmation of Payee requests.**<sup>5</sup> All firms that use these payment schemes benefit commercially from these payment schemes, and the credibility that such schemes offer their businesses. Given the net benefits identified by the PSR of implementing Confirmation of Payee, it should form part of the minimum standards for firms offering Faster Payments and CHAPs. This will also prevent scammers from targeting payments involving firms that do not operate Confirmation of Payee.

<sup>3</sup> Payments Council (2011), *National Payments Plan*

<sup>4</sup> Payments UK (2015), *World Class Payments in the UK*

<sup>5</sup> Answers to consultation questions 2,3, 4 and 8

- **Cover all payment channels that a payment can be initiated from (currently mobile, internet, telephony and in-branch).**<sup>6</sup> Without complete coverage of payment channels, scammers will simply target those payment channels that are not covered.
- **Apply only when a new payment mandate is being set up or changed, rather than for all payments.**<sup>7</sup> This is where there is the greatest risk of fraud occurring and where the benefits of introducing greater checks significantly outweigh the costs to consumers in terms of speed of making payments. The PSR should also keep under review whether this requirement should be extended to include making payments to existing payees under certain circumstances, such as transactions above certain amounts or transactions that are made within a certain period of a payment mandate being set up or changed. We would also expect signatories to the contingent reimbursement code to go above and beyond the PSR's proposed general directions if they find evidence that certain types of payment are at greater risk of authorised push payment scams and could benefit significantly from Confirmation of Payee.
- **Be mandatory for customers to use Confirmation of Payee.**<sup>8</sup> Checking the name matches the intended recipient should be an integral part of the transaction, since this process is so important for preventing authorised push payment scams and misdirected payments. We therefore do not think that this should be an optional step for customers.
- **Require firms to give effective warnings to customers who receive a partial or failed match with the name of their intended recipient, and for firms to subject any payments to failed matches to a greater degree of checks.** Effective warnings for partial matches are especially important as customers are likely to receive a high number of partial matches. Many of these will be in cases where the intended recipient is correct but the way they have written the name does not exactly match the form of the name on the account (eg due to a shortened first name or use of initials). We therefore support the principle in the the draft contingent reimbursement code that if a customer proceeds with a payment following a partial match this should not mean they will not be reimbursed if they are the victim of an authorised push payment scam. For failed matches, there is clearly a heightened risk of a payment being made to a fraudster. If having received a clear and effective warning following a failed match a customer still proceeds with making a payment then the firms' responsibility to prevent fraud should not end there. As set out in the contingent reimbursement code, there are a range of measures that sending and receiving firms can take to try to detect payments and accounts used for authorised push payment scams. Such measures should not be voluntary in response to failed matches. The PSR should therefore require

---

<sup>6</sup> Answer to consultation question 5 (i)

<sup>7</sup> Answer to consultation question 5 (ii)

<sup>8</sup> Answer to consultation question 6

all payment service providers to conduct a greater level of checks in response to failed matches.

- **Come into force as soon as is practically possible.**<sup>9</sup> We understand that it will take firms time to implement the PSR's general directions and the technical requirements set out by Pay.UK. The deadlines proposed by the PSR – of 1 April 2019 for receiving and responding to requests, and 1 July 2019 for sending requests and presenting responses to customers – could arguably be challenging for some firms given that Pay.UK only relatively recently published its technical standards for firms. However, Pay.UK has been developing Confirmation of Payee in conjunction with firms for some time. Firms should therefore be expected to be well developed in their preparations. Unless there is clear evidence that the PSR's proposed deadlines could be detrimental to customers by undermining the effectiveness of the system, then the PSR should go ahead with the proposed deadlines.
- **Outline clear expectations of how Pay.UK and payment service providers should work together to communicate the launch of Confirmation of Payee.**<sup>10</sup> Consumers need to be given clear messages about how Confirmation of Payee will change how they make payments. We are concerned that Pay.UK plans not to take an 'active role in education'.<sup>11</sup> As the organisation responsible for introducing Confirmation of Payee and for overseeing the Faster Payments Scheme, which is by far the largest push payment scheme, Pay.UK should coordinate communication and customer education around the launch of Confirmation of Payee to ensure there is consistency across payment service providers.

In future, however, regulatory intervention should not necessarily be required to force the introduction of other types of system-wide fraud prevention measures where there are clearly evidenced benefits. Instead, the payment schemes (Faster Payments and CHAPS, which are led by Pay.UK and the Bank of England respectively) should take greater responsibility for reducing scams that take place on their payment systems by requiring all firms using these schemes to adopt effective new measures.

As the PSR concluded in response to our super-complaint, neither the Faster Payments scheme nor the CHAPs scheme have any rules, policies or procedures related to consumer protection against scams.<sup>12</sup> This is unlike other payment schemes, such as card schemes and direct debits, which have rules that protect consumers against fraudulent payments. These include

<sup>9</sup> Answer to consultation question 9

<sup>10</sup> Answer to consultation question 9

<sup>11</sup> 'Pay.UK's role is to deliver the market capability for PSPs to offer the service to their customers and Pay.UK will therefore not take an active role in education. Raising awareness of CoP, educating customers on how to get the most out of the service and ultimately changing customer behaviours will all be critical to the medium- to long-term success of CoP as a service. This is a role that needs to be undertaken by PSPs with their customers and Pay.UK will provide support and guidance to help PSPs with this important deliverable as part of the implementation of CoP.' Pay.UK (2018), *Confirmation of Payee: Understanding consumer and stakeholder perspectives*, p.11

<sup>12</sup> Payment Systems Regulator (2016), *Which? authorised push payments super-complaint: PSR response*, p.5



mechanisms for payments to be challenged and reversed. Therefore, Pay.UK and the Bank of England should incorporate the principles of the finalised contingent reimbursement code into the detailed scheme rules that firms using the Faster Payments and CHAPS schemes are required to follow.

**About Which?**

Which? is the largest consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an independent, a-political, social enterprise working for all consumers. We are funded solely by our commercial ventures and receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.



**January 2019**

WorldFirst

### Question 5

Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from?

Answer: Yes

Should a CoP request only apply when a new payment mandate is being set up or changed?

Answer: Yes. I assume if this is followed then when the account details are used for payment, after being validated originally, then they will not need to be revalidated every time they are used. This leads to a further question around historical data, will these need to be validated by CoP? I assume no, due to historical data not being in line with new requirements. However, obviously if pre-CoP account details are modified post-CoP, the validation will occur.

### Question 9

Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.

Answer: I don't agree with the deadlines for the introduction of CoP. This is because I feel the majority of documentation circulated around CoP was finally published towards the end of last year, leaving 6 months to obtain budget, build into roadmap, scope, develop, test and deploy the first stage of the solution and then 3 further months for second stage. That is too short a space of time and will lead to a poorly delivered project, negatively affecting customers experience, perception of the change and the functionality. Coupled with this, given the consultation points likely won't be published until March 2019, that is too close to the first deadline to realistically expect the participants to be ready.

A point to note within this is given the growth of payment institutions in the UK, applying a directive to this at the current deadlines would be unrealistic for the majority of these businesses, given the lack of internal resources available, lack spare capital to outsource the development and roadmaps generally full going out 6 months+. I appreciate the intent of CoP is to improve consumer security, which I feel it will, but I feel the diverse range of institutions affected, their business models and markets they operate in need to be accounted for properly. I appreciate question 2 asks this, but I do feel operating a tiered directive could be sensible as generally the institutions whom are most capable of delivering the change in a timely fashion are the ones whom will have the greatest impact. All institutions should be required eventually, but accounting the value it will add vs the impact on those businesses.

The impact on costs internally would be that they increase, due to additional resource being required to deliver the project in the timeline. In terms of the benefits, as mentioned previously, it could affect the quality of the solution and thus these would be reduced.

More appropriate dates would be:

01 September 2019: PSPs must be capable of receiving and responding to CoP requests from other PSPs.

01 January 2019: PSPs must send CoP requests and present responses to their customers.

Worldpay

To: [app-scam-pso-project@psr.org.uk](mailto:app-scam-pso-project@psr.org.uk)

Subject: Response to CP18/4: Consultation on general directions on implementing Confirmation of Payee

---

Dear Sir/Madam,

I am writing on behalf of Worldpay in response to the PSR consultation “CP18/4: Consultation on general directions on implementing Confirmation of Payee”.

**Question 2: Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

The PSR is currently considering whether the proposed directions should apply to “all or only some PSPs carrying out FPS and CHAPS transactions”. We are of the view that, if the proposed directions are introduced, they should apply *only* to Account Servicing PSPs (ASPSPs), rather than to *all* PSPs more generally. As set out below, applying the directions to *all* PSPs that carry out FPS and CHAPS transactions would not be proportionate or appropriate and would likely result in widespread industry confusion.

An ASPSP, as defined in PSD2, means “a payment service provider providing and maintaining a payment account for a payer”. It is only ASPSPs that provide the payment accounts that are used in the execution of authorised push payment (APP) scams, on both the side of the payer/victim and the payee/scammer. It is also only ASPSPs that can fundamentally implement CoP, as they hold the direct relationships with the underlying payment account holders.

Other types of PSP that do not provide payment accounts (i.e. non-ASPSPs) may nonetheless still carry out FPS and CHAPS transactions in the course of the provision of other payment services. For example, in providing card acquiring services, Worldpay uses these payment systems extensively to make settlement payments to our merchant customers for the card payments they have accepted. It is not possible for Worldpay to implement Confirmation of Payee in this situation, as we are neither the sending PSP (this is instead Worldpay’s sponsor bank, an ASPSP) nor the receiving PSP (this is the merchant’s bank, also an ASPSP). Further, the risk of APP scams being associated with settlement payments to our merchants is very low (e.g. as these are typically repeat payments made to the same sort code and account number each month). It is unclear to us how the directions will apply to non-ASPSPs, and will be disproportionate to implement given likelihood and application of the types of payments that could result in APP scams.

By focussing the scope of any potential CoP direction on ASPSPs only is logical and will remove any potential confusion over the obligations of non-ASPSPs. We would therefore urge the PSR to consider only applying the directions to ASPSPs.

Thank you for considering our submission to this consultation. Please let me know if you have any follow-on questions.

Kind regards,

[Redacted signature block]

# Yorkshire Building Society

## Payment Systems Regulator Confirmation of Payee Consultation - YBSG Response

**Q1) Is giving directions under section 54 of FSBRA to PSPs requiring them to introduce CoP the right approach to securing our objectives, in particular to reduce significantly losses and harm from APP scams and accidentally misdirected payments as soon as possible? Are there other approaches that would lead to the same outcomes that we should consider, and, if so, what are they? Do you have any other comments on the issues raised above?**

YBSG is fully supportive of the ambition of reducing the amount of Authorised Push Payment (APP) fraud and therefore welcomes the introduction of Confirmation of Payee (CoP) functionality. While there are a number of options available to ensure that the functionality is implemented in a timely manner, YBSG view the use of directions are the most appropriate to ensure a timely delivery. The key to the success of CoP is the availability and ubiquity of the service and therefore it must be implemented by PSPs across the industry and not just larger PSPs that offer Current Accounts. However, this requirement for all PSPs to participate will introduce a high level of complexity as different PSPs will have access to differing technologies and some will therefore find it much harder to meet the obligations outlined within the directions.

**Q2) Assuming directions in respect of FPS and CHAPS are given, are there any types of PSP that should not be given the directions? What is the basis for your view, particularly having regard to the likelihood of achieving the benefits of CoP?**

Our view is that in order for CoP to be a success, all savings accounts that are able to receive inbound electronic payments should be addressable via CoP. Allowing some organisation to be out of scope of CoP will have negative implications to the success of CoP in two ways:

- 1) Allowing certain organisations or account types to be out of scope will introduce a level of distrust in CoP as a service as there will be a number of accounts that are knowingly not addressable. The sending party is unlikely to know the type of account that they are sending money to and therefore there is a strong possibility that they will not understand why CoP functionality cannot be used. If this becomes normal for sending parties, they are less likely to take advice when a partial or no match is returned which will in turn fail to reduce the amount of misdirected payments or payments sent as part of an APP fraud.
- 2) If there are certain organisations or account types that are out of scope of CoP, these accounts will become the target for fraudsters as they attempt to continue to perform APP frauds. The introduction of CoP will make it significantly more difficult to perform APP frauds and fraudsters will look for any opportunity to use accounts that are not addressable under CoP for a genuine reason.

While many PSPs may struggle to implement CoP functionality, excluding them will not only negatively impact those organisations in the long term but will also reduce the effectiveness of CoP overall.

**Q3) Should the same PSPs be subject to a requirement to respond to a CoP request as those that are required to send a request?**

The view of YBSG is that a direction should only be required for PSPs to be able to respond to CoP requests. While it is also essential for PSPs to send CoP requests, YBSG believes that there are other incentives in place to ensure that this happens such as the Contingent Reimbursement Model (CRM). Our view is that because of the high levels of complexity involved and wide ranging use cases, the sending of CoP requests should sit in the competitive space in order to allow PSPs to focus on being able to respond to CoP requests.

However, YBSG also acknowledges that in order for CoP to be successful in reducing the amount of APP fraud, there must be a high number of PSPs sending CoP requests. With this in mind, YBSG would support the use of directions to enforce the sending of CoP requests however this must be done within a realistic timeframe to ensure that those PSPs that do not have the same access to technology are not disadvantaged or that they impact the successful implementation of CoP functionality.

**Q4) Do you think that we should consider giving directions in relation both to FPS and CHAPS transactions? If you believe that we should consider giving directions in relation to only one of these payment systems, or more than FPS and CHAPS, please set out why. Are there any other issues that we should consider when deciding which payment systems should be in scope?**

Our view is that CoP functionality should be payment scheme agnostic to ensure that as the industry develops over the coming years; the directions given do not become ineffective. The introduction of the New Payment Architecture as defined in the work of the Payment Strategy Forum will change how payment methods are viewed with the introduction of overlay services and any direction that is introduced should be done in a way that ensures that future innovation is not hindered. As fraud detection is improved with the introduction of new controls and technology, the prevalence of APP fraud will reduce and consideration must be taken as to when/how the requirement to use CoP functionality can be removed/relaxed at the appropriate time.

**Q5) Should the directions apply to all payment channels that an FPS or CHAPS payment can be initiated from? Should a CoP request only apply when a new payment mandate is being set up or changed?**

YBSG believes that CoP functionality should also be channel agnostic and should be at the discretion of the PSP as to how and when it is applied. Our view is that the majority of PSPs will apply CoP functionality to all digital channels however some channels, such as Interactive Voice Recognition (IVR) and postal will prove more difficult to implement. Enforcing the use of CoP functionality could have the negative effect of closing some channels to customers if a satisfactory method of implementing CoP cannot be found. Instead we believe that if this is in the competitive space, PSPs will be forced to find new and innovative ways to combat APP fraud through these channels while still delivering a satisfactory customer experience. The introduction of the CRM will ensure that the consumer is protected and will provide a sufficient incentive to PSPs to combat APP fraud.

**Q6) How should any directions deal with the potential for people to opt out of the CoP process?**

YBSG has no specific view on how the directions should deal with the potential for consumers to opt out of the CoP process. However, guidance and advice will be required to assist PSPs in determining when a customer is able to opt out of the service. For example, if there would need to be specific criteria that would need to be met before a customer could opt out of CoP, if it is completely the choice of the customer or if it is at the discretion of the PSP. Special consideration will also need to be made to ensure that PSPs obligations under GDPR can be met while still delivering a consistent approach across the industry.

**Q7) Should any directions cover the sending of money from both individual and business accounts?**

YBSG has no view on how the directions could be implemented to cover both individual and business accounts however it must be acknowledged that the requirements of CoP functionality for business accounts will differ significantly to those of individual accounts. It is the view of YBSG that CoP functionality for business accounts should be considered separately to CoP for consumer accounts as the customer journeys and the requirements will be different.

**Q8) Should the directions separate out responding to CoP requests from being able to send CoP requests? Should directions cover both sending and responding?**

If a direction is used for both the sending and the receiving of CoP requests, it is essential that these are separated out. Unless the go-live of CoP functionality can be implemented across the industry at the same time, which would be unrealistic, it is essential that all PSPs are able to respond to CoP requests as soon as one PSP is able to send a request. This would ensure that the number of CoP requests with a null return is kept to a minimum when the functionality is first released and will also allow PSPs to focus on the sending and receiving of CoP requests separately. This is especially important for mid-tier and smaller PSPs that do not have the same resources available as larger PSPs.

**Q9) Do you agree with the deadlines for the introduction of CoP? If you do not agree, please set out why you consider different dates would be more appropriate and your view of the impact that would have on the costs and benefits of**

**CoP. If the dates are not considered achievable, please give reasons and alternative dates that you consider achievable and the reasons why.**

The view of YBSG is that the deadlines outlined in the consultation are not realistic and must be reassessed to ensure that all PSPs have adequate time to implement CoP functionality. Our view is that the likely effect of directions applied in line with the proposed deadlines will do little more than create a scenario where many PSPs are unable to comply with a legally binding order. While larger PSPs may be able to implement CoP within the outlined deadlines, smaller organisations will have challenges around the resources available and the technical ability to implement CoP. It must be acknowledged that the UK payments landscape is going through a significant period of change currently with major programmes of work underway to meet the obligations of PSD2 and the requirements of Strong Customer Authentication. There is a significant risk that the implementation of CoP in line with the deadlines proposed in the consultation could put the delivery of PSD2 and SCA at risk because of the overlap of the systems, resource and technical knowledge required to implement both. CoP is not technology agnostic and requires PSPs to utilise APIs in order to send and receive CoP requests. While those organisations with Payment Accounts may already be implementing API functionality in order to meet their obligations under PSD2, for many organisations this will be completely new. The April date outlined within the consultation also coincides with the exit of the UK from the European Union. It is not yet understood how this will affect PSPs but it is our view that this could be a challenging time for many PSPs which could impact on the implementation of CoP.

It must also be noted that many PSPs will be reliant on third parties to deliver their CoP functionality. As yet only a small number of vendors have come forward with proposed solutions that may be utilised by smaller PSPs however these solutions will still require significant IT development to implement and will require time for any commercial agreements to be in place. Until all the details of vendor propositions are made available, it will be difficult for PSPs to make an educated assessment of the most suitable solution and what will be required to implement such a solution. It is also not yet understood if the vendors that are offering solutions have access to all of the required technical information required to actually build a solution. There are genuine concerns that the vendors offering solutions may not be able to on-board a significant amount of PSPs if their proposition proves to be popular. These concerns relate to not only the commercial aspects of on-boarding but also their ability to support the technical implementation and testing.

It must also be acknowledged that if CoP is not implemented correctly across the industry, the benefits outlined within the consultation cannot be realised. This means that all PSPs will need to build/procure a solution that will meet the requirements of CoP and that it is implemented in line with the rest of the industry. This will require significant testing internally as well as with other PSPs which will need some kind of organisation and co-ordination to be successful - this will take time.

There are two key risks associated with the implementation of CoP:

- 1) Not all participants are able to respond to CoP requests resulting in a high number of accounts that can't be checked, thus reducing the trust in CoP functionality.
- 2) A high number of false positives are returned due to insufficient testing of name matching functionality.

Our view is that attempting to implement CoP functionality within the deadlines outlined within the consultation will result in the highlighted risks being more likely rather than being mitigated. The amount of customer education that is required should also not be underestimated as this will be key to the success of CoP and will take time, especially for vulnerable customers such as those with disabilities such as dyslexia and those customers where English is not their first language.

**Q10) Are there any alternative approaches that we should consider instead of giving directions to PSPs as set out in this document?**

YBSG has no view or additional information to add relating to this question at this time.

**Q11) Is our assessment of the benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

YBSG has no view or additional information to add relating to this question at this time.

**Q12) Is our assessment of the costs the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

YBSG has no view or additional information to add relating to this question at this time.

**Q13) Is our assessment of the trade-off between costs and benefits the right one? If you do not agree, please set out what you consider would be more appropriate and your view of the impact that would have.**

YBSG has no view or additional information to add relating to this question at this time.

**Q14) What is your view on the impact of the proposed dates in our approach to the trade-off between costs and benefits. Do you consider that imposing April and July deadlines impacts either the costs or benefits of implementing CoP relative to a later implementation date – for example, 2020 or later?**

YBSG has no view or additional information to add relating to this question at this time.

**Q15) Do you have any comments on our assessment of the impacts of the directions we are considering on protected groups or vulnerable consumers? Do you have any evidence that will assist the PSR in considering equality issues, and in particular complying with its public equality duty, in deciding whether to give directions and considering alternatives?**

YBSG has no view or additional information to add relating to this question at this time.