Response to the Payment Service Regulator's Consultation on Confirmation of Payee

Submission by the Transparency Task Force, June 30th 2021

About the Transparency Task Force

The Transparency Task Force is a Certified Social Enterprise, meaning that we exist to make an impact, not profit.

The mission of the Transparency Task Force is to promote ongoing reform of the financial sector, so that it serves society better. Our vision is to build a large, influential and highly respected international institution that helps to ensure consumers are treated fairly by the financial sector.

The primary beneficiaries of our work will be consumers; but the sector itself will also benefit through improved market conduct and increased trust in the services it provides.

Our objective is to carry out a broad range of activities that help to drive positive, progressive and purposeful finance reform, such as:

- Building a collaborative, campaigning community; the larger it is the more influence it can have in driving the change that is needed
- Raising awareness of issues; so that society better understands the problems that exist in the financial sector and how they can be dealt with
- Engaging with people who can make change happen; because through such dialogue we can influence thinking, policy making and market conduct

Much of our focus is on rebuilding trustworthiness and confidence in financial services. To make this possible we are busy developing a framework for finance reform which we describe as a

"whole system solution for a whole-system problem" as described in <u>our recently published book</u>

Our response to you has been produced by a highly collaborative group of TTF volunteers, our "Response Squad," working together to build consensus, whilst always remaining true to our "North Star" question: "What is best for the consumer?"

For further information about the Transparency Task Force see:
<u>http://www.transparencytaskforce.org</u>

Introduction

The Executive Summary of the Call for Views sets out, in paragraphs 1.7 and 1.8, an open and honest assessment of where we have reached with CoP Phase 1. This approach is appreciated. I note that certain types of APPFraud have reduced where the sending bank is an SD10 bank, but there has been a not unexpected shift for 'fraudulent' beneficiary accounts to PSPs that are not CoP-enabled. This is an obvious concern.

Before responding to the specific questions in this Call for Views there are a number of points that I would like to make.

In looking to the future of CoP it is important to recognise that although the SD10 banks represent the overwhelming majority of transactions, they actually represent less than 5% of all Retail Banks and less than 2% of all Payment Service Providers (PSPs). Also, in addition to PSPs, there are a large number of other businesses, such as solicitors, investment companies and IFAs, who would benefit from having full access to CoP but are not part of the Open Banking system.

The Call for Views recognises the challenge of accounts that are identified by Secondary Reference Data (SRD) but does not clearly identify the importance of Electronic Money Institutions (of which there are about 85) or Authorised Payment Institutions (of which there are about 253). This may be important because it appears that EMIs and APIs are 'hosting' an increasing number of beneficiary accounts, or e-wallets, that are being used for fraud.

The system that has been implemented by the SD10 banks, and the other banks that have joined CoP voluntarily, requires full participation in Open Banking. CoP Phase 2 will be based on a dedicated 'CoP-only' role profile in Open Banking which will not only apply to new entrants but also requires upgrades by the existing users.

These points raise the rather important question of: "Is the current plan for CoP Phase 2 the best way forward, or is there an alternative way forward that would be significantly easier to implement across all PSPs and could also be extended to cover related financial service providers?"

I understand that SurePay operates the CoP system in Holland, and that it covers 99.6% of all payment transactions within the Dutch banking system. Is this an option that has been seriously considered for either all, or part of, the UK financial services sector?

There is one other matter that is not covered in the Call for Views but which I believe should be given serious consideration.

A significant proportion of both personal accounts and business accounts are in a name that is not used by the account holder in everyday life. Obvious examples include Muslim men who commonly have "Mohammed" (or an alternative spelling of it) as their first name but use their 'middle' name in everyday life. Has consideration been given to allowing account holders a 'one-time-only opportunity' to create a 'known as' name for the purposes of CoP?

Response to Questions

Question 1: Phase 1 trends and impact:

Do you have any comments on the trends presented above regarding the impact of CoP on the relevant types of misdirected payments and the relevant types of APP scams? Do you believe that, in light of the decreases in the relevant types of misdirected payments and despite an increase in the relevant types of APP scams, CoP has had a positive impact? Do you believe that CoP has resulted in improved customer experience and confidence in electronic bank transfers?

CoP has had a positive impact but it has not been as impactful as it could, and should, have been because of the almost complete absence of customer education. This needs to be addressed in the implementation of Phase 2.

Question 2: Fraud migration and bypassing a no match:

Do you agree that the analysis shows that financial institutions that haven't implemented CoP provide opportunities for the relevant types of APP scams to continue to grow? Are there any other type(s) of institution where the relevant types of fraud have migrated to? Do you agree with the analysis showing that scams continue even when a 'no match' occurs? Do you have any views as to how these areas could be addressed in future?

This question is in two parts.

Fraudsters have migrated their accounts to non-CoP PSPs, in particular to Electronic Money Institutions (EMIs), that are both poorly regulated by the FCA and provide a direct route for converting the stolen funds into untraceable crypto-currencies.

There are a number of reasons why customers continue with the transaction following a 'no-match' warning, including:

· the SD10 banks failed to educate their customers about CoP, thus allowing fraudsters to assert lies such as "your new account won't show up for CoP verification for 24-hours after we have created it for you"

· the no-match warnings are ineffective in terms of both wording and presentation

· the process for over-riding a 'no-match' warning should be clearly different from the process for accepting a 'match' or 'close-match' response.

The banks' response to customers continuing past a 'no-match' warning needs to be a combination of effective customer education, a slow-down in the payment system in respect of high value payments to new Payees, and a greater willingness of the banks to intervene in payments to new Payees.

Question 3. Phase 2 progress and dependencies:

Do you have any comments on the progress and dependencies of Phase 2 and the CoP-only role profile presented above? Are there any other dependencies or barriers that you would like to highlight?

My understanding is that each PSP (or other organisation) that wishes to implement CoP, has to either develop or source software to manage the verification and response processes. The question must be: "Why?" Why is the process not managed centrally, as it is in Holland, as this would substantially reduce the barriers to entry.

Question 4: Costs and benefits of including SRD accounts:

Do you have any comments on the specific costs and benefits of including SRD accounts in CoP Phase 2? Are there any other potential costs or benefits that you would like to raise? Do you have any comments on whether there are certain types of SRD accounts which would not yield a significant benefit from CoP, and/or whether the industry should focus its efforts on SRD accounts that allow for transactions to both into and out of them?

CoP Phase 2 must address the issue of SRD (Secondary Reference Data) accounts because there is already evidence that fraudsters are moving their accounts into those PSPs that rely on SRD, for example, EMIs referencing of e-wallets for crypto-currency.

There is no single solution to this question.

Where an SRD is used by a Building Society, for example for a mortgage, it can be excluded from CoP because payments in and out of the account are 'managed' by the society.

Where SRDs are used by APIs and EMIs the best option might be to 'upgrade' the API or EMI to a 'sort-code holding entity' so that all customer accounts (and e-wallets) would be directly addressable via a standard 8-digit account number. This would have the added advantage of being able to identify all accounts using a standard IBAN format and facilitate integration with an international payments system.

Question 5: Alternative solutions for SRD accounts:

Do you have any comments on whether the alternative solutions presented above could bring the benefit of CoP at a lower cost than creating a specific CoP solution for SRD accounts? Do the alternative solutions have any downsides?

(see above)

Question 6. Phase 2 benefits and costs:

Do you have any comments on the benefits of CoP Phase 2 presented above? Are there any other potential costs or benefits that you would like to raise?

The real benefits of CoP Phase 2 will come when fraudsters have nowhere to hide their fraudulent beneficiary accounts and the banks have educated their customers about CoP and other fraud prevention measures.

With reported APPFraud likely to exceed £500m this year there is both a lot of money, and a lot of heartache, to be saved if we can achieve the 99.6% validation that is achieved in Holland.

Question 7. Messaging and warnings:

Do you have any comments on how CoP messaging works and how this could be improved in order to avoid the issues raised above – for instance, by standardising messaging? What other enhancements could be brought to the CoP service?

The current CoP messages are ineffective in respect of both the words and the visual presentation. The messages should be standardised, and there should be regular reviews to test customer reaction to different wordings.

The visual presentation should also be strongly guided in terms of font size, colour and position. For example, a message in a small font on the top line of the screen when the 'continue' button is at the bottom of the screen makes the message missable. A 'no-match' warning should be 'front and centre' on the display.

It is also important to make the process of over-riding a 'no-match' warning substantially different from the standard 'continue' option.

Question 8. Directing migration by SD10 banks to Phase 2:

Do you think we should direct the SD10 banks to move to the Phase 2 CoP-only role profile environment by the end of 2021? Is it also important to include in any such direction a period of dual running for Phase 1 and 2 ending in Q1 2022, as currently foreseen by Pay.UK?

I understand that the SD10 banks have already agreed to this.

Question 9: Directing Phase 2 implementation by non-SD10 PSPs with unique sort codes:

Do you have any comments on whether we ought to direct non-SD10 PSPs with unique sort codes to implement Phase 2, in addition to the SD10 banks? In particular:

1. **Should we direct non-SD10 Phase 1 participants to move to the Phase 2 environment, and/or PSPs that have not yet adopted CoP to implement CoP under Phase 2? If so, by what date? Are there any specific PSPs or groups of PSPs that we ought to prioritise and/or exclude from an eventual direction, such as medium sized and/or small financial institutions?**
2. **Should we direct PSPs to develop both the responding and sending capabilities for CoP, or responding or sending only?**
3. **Is a PSR direction the best way to achieve the necessary changes? Do you have any other suggestions to achieve these changes?**

All PSPs should have unique sort codes and they should all be directed to implement CoP Phase 2. Anything less than this will create a situation that will be exploited by the fraudsters. If this happens for any reason, it must be clearly addressed in the CRM Code where the question of reimbursement by non-Code firms is currently unclear.

This means that the overall cost of implementing and running CoP must be made proportionate to the size of each business. Recognising the large number of smaller PSPs, including all of the

APIs and EMIs, I suggest that there may need to be a fundamentally different approach for these organisations, such as a centrally shared system specifically created to combat fraud.

Question 10: Enabling CoP participation by SRD accounts:

In relation to SRD accounts, do you have any comments on the following:

1. **For those SRD accounts where CoP would be beneficial, is a PSR direction to deliver a specific CoP capability for these accounts the best way to achieve the necessary changes? Do you have any other suggestions to achieve participation in CoP by those accounts, such as the alternative industry-led solutions in paragraphs 4.23 to 4.24 ? Do you have any comments on the costs of the industry introducing unique sort codes and account numbers for (certain types of) SRD accounts?**

2. **If a PSR direction were to be needed, should we direct the SD10 banks to implement the capability to send SRD information by the end of H1 2022 in accordance with the timeline established by Pay.UK? Should we direct PSPs beyond the SD10 banks to deliver this capability?**

3. **Should we also direct PSPs that offer SRD accounts to implement CoP responding capabilities for SRD accounts by the end of H1 2022 in accordance with the timeline established by Pay.UK?**

(see above)

Question 11: Pay.UK's role:

In view of Pay.UK's role described in paragraphs 1.10 and 2.2, do you have any comments on whether we ought to require Pay.UK to have a greater role in terms of the CoP messaging? Do you have any comments on the role we should require Pay.UK to play in monitoring adherence to the CoP rules, standards and operating guidance, and communicating relevant statistics?

Pay.UK should set all of the standards for CoP messaging, including the actual words, the font, style, position and visual presentation, and they should be responsible for enforcing these standards.

Question 12: Regarding the future of SD10:

a. Do you believe that SD10 has achieved its objectives, will be technically redundant once Phase 2 is implemented, and should therefore be revoked?

b. Should SD10 be revoked in circumstances where there is no direction in relation to CoP Phase 2? Are there any elements of SD10 that should be continued into any future direction, and how long should these be for?

SD10 has proved that SoP is a vital tool in the prevention of APPFraud and it must become part of the standard requirements for a PSP to be registered with, and regulated by, the FCA.

Andy Agathangelou FRSA
Founder, Transparency Task Force; a Certified Social Enterprise
Governor, Pensions Policy Institute
Chair, Secretariat Committee, APPG on Pension Scams
Chair, Secretariat Committee, APPG on Personal Banking and Fairer Financial Services
Chair, Violation Tracker UK Advisory Board
Policy Adviser to Parrhesia, the Whistleblower Research Charity
Telephone: +44 (0)7501 460308