A2(d)-Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code

Consultation Document

Date : 01 02 2021
Version : 0.1
Classification : PUBLIC

CONTENTS

CONTENTS 2

3. Background 6
- 3.1 Confirmation of Payee 6
- 3.2 Confirmation of Payee 8
- 3.3 APP Fraud Analysis 9

4. Evaluation of the Risk of APP in PISP Use Cases 11
- 4.1 Evaluation Objectives 11
- 4.2 Evaluation Approach 11
- 4.3 PISP Use Case Categorisation 12
- 4.3.1 Merchant Initiation via PISP (paying for goods or services): 12
- 4.3.2 P2P Initiation via PISP (transferring money to someone else) 13
- 4.3.3 Transferring Money between Accounts in the Same Name (payments between my own accounts) 13
- 4.4 Propensity to APP Fraud 13
- 4.4.1 Evaluation of Merchant Initiation via PISP (paying for goods or services): 14
- 4.4.2 Evaluation of P2P Initiation via PISP (transferring money to someone else) 16
- 4.4.3 Evaluation of Transferring Money between Accounts in the Same Name (payments between my own accounts) 18
- 4.5 Summary Conclusions 20
- 4.6 Merchant Initiation – Consideration of Additional PISP Requirements 21
- 4.7 Recommendations 22

5. Effective CRM Warnings 23
- 5.1 Evaluation Objectives 23
- 5.2 Experimental Design Summary 24
- 5.3 Experimental Results Summary 25
- 5.4 Preliminary observations 27

6. Direct Participation of PISPs in CoP 29
- 6.1 Option Evaluation 29
- 6.2 Observations 32

7. Direct Participation of PISPs in CRM Code 33

1. Executive Summary

Confirmation of Payee (CoP) and the Contingent Reimbursement Model (CRM) Code are both UK industry initiatives to reduce the incidence of Authorised Push Payment (APP) fraud and its impact on payment users. Both initiatives impact interbank payment journeys, in ways that will have consequences for Open Banking Payment Initiation Service (PIS) payments.

This Evaluation seeks to establish how CoP and CRM can be most appropriately embedded into PISP payments in a way that is aligned to the objectives of both initiatives and are not unnecessarily or inadvertently disruptive to legitimate payment journeys. The aim is to ensure that how CoP and CRM are implemented is proportionate and maximises their effectiveness. The output of this Evaluation will be recommendations to Pay.uk and the Lending Standards Board (LSB), who are the entities responsible for the governance of CoP and the CRM Code, respectively.

We have provisionally concluded that the risk of APP fraud in a sub-set of PISP use cases related to Merchant Initiation via PISP, where the PISP onboarding processes are sufficiently robust, is low. Our conclusion is that for this category of transaction CoP checks and CRM warning messages are of limited utility and that that the resultant additional friction together with the incremental costs of deployment are not justified. Indeed, emerging evidence from our consumer research suggests that there would be positive benefits from eliminating the overuse of warning interventions; customer fatigue erodes their effectiveness.

Conversely, we have found that the risk of APP fraud in relation to peer to peer payments via PISP is comparable to other inter-bank payment transactions and equally susceptible to APP fraud. Consequently, the inclusion of both CoP and CRM warning interventions may be warranted. CoP should be used when a new payee is established to make a payment transaction of this type. CRM warnings should also be applied, on a risk-based approach, in the payment journey.

Finally, we conclude that PISP payments used for transferring money between accounts held by the same payer(Me2Me) could be potentially susceptible to **malicious re-direction** fraud, but not **malicious payee** fraud. CoP is an appropriate countermeasure to the risk of **malicious re-direction** fraud and should be used where a payment of this nature is being made to a new account.

Where warning interventions are required, they should be as effective as possible. We commissioned an extensive piece of consumer research, based on behavioural science, the objective of which was to identify optimal warning interventions that increase consumer attention, increase identification of fraud and improve the overall consumer experience. Various approaches to warning interventions were tested in a large-scale online randomised controlled trial, designed to provide robust evidence as to what works. As described in section 5, we took extensive steps to ensure that the experimental design was rigorous.

The consumer research findings presented in this paper are provisional. A considerably more detailed analysis of this extensive piece of research is currently underway and we will publish more detailed conclusions in the next phase of our consultation. The intention is to distil the findings of this piece of research to provide relevant recommendations to the LSB to inform development of the Code and their associated Practitioner Guidance. It should also be noted that it was never the intention that the results of this research would be used to develop prescriptive or mandatory requirements. The results are formative and provide an informed basis for follow on research, potentially in live environments, that further inform how warning interventions could usefully evolve to become a more effective fraud prevention tool.

However, the preliminary results of this research demonstrate that various enhancements to warning interventions have potential to significantly increase PSU detection of APP fraud. The results indicate that the largest effects are achieved when introducing call to action options (CTAs) that offer PSUs the opportunity to cancel and defer payments. This is in fact consistent with an observation made by the LSB in the context of their Thematic Review. We also note that there is some evidence that a risk-based approach, which provides more targeting of interventions such that warnings are presented more sparingly is likely to improve their effectiveness.

The preliminary results also suggest that it does not make a big difference if the responsibility for COP and CRM are allocated to a bank or a PISP. However, there is significant evidence that it is detrimental to split the responsibility between the two parties. Further analysis is also taking place in relation to any recommendations flowing from these finding. Nevertheless, our provisional conclusion is that there is likely to be benefits from a fraud reduction perspective in enabling PISPs, to play an autonomous role in the presentation of CoP and CRM messaging.

Participation in CoP is currently not open to PISPs, but Pay.UK plans to develop an extended CoP proposition for a wider range of participants, including PISPs, in due course. We have identified three options that would support the integration of CoP into PISP payment journeys :

1. CoP call by Sending Bank after authentication
2. CoP call by PISP
3. CoP call by Sending Bank before authentication

It is envisaged that the first two of these are both likely to be required options. The third is more challenging in terms of complexity, particularly as the PISP handles customer messaging, but the ASPSP processes the API Request and Response, which may result in the need for more complex liability sharing arrangements. The purpose of the consultation is to validate the three options outlined above, identify any others and assess the extent to which should be progressed by Pay.uk .

We provisionally conclude that it is beneficial to include effective warning interventions in certain categories of PISP payments. The research also indicates that these interventions are more effective when presented together with the CoP response by the same entity. Consequently, we can also see the possibility that PISPs may wish to play a central role in delivering warning interventions in the payment journey. In line with our observations on CoP, we anticipate that there may be appetite from certain PISPs in participating as a subscriber to the CRM Code. Participation in the CRM Code is voluntary.

We note that the Code was originally developed by the APP Steering Group to accommodate a number of large banks who were committed to its introduction. In this development phase the specific needs or constraints of PISPs were not considered. The LSB is currently consulting on potential revisions to the Code as part of a first post-implementation review, that will facilitate greater participation from more diverse range of participants, including PISPs. This includes consideration of challenges or barriers which specifically may exist that would prevent PISPs from becoming a signatory to the Code, for example because they are unable to meet the requirements of the Code as it currently stands. The specific needs and constraints of PISPs were not considered within the original development of the Code. As the LSB looks to extend participation within the Code to a wider range of participants, including PISPs, there is an increasing need to identify and address components of the Code that may act as potential barriers to PISP participation. There are a number of provisions within the current version of the Code, that in the view of OBIE , would be difficult for PISPs to fully comply with. We have set out recommendations where we think certain provisions should be modified.

2. Introduction

2.1 Purpose of this Report

The purpose of the Confirmation of Payee (CoP) & Contingent Reimbursement Model (CRM) Evaluation is to determine the most appropriate approach to development of new OB Standards (including API specifications CEG and OG), to enable low-friction, low obstacle open banking customer journeys that take appropriate account of the requirements of the Contingent Reimbursement Model (CRM) code and Confirmation of Payee. CoP and CRM are new features of a large volume of Single Immediate Payments over the Faster Payments network.

This Evaluation is intended to determine:

1. Where and how warning interventions should be proportionately applied to PIS transactions to ensure that they introduce additional friction appropriately correlated to risk of susceptibility to APP fraud. The objective is to ensure that the approach is aligned to the overarching principles of both CoP and the CRM Code and appropriately protects end-users of PIS from the risk of APP fraud.

2. How to optimise iso that they increase consumer attention, reduce fraud, and improve the overall consumer experience.

3. Understand the potential advantages to PISPs of direct participation in both the CoP / CRM initiatives, and if there are rules or other existing requirements of CoP/ CRM that act as barriers to direct PISP participation.

4. To the extent that there are any observable barriers, develop recommendations as to how these could be modified by Pay.uk and the LSB to facilitate broader access to these two initiatives. This is responsive to key elements of the LSB Code Review Consultation.

2.2 Consultation Process

1. The OBIE welcomes responses to the consultation from all interested parties, including PISPs, trade associations and groups representing consumers and SMEs. Informal bilateral consultation commenced on 18 January 2021.Discussions have taken place with the LSB , the Fraud & Security Working Group , Pay.uk and UK Finance. The first phase of the formal consultation Process will take place between the 1st February and 1st March 2021.

2. An Expert Advisory Group will be established to discuss the draft recommendations and obtain feedback. The OBIE will also arrange specific events for stakeholder groups e.g. the Security & Fraud Working Group.

3. A seminar will be arranged in the second week of February to present the final results of the consumer research. Specific workshops on CoP & CRM will also be arranged.

4. Written consultation responses are due **by 5pm on Monday 1 March 2021** . Please respond to the questions only; there is an additional comments section at the end. Consultation responses to the questions (see below) should be provided using the online portal provided at [insert link to survey monkey]. Please submit one response document per organisation.

5. Responses to the consultation are deemed to be non-confidential.

6. Following the consultation period, all responses will be reviewed, collated and summarised ahead of discussion at the March Implementation Entity Steering Group (IESG) meeting on March 25, 2021. Following this OBIE will provide an update and next steps.

3. Background

3.1 Confirmation of Payee

Confirmation of Payee (CoP) is a mechanism designed to give end-users assurance that they are making payments to the intended recipient. Customers setting up a new payee will now be able to confirm that the name they've entered matches the one on the account they're intending to pay. It addresses both the detriment caused by payments being misdirected due to errors and prevents the occurrence of certain types of Authorised Push Payment (APP) fraud. Prior to setting up a new payee, the name, sort code and account number that a PSU enters are checked against the details of the payee held by the Receiving Bank (the payee's PSP). A CoP check is done directly between the sending and receiving PSPs.

In August 2019, the Payment Systems Regulator (PSR) issued Specific Directions to require members of the UK's six largest banking groups to implement CoP by the end of March 2020. That date was subsequently delayed to 30 June 2020.1

The Directions require those banks to:

1. Introduce CoP for the Faster Payments Scheme (FPS) and CHAPS.

2. Respond to every CoP request made to it in a way that complies with the CoP rules and standards established by Pay.uk; and

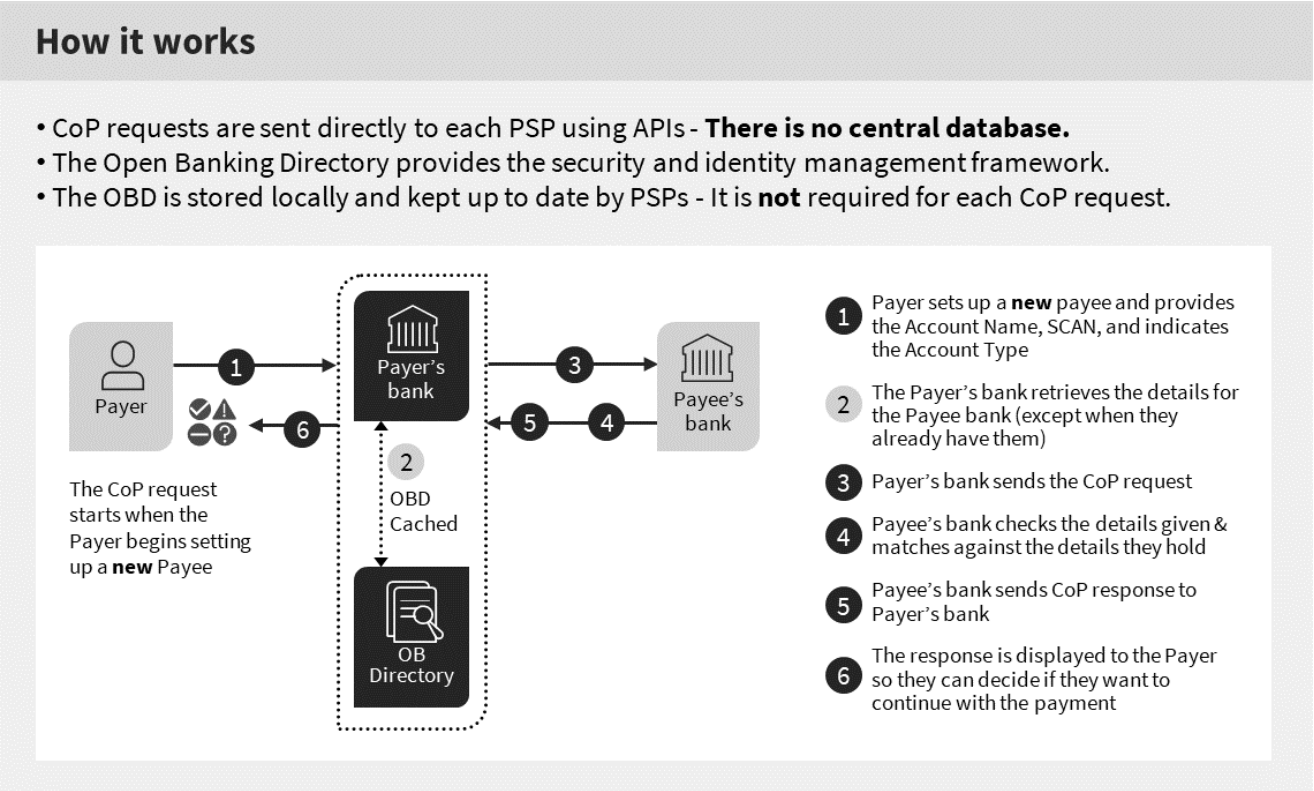
3. Send a CoP request the first time the PSP's customer provides the details necessary to pay a new payee (or amends the unique identifiers in relation to an existing payee), whether or not funds are sent immediately following the provision of the details.

Delivery of CoP will be in two distinct phases. "Phase 1" covered the requirements for banks who are Direct participants in the Faster Payments and CHAPS payment systems and have their own unique addressable sort code. for CoP, including the potential of the proposition for bulk payments, other corporate applications. how it can be utilised by PSPs without and addressable sort-codes This also includes the use of CoP by PISPs.

The design for CoP was developed and agreed by the Payments Strategy Forum in December 2017. Following this Pay.UK developed CoP rules and standards. A high-level overview of the process flow is set out in **Fig 1.**

[1] LBG, Barclays, HSBC, NatWest Group, Nationwide& Santander.

Figure 1: CoP Process Flows



Source Pay.uk

There are 4 possible outcomes that can be returned to the Payer:

1. **Yes, there is an exact match** – the customer used the correct name of the account holder and the details match. The customer can then proceed with the payment.

2. **Partial or close match** - the customer used a similar name to the account holder. The customer is provided with the name of the payee to confirm. If the customer recognises the name provided, they may opt to proceed with the payment. Alternatively, they will be able to update the details and check the name again or contact the intended recipient to confirm the details before proceeding further.

3. **No match** – the details input does not correspond with the details held. The customer will not be able to see the actual name on the non-matched bank account. Customers are advised to make further checks.

4. **Confirmation of Payee Unavailable** – payee account not available temporarily or otherwise, and the name cannot be confirmed.

The PSR confirmed that their direction only relates to proposed transactions involving accounts that the Pay.UK rules and standards. [2] This currently relate to Pay.UK CoP rules and standards for 'phase one' covering UK-regulated account-servicing PSPs that operate in the UK, are Direct participants in

[2] PSR Specific Direction 10 1.8 (j)

the Faster Payments and CHAPS payment systems and have their own unique addressable sort code. The current rules do not cover PISP.

For this reason, the Directed Banks are not required to introduce CoP into PISP journeys. Pay.uk have confirmed that the 6 Directed banks are not currently utilising CoP in relation to PIS payments and do not intend to do so until Phase Two development is complete.

Phase Two, as described previously, was originally planned to be substantially delivered within 2020, but for a number of reasons, including impacts of Covid-19, Pay.uk has reprioritised certain elements of the Phase Two activity. This includes addressing the PISP proposition at a later phase. Currently it is anticipated that Phase Two will commence in Q2 2021, subject to agreement by the Pay.uk Board.

3.2 Confirmation of Payee

In 2016, Which? submitted a super-complaint concerning the inadequate levels of consumer protection for customers who fall victim to APP scams. In its response to the super-complaint the PSR set out a number of recommended actions to be taken forward by the banking industry, including the introduction of a 'contingent reimbursement model'. Following this, in early 2018, the PSR established a Steering Group to design and implement a voluntary industry code, the objective of which is to reduce the occurrence of APP scams and reduce the impact of these on consumers. This was comprised of both industry and consumer representatives, as well as observers from regulators, government and law enforcement. The Contingent Reimbursement Model (CRM) Code came into force on 28 May 2019. The voluntary code sets out good industry practice for preventing and responding to APP scams. It also sets out the requisite level of care expected of customers to protect themselves from APP scams. Currently there are nine firms, comprising of 19 brands, signed up to the Code. When adjudicating APP fraud complaints, the Financial Ombudsman Service will consider any relevant code of practice to help it decide what is fair and reasonable.

The overarching objectives of the CRM Code principles as set out at the start of the Code are to:

- reduce the occurrence of APP scams
- increase the proportion of customers protected from the impact of APP scams, both through reimbursement and the reduction of APP scams; and
- minimise disruption to legitimate Payment Journeys.

In addition to the Code, there is a Practitioners Guide.

The key components of the code are as follows:

- **Measures for detecting, preventing and responding to APP scams** - The Code sets out a general expectation that firms should participate in consumer education and awareness campaigns to inform consumers about APP scams and the actions that they can take to reduce the risk of APP fraud. The Code also sets out obligations on firms to provide "effective warnings", in payment journeys which are at risk of APP fraud. The Code and associated guidance are principles based, rather than at a detailed level of specificity. The issue of effective warnings is explored in more detail in Section 5.

  It was originally envisaged that subscribers to the Code would implement CoP, but it does not currently specify the date on which this will become an effective requirement of the Code. CoP potentially places an additional responsibility on customers as a firm may elect not to reimburse a customer if a warning that the name of the recipient does not match is ignored by the customer. While the UK's six largest banking groups, covering around 90% of inter-bank payments have fully implemented Cop, some banks beyond those directed by the PSR have

voluntarily introduced CoP, and Pay.uk report that there is a pipeline of additional banks expected to introduce CoP. The Lending Standards Board (LSB) is currently consulting on whether and, if so, from when, it should be mandatory for Code subscribers to implement CoP.

- **The circumstances in which customers can expect to be reimbursed** - A fundamental objective of the Code is to ensure that a higher proportion of customers receive reimbursement of APP fraud losses in circumstances where they are not to blame. Particular attention is paid in the Code to assessing particular vulnerabilities of customers which may contribute to their susceptibility to APP fraud. The presumption in the Code is that victims should be reimbursed unless there is an objective reason for attributing blame to the customer. Key to this assessment is a judgement of what consumers may have reasonably believed at the time. In addition, the firm is required to have a robust process for resolving claims and to provide appropriate aftercare whether or not a customer is reimbursed.

On 1 July 2019, the LSB became the official governing body for the CRM Code. Its role is to monitor the implementation of the Code, to ensure its effectiveness, and to maintain and refine it. In this role, the LSB has undertaken a number of thematic reviews and on the 10 December 2020 published a summary report of its Review of effective warnings. The findings from this review will feed into the wider CRM Code review recently undertaken by the LSB, the results of which will be published early next year.

3.3 APP Fraud Analysis

Authorised push payments (APPs) occur when victims are persuaded to make payments from their account to an account that the criminal controls. Fraudsters use a variety of social engineering techniques, typically they include posing as individuals or organisations. APP fraud is differentiated from an unauthorised transaction, where the PSRs provide legal protection to cover losses. As described above, where a customer falls victim to an APP fraud, if both the customer and their financial service provider meet the standards set out in the CRM code, and the company is a signatory of the code, then they will be reimbursed.

There are two distinct types of APP fraud:

- **Maliciously misdirected** – the payer thinks they are paying a legitimate payee but is instead deceived into transferring the funds to a different person.
- **Malicious Payee** - The Customer transfers funds to a payee person for what they believe is legitimate purposes, but which is in fact fraudulent.

UK Finance has established 8 specific categories of fraud, which underpin their analysis and presentation of APP fraud data. These are as set out in **figure 2**.

Figure 2: APP Fraud Categories

Malicious Redirection	
Invoice & Mandate Scams	The victim is persuaded to redirect the payment to an account they control when the customer intends to pay a legitimate invoice. Typically includes criminals targeting consumers posing as conveyancing solicitors, builders and other tradespeople, or targeting businesses posing as a supplier, and claiming that the bank account details have changed. This type of fraud often involves the criminal either intercepting emails or compromising an email account.
CEO Fraud Scam	The fraudster impersonates the CEO of the victim's organisation to convince the employee to make an urgent payment to an account that the fraudster controls. The message commonly requests a change to payment details or for a payment to be made urgently to a new account. Typically, the fraudster will either access the company's email system or use spoofing software to email a member of the finance team with what appears to be a genuine email from the CEO.
Impersonation Police/Bank Staff	The fraudster purports to be from the victim's bank and convinces the victim to make a payment to an account they control. Typically, the scam involves persuading the victim that they are at risk of fraud and should transfer the money to a 'safe account'. Fraudsters may also pose as the police and ask the individual to take part in an undercover operation to investigate 'fraudulent' activity.
Impersonation Other	The fraudster claims to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help 'fix' a problem.
Malicious Payee	
Purchase Scam	The victim pays in advance for goods or services that are never received. Typically, the victim will be offered goods at an exceptionally discounted price. The fraudster will persuade their victim not to pay via payment mechanisms that offer the customer protection in the event of non-delivery.
Investment Scam	The victim is persuaded to invest in a fictitious fund/ investment. High returns are often promised to entice the customer. in order to entice their victim into making the transfer.
Romance Scams	The victim is convinced to make a payment to a person they have met, often online through social media or dating websites, and with whom they believe they are in a relationship. Fraudsters. use fake identities target their victims in an attempt to start a relationship which they will try to develop over a long period of time. Once they have established their victim's trust, the criminal will then request money to resolve a problem they claim be experiencing.
Advance Fee Scams	A criminal convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high-value goods. These scams include scenarios where the fraudster claims that the victim has won a lottery, that goods are being held at customs or that an inheritance is due. These scams often begin with an email or a letter sent by the criminal to the victim.

4.Evaluation of the Risk of APP in PISP Use Cases

4.1 Evaluation Objectives

The key objective of CoP is to reduce fraud and misdirected payments. As set out in Section 3.1 the Directed banks, subject to the PSR's Specific Direction 10, were not required to introduce CoP in relation to PISP payment journeys. It was envisaged that the future use of CoP in relation to these transactions would be considered in a subsequent Phase of work; at which point PSR in conjunction with Pay.uk will have to determine the extent to which CoP should be introduced into all or certain PISP types of payments. Under the current Direction, if Pay.uk were to amend its rules to cover PISP, they would then fall within the scope of Direction 10 and Directed banks would be obliged to introduce the CoP process. Pay.uk have indicated that they will consider this question in the context of Phase II of the CoP programme. Nevertheless, one of the key objectives of this Roadmap evaluation is to inform the circumstances in which it is appropriate and proportionate to introduce CoP interventions.

In its original assessment of the applicable scope of CoP, the PSR recognised that it was not desirable for all transactions to fall within the scope of the CoP process. For example, it was concluded that it was not necessary or desirable to require a CoP process where the funds are being transferred between financial institutions for their own purposes or in connection with other wholesale transactions. In our view the appropriate test of whether or not particular PIS transactions should be subject to CoP interventions is the extent to which a category of PISP transactions is susceptible to APP fraud. The evidence that the application of CoP can effectively mitigate a risk of APP fraud, should be the exclusive determining factor in this evaluation.

Similarly, the overarching principles of the CRM Code are to ensure that end-users of payments are effectively protected from the risk of APP fraud and that interventions in the payment journey are highly correlated to the risks of APP fraud. CRM interventions should be proportionately applied where there is a good basis for determining that they can play a positive role in meeting that objective.

The objective of the current analysis is to determine the extent to which both CoP & CRM interventions can play a significant and useful role in achieving fraud reduction in various PISP journeys.

4.2 Evaluation Approach

We have approached this evaluation as set out in figure 3 below.

Figure 3: Evaluation Process

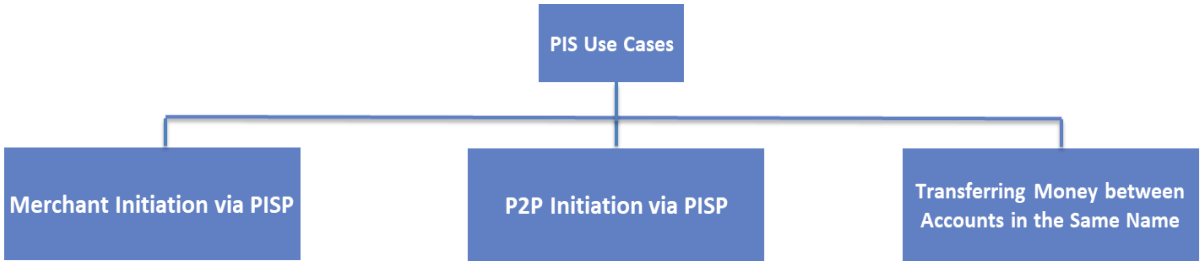
1. There are a range of PISP related use cases. In undertaking this analysis, we have classified these use cases into distinct categories, based on intended purpose.
2. We have identified unique characteristics, relevant for the purpose of this particular evaluation, that are applicable to the identified PISP transaction categories.
3. We have then undertaken analysis to assess the extent of the risk of the occurrence of APP fraud on the basis of the identified attributes applicable to the identified PISP transaction categories.

4. Finally, we have identified key actions, additional to CoP or CRM interventions that could mitigate the risk of APP fraud in various payment journeys. Consideration is given to the extent that it is desirable and proportionate to conclude that these should be considered as essential to embed into the process, additionally or instead of the CoP & CRM intervention.

4.3 PISP Use Case Categorisation

In parallel to work that has been progressed for both the Customer Evaluation Framework and the Consumer Protection Working Group, we have classified PISP propositions in market into 3 broad categories as set out in figure 4.

Figure 4: Categorisation of PIS Use Cases



The characteristics of these transactions are as follows:

4.3.1 Merchant Initiation via PISP (paying for goods or services):

1. The PISP has an underlying contract with the merchant for the provision of PIS payment acceptance services.
2. The PIS payment option is an available option on the merchant's customer facing website.
3. The transaction is a payment to the merchant for specified goods and services comprised in the transaction.
4. There is an integrated check-out and pay facility between merchant and PISP.
6. The PSU initiates a payment order via the PISP, which requires the ASPSP makes a Payment Order via their ASPSP to make a payment to the payee that has a contractual relationship with the PISP and from whom the PSU is purchasing goods or services. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1).
7. In the payment process, within the PISP domain, the PISP prepopulates for the PSU:
    a. The Payee Account Name
    b. The Payee Account Identification details (sort code & account number or full IBAN)
    c. Payment Amount & Currency (GBP for UK implementations)
    d. Payment Reference (optional)
5. The pre-populated fields in 5 above are immutable and cannot be altered by the PSU in the transaction journey.

4.3.2 P2P Initiation via PISP (transferring money to someone else)[3]

1. The PISP does not have an underling contractual relationship with the payee for the provision of PIS payment acceptance services – the relationship is with the payer .
2. There is no integration between the payee and PIS domains.
3. The PSU makes a Payment Order via their ASPSP initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee nominated by the PSU. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1).
4. The PSU populates the payee's details in the payment journey in the PISP domain.
5. The payee details are amendable by the PSU prior to the creation of the Payment Order at the PISP. These details are not amendable in the ASPSP domain (for example in response to CRM warning interventions).

4.3.3 Transferring Money between Accounts in the Same Name (payments between my own accounts)[4]

1. The accounts are in the name of the same PSU held at different institutions.
2. There is no integration between the payee and PIS domains.
3. The PSU can initiate, subject to providing the appropriate consent, an instruction to their ASPSP to make a payment to the other account that they hold. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1).
4. The PSU requires to populate the payee's details in the payment journey in the PISP domain.
5. The payee details are amendable by the PSU prior to the creation of the Payment Order. These details are not amendable in the ASPSP domain. To amend the payee details in the course of the journey (for example in response to CRM warning interventions).

4.4 Propensity to APP Fraud

We have evaluated the propensity of each of the PISP use case category against the two distinct types of APP fraud, namely :

malicious misdirection [5] - This is where the payer authorises a payment to an account the payer believes belongs to a legitimate payee, however, the payer was deceived into inputting the sort code and account number of a fraudster, or an account controlled by a fraudster.

malicious payee - This is where the payer is duped into paying for goods and services, they believe they are legitimately buying, but in fact are being drawn into a scam. The goods and services promised are non-existent and never supplied.

Each of the characteristics of particular use cases have been assessed to determine if they are

[3] This could also be a P2B payment for example paying an individual or business company or a supplier although we anticipate that most P2B transactions will fall within the preceding Merchant Initiation via PISP category.
[4] The evaluation of sweeping is being considered separately
[5] Referred to as "manipulation of the payer by the fraudster to issue a payment order" in the FCA Handbook SUP 16 Annex 27F Notes on completing REP017 Payment Fraud Report

contributing or mitigating factors in relation to APP fraud. The assessment rating is set out in the table below.

Table : Key for criteria assessment

Assessment	Rating
Significantly mitigates the risk of APP fraud	✓✓
Somewhat mitigates the risk of APP fraud	✓
Neutral impact to APP fraud	---
Somewhat contributes to the risk of APP fraud	×
Significantly contributes to the risk of APP fraud	××

4.4.1 Evaluation of Merchant Initiation via PISP (paying for goods or services):

	Characteristic	Implication for APP Fraud	Risk Implication
Malicious Redirection	The PISP has an underlying contract with the merchant for the provision of PIS payment acceptance services (similar to card acquirer)	Extensive due diligence and risk assessment will take place between the PISP and merchant, which should provide certainty that the beneficiary account is associated with a legitimate merchant that is in existence. This prevents fraudulent transfer to a fraudster-controlled account.	✓✓
	The PIS payment option is an available option on the merchant's customer facing website.	Integration gives the consumer confidence that they are engaging in a genuine transaction with a legitimate merchant.	✓
	The transaction is a payment to the merchant for specified goods and services comprised in the transaction.	The payment is exclusively for goods or services the merchant provides and there is complete transparency around purpose of payment and the link to the goods or services to be provided.	✓
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee that has a contractual relationship with the PISP and from whom the PSU is purchasing goods or services. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1).	Currently, the ASPSP will not utilise CoP in the payment process. Consequently, the PSU will not receive CoP mismatch fraud warning interventions. However, this does not increase the vulnerability of these payments to APP fraud, the validity of the payee account and the immutability of the mandate details (as outlined below) significantly reduces this risk and there is no obvious role for CoP warning interventions.	---
	In the payment process, within the PISP domain, the PISP prepopulates for the PSU a) The Payee Account Name b) The Payee Account Identification details (sort	The pre-population of SCAN prevents payments being misdirected due to errors, but in addition prevents the occurrence of Malicious Redirection, because the PSU plays no role in the data entry. While CoP is currently not undertaken by the ASPSP in the payment process this does not introduce additional risk, since the payee details have been previously validated by PISP.	✓✓

	code & account number or full IBAN) c) Payment Amount & Currency (GBP for UK implementations) d) Payment Reference (optional)		
	The payee details are amendable by the PSU prior to the creation of the Payment Order.[6]	The immutability of the payee details prevents intervention to convince the PSU to vary these details so that the payment is directed to an account, controlled by the fraudster.	✓✓
Malicious Payee	The PISP has an underlying contract with the merchant for the provision of PIS payment acceptance services (similar to card acquirer)	Extensive due diligence and risk assessment will take place between the PISP and merchant, which should provide certainty that the beneficiary account is associated with a legitimate merchant that is in existence. This prevents fraudsters from purporting to be a legitimate merchant, when they are not. However, the effectiveness of this as a mitigating factor depends on the robustness of the PISP onboarding procedures. The PISP would be likely to become aware of unsatisfied orders and emergence of customer complaints as fraud was perpetrated allowing early suspension of the payment facility.	✓✓
	The PIS payment option is an available option on the merchant's customer facing website.	In order to perpetrate fraud, the fraudster would have to establish and maintain a fake website. This would impose an additional constraint on the fraudster not applicable to inter-bank payments absent PISP involvement.	✓
	The transaction is a payment to the merchant for specified goods and services comprised in the transaction	The potential for fraud is limited to Purchase & Investment fraud types. The PISP has the potential to monitor merchant websites to identify key indicators of APP fraud.	✓
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee that has a contractual relationship with the PISP and from whom the PSU is purchasing goods or services. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1).	There is no CoP mismatch in these fraud scenarios, so CoP is not a particularly useful tool to detect this form of APP fraud. We conclude therefore that this factor has no appreciable impact on the fraud risk.	---
	In the payment process, within the PISP domain, the PISP prepopulates for the PSU The Payee Account Name The Payee Account Identification details (sort code & account number or full IBAN) Payment Amount & Currency (GBP for UK implementations) Payment Reference (optional)	In the event that the fraudster is able to establish an account that is accepted by the PISP, the prepopulating of these payment details does not have an appreciable effect on the risk of APP fraud. The account controlled by the fraudster will be credited and the goods and services not then supplied.	---
	The payee details are not amendable by the PSU prior to	In the event that the fraudster is able to establish an account that is accepted by the PISP, the	---

[6] If the payment details are changed in the ASPSP domain, the payment initiated would be invalid as the payment order submitted by the PISP cannot be changed in any way.

	the creation of the Payment Order in the TPP domain.	immutability of the pre-populated details in the payment journey does not have an appreciable effect on the risk of APP fraud. The account controlled by the fraudster will be credited and the goods and services not then supplied.	

Observations

The characteristics of Paying for Goods or Services (Merchant Initiation via PISP) and in particular the extent to which the PISP has undertaken independent actions to validate the ultimate payee details plays a key role in ensuring the integrity of those details is a key mitigating effect in relation to **malicious re-direction** fraud. The evaluation processes, provided that they are sufficiently robust (see xx below) have an equivalent effect of a CoP process. Indeed it is reasonable to conclude that they are significantly more effective, since this approach does not rely on the PSU to act on CoP mismatch interventions, which removes any dependency on the PSU to understand and act on any warning interventions in the payment journey. In conjunction with this the inability of the PSU to amend the payee details is an effective countermeasure to any risk of **malicious redirection**, since the fraud is entirely dependent on the fraudster convincing the PSU to amend the payee details.

The susceptibility of this category of transactions to the **malicious payee** fraud is modest. The identified risk is principally that the PISP onboarding processes are insufficiently robust so that nefarious actors are not identified in this process and the fraudster is provided with a payment facility that is endorsed by the PISP.

The logical conclusion of this is that additional CoP checks and CRM warning messages serve no useful purpose and indeed would be confusing for PSUs , who may be using services precisely because it is a more secure.

Recommendations are set out in Section 4.6 as to the steps that PISPs should consider when onboarding to eliminate this risk.

4.4.2 Evaluation of P2P Initiation via PISP (transferring money to someone else)

	Characteristic	Implication for APP Fraud	Risk Implication
Malicious Redirection	The PISP does not have an underlying contractual relationship with the payee for the provision of PIS payment acceptance services.	The additional involvement of the PISP may inadvertently give the PSU reassurance concerning the integrity of the payee, when this is not necessarily warranted since the PISP has not undertaken any due diligence on the payee.	×
	There is no integration between the payee and PIS domains.	This factor has no appreciable impact on the risk of fraud	---
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee nominated by the PSU. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1)	Currently, the ASPSP will not utilise CoP in the payment process. Consequently, the PSU will not receive CoP mismatch fraud warning interventions. This potentially increases the vulnerability of these payments to APP fraud as well as the extent to which PSUs are dissuaded from making fraudulent payments.	××
	The PSU populates the payee's details in the payment journey in the PISP domain. These details are not amendable in the ASPSP domain.	PSU autonomy in varying the payee details introduces a risk of susceptibility to APP fraud in a way inherent in parallel inter-bank journeys. It is not considered to have an exacerbating impact in this use case, however.	---

	The payee details are amendable by the PSU prior to the creation of the Payment Order in the TPP domain.	There is a complexity in the PISP / ASPSP payment journey interaction in that the two-step process to alter the payee details imposes an additional burden on the PSU in a process that is both cumbersome and not intuitive.	××
Malicious Payee	The PISP does not have an underling contractual relationship with the payee for the provision of PIS payment acceptance services	Despite the absence of a direct contractual arrangement the PISP might become aware of unsatisfied orders and emergence of customer complaints as fraud was perpetrated allowing blacklisting of certain payee accounts.	✓
	There is no integration between the payee and PIS domains.	This factor has no appreciable impact on the risk of fraud	---
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee nominated by the PSU. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1)	There is no CoP mismatch in these fraud scenarios, so CoP is not a particularly useful tool to detect this form of APP fraud. We conclude therefore that this factor has no appreciable impact on the fraud risk.	---
	The PSU populates the payee's details in the payment journey in the PISP domain. These details are not amendable in the ASPSP domain.	PSU autonomy in varying the payee details does not introduce any additional risk as the integrity of the payee rather than the legitimacy of the payee's account details are in question is not in question, but rather introduces a risk of susceptibility to APP fraud in a way inherent in parallel inter-bank journeys. It is not considered to have an exacerbating impact in this use case however	---
	The payee details are amendable by the PSU prior to the creation of the Payment Order in the TPP domain.	In the event that the fraudster is able to establish an account that is accepted by the PISP, the immutability of the pre-populated details in the payment journey does not have an appreciable effect on the risk of APP fraud. The account controlled by the fraudster will be credited and the goods and services not then supplied.	---

Observations

Our expectation is that most P2B transactions will fall within the preceding Merchant Initiation via PISP category. However, there will be examples of payments to businesses e.g. payments to tradesmen etc that fall within this category. The characteristics of Transferring Money to Someone Else (P2P Initiation via PISP), where the PISP has not independently validated the authenticity of the Payee and the PSU is responsible for inputting the payees details are largely similar to comparable inter-bank payment journeys and are equally susceptible to fraud. The fact that CoP is not currently utilised in these journeys, in our view, exacerbates that risk in relation to ***malicious redirection***. While the volume of PISP payments is reasonably small at present, low volumes of fraud have been reported. However, it is possible that the volume of APP fraud will increase as volumes grow. It is reasonable to assume that this may be exacerbated by the fact that CoP is not applied in these journeys given that fraudsters commonly target their activities in areas where countermeasures are least developed.

CoP is not an effective counter-measure in relation to ***malicious payee fraud***, since this type of fraud is not reliant on persuading the PSU to make a payment to an unintended payee and in these cases the fraudster has established an account the details of which entirely correspond to the payee account information that the payer has.

CRM warning intervention, on the other hand can act as a useful counter-fraud measure in these payment journeys and it is desirable that CRM messaging is appropriately incorporated wherever there are good grounds to do so. Our observations on effective warnings are set out in Section 5 below.

4.4.3 Evaluation of Transferring Money between Accounts in the Same Name (payments between my own accounts)[7]

	Characteristic	Implication for APP Fraud	Risk Implication
Malicious Redirection	The accounts are in the name of the same PSU held at different institutions.	There is some emerging evidence that fraudsters are increasingly encouraging victims to move funds between various accounts they hold at different institutions to engender confidence on the part of the PSU as to the legitimacy of such requests (e.g. the funds remain in the PSUs control in the initial phases of the scam) and to exploit differences in the effectiveness of APP fraud counter-measures adopted by different firms. This transaction type may therefore become increasingly more susceptible to fraud.	×
	There is no integration between the payee and PIS domains.	This factor has no appreciable impact on the risk of fraud	---
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the PSU's other account. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1)	Currently, the ASPSP will not utilise CoP in the payment process. Consequently, the PSU will not receive CoP mismatch fraud warning interventions. This potentially increases the vulnerability of these payments to APP fraud, where the PSU has been persuaded in the process to remit money to an account which is purported to be their account but is in fact not.	××
	The PSU populates the payee's details in the payment journey in the PISP domain.	PSU autonomy in varying the payee details introduces a risk of susceptibility to APP fraud in a way inherent in parallel inter-bank journeys. It is not considered to have an exacerbating impact in this use case.	---
	The payee details are amendable by the PSU prior to the creation of the Payment Order. These details are not amendable in the ASPSP domain. To amend the payee details in the course of the journey (for example in response to CRM warning interventions).	There is a complexity in the PISP / ASPSP payment journey interaction in that the two-step process to alter the payee details imposes an additional burden on the PSU in a process that is both cumbersome and not intuitive.	××

[7] The evaluation of sweeping is being considered separately

Malicious Payee	The accounts are in the name of the same PSU held at different institutions.	This type of fraud requires a payment to a third party. In these circumstances the PSU is transferring funds to another account that they hold. This does not support the intended objective of the fraudster and is not congruent with the scenario presented to the victim. There is no evidence of fraud of this nature.	✓✓
	There is no integration between the payee and PIS domains.	This factor has no appreciable impact on the risk of fraud. As set out above there is very little risk of malicious payee fraud in this payment type.	---
	The PSU initiates a payment order via the PISP, which requires the ASPSP to make a payment to the payee nominated by the PSU. The ASPSP does not utilise CoP in the payment journey (as referenced in Section 3.1)	This factor has no appreciable impact on the risk of fraud. As set out above there is very little risk of malicious payee fraud in this payment type.	---
	The PSU populates the payee's details in the payment journey in the PISP domain	This factor has no appreciable impact on the risk of fraud. As set out above there is very little risk of malicious payee fraud in this payment type	---
	The payee details are amendable by the PSU prior to the creation of the Payment Order. These details are not amendable in the ASPSP domain. To amend the payee details in the course of the journey (for example in response to CRM warning interventions).	This factor has no appreciable impact on the risk of fraud. As set out above there is very little risk of malicious payee fraud in this payment type	---

Observations

Our analysis suggests that the characteristics of transferring money between accounts held by the same payer does mean that these payment journeys are susceptible to ***malicious re-direction*** fraud. However, the occurrence of APP scams between accounts held by the same beneficial owner are relatively uncommon. Nevertheless, there are examples of fraud occurring where the fraudster purports to be from the victim's bank and convinces the victim to make a payment to an account that the victim believes is their own but is in fact an account that the fraudster controls.

There is emerging evidence that fraudsters are increasingly encouraging victims to move funds between various accounts they hold at different institutions to engender confidence on the part of the PSU as well as in an attempt to target as to the legitimacy of such requests (e.g. the funds remain in the PSUs control in the initial phases of the scam) and to exploit differences in the effectiveness of APP fraud counter-measures adopted by different firms. From the sending & receiving banks perspective, the inter-account transfers that precede the fraud in these situations, are ostensibly legitimate and don't result in a fraud loss. However, it may be of benefit to provide warning

interventions that alert potential victims to the risk. Fraud of this nature relies on extensive "grooming" of victims, playing on their vulnerabilities. The views we have heard suggests that where a victim has been lured into the scam, it can be challenging to break "the spell". Targeted repeated warnings are desirable in these scenarios seem proportionate. While we have no empirical evidence to support the assertion that additional friction is unlikely to significantly increase transaction abandonment where payments are being made to other accounts that the payer holds.

What is more certain is that a CoP mismatch when establishing a new payee, who is the same beneficial owner of the payer account, is a key indicator of APP fraud risk. The fact that CoP is not currently utilised in these journeys, introduces a risk in these transaction types which may be increasingly open to exploitation by fraudsters in future. Fraud is commonly targeted in areas where countermeasures are least developed.

In contrast, ***malicious payee fraud*** is predicated on the victim transferring funds to a payee for good or services, which are never rendered or for a purpose e.g. romance scams that is predicated on deception by the fraudster. The common factor is that the payee is invariably a 3rd party. Payment to that 3rd party underpins the fraud. We conclude that it is improbable that **malicious payee** fraud will take place in relation to these payment types and the risk is low. CRM warning interventions are not considered necessary or proportion interventions as a countermeasure to **malicious payee** fraud, given the low risk of this in these payment journeys.

As previously outlined , CoP is not an effective countermeasure in relation to **malicious payee** fraud, since this type of fraud is not reliant on deceiving the PSU in relation to the payee details.

Our preliminary conclusion is that the risk of APP fraud in these transaction types is comparable with that in other inter-bank payment transactions and that consequently the inclusion of both CoP and CRM warnings interventions (either by PISP or ASPSP) is warranted and should provide a reasonable counter-measure if implemented effectively . Observations on how to optimise approaches to effective interventions, based on the body of research undertaken are set in Section 5.

4.5 Summary Conclusions

Based on our evaluation we have reached preliminary conclusions as to the susceptibility of the three identified use case categories to each type of APP fraud. Our summary conclusions are summarised in the table below .

	Merchant Initiation via PISP	P2P Initiation via PISP	Transfers between accounts in the same name
Malicious Redirection **Fraud Risk**	No	YES	YES
Malicious Payee **Fraud Risk**	No	YES	No
CoP as Countermeasure	✘	✓	✓
Effective Warnings as Countermeasure	✘	✓	✘

- Our preliminary conclusion is that the risk of APP fraud in **Merchant Initiation via PISP** is exceptionally low and that the inclusion of both CoP and CRM warnings interventions (either by PISP or ASPSP) will not materially reduce the risk. To that extent the use of CoP in these transactions is unwarranted and would introduce:
    - inappropriate and unnecessary friction that is disproportionate to any potential benefit.
    - additional unnecessary cost and effort to PISP and/or sending bank without incremental benefit; and
    - risk of degradation to the overall effectiveness of warning interventions based on the emerging evidence from our experimental research that indicates that unnecessary overuse of warning interventions erodes their broader effectiveness.
- Conversely, our preliminary conclusion is that the risk of APP fraud in relation **to P2P Initiation via PISP** that these transaction types is comparable to other inter-bank payment transactions. Consequently, the inclusion of both CoP and CRM warnings interventions (either by PISP or ASPSP) is warranted and should provide a reasonable countermeasure if implemented effectively. This is not withstanding that there are regulatory challenges for COP being performed in the ASPSP domain e.g. the PSU cannot edit the payment order including the payee in the domain of the ASPSP. The fact that on an existing basis CoP is not being utilised in these journeys is likely to exacerbate that risk. Although there is no existing evidence that this is resulting in the occurrence of fraud, could pose some medium to long terms risk of fraud migration.
- CoP should be used when a new payee is established to make a payment of this type. CRM warnings should be used in the course of each executed payment. Observations on how to optimise approaches to effective interventions, based on the body of research undertaken are set in Section 5.
- Finally, our analysis of the characteristics **of transferring money between accounts held by the same payer** does mean that these payment journeys could be susceptible to **malicious re-direction** fraud, albeit to a modest extent but not **malicious payee** fraud. Consequently, we conclude that it would be beneficial to ensure that CoP should be applied to these transactions, when a new payee is established to make a payment

4.6 Merchant Initiation – Consideration of Additional PISP Requirements

We noted in our evaluation of **Merchant Initiation via PISP** that the due diligence and risk assessment of the merchant , with whom they have a contract is a key mitigant to the potential for APP fraud. This should provide assurance that the beneficiary account is associated with a legitimate merchant. This prevents fraudulent transfer to a fraudster-controlled account, which is a key feature of APP fraud. It is on this basis that we have provisionally concluded that neither CoP nor CRM warning interventions need to be embedded within these journeys. The rationale for this conclusion is that if the TPP undertakes an appropriate degree of due diligence in this area and the payee details are immutable in a payee journey that this essentially eradicates the risk of APP fraud (and error).

Consequently, it is important for the PISP to properly assess each merchant that they on-board and undertake the necessary checks to ensure appropriate validation of payee accounts.

We believe that as a minimum the PISP should undertake a rigorous assessment of the merchant, including the following activities:

- An assessment against the PISP's criteria for accepting merchants e.g. acceptable business types, time in business, location, sales volumes, and financial track record.
- Undertaking a commercial credit report from an FCA regulated Credit Reference Agency or Credit Information Service Provider.
- Interrogation of Companies House Data.
- Perform a robust review of the merchant's location, establishing whether the company and website are in fact legitimate.
- Review any discrepancies in trading or customer reviews using Third Party and Vendor Screening solutions.
- Perform an AIS consent journey to obtain the following information from their ASPSP(s) - Sort-code, account number, account name, where the entity holds the requisite regulatory permission to do so.
- Where the entity is not authorized as an AISP undertake verification of account details in other ways, e.g. validation of copies of their bank statement during the onboarding process.
- Use the 'account name' obtained as described above to populate the payee details, ensuring that there is no mechanism available to the PSU to over-write or amend the pre-populated details either accidentally or via fraudulent manipulation of the PSU.

It is recommended that these, together with any other potential requirements identified in the consultation, are integrated into the requirements of Pay.uk and the LSB and are potentially included as requirements to qualify for any exemption from applying CoP or CRM effective warning innervations, as set out in our related recommendations.

4.7 Recommendations

On the basis of the preceding evaluation we recommend that :-

1. Pay.uk should in the context of their CoP Phase 2 work relating to PISPs amend their rules to clarify that CoP should not be applied when a new payee is established in the course of a Merchant Initiation via PISP payment journey, where the receiving bank is a CoP participant, but should be applied to the other two categories of PISP transactions.
2. The LSB revise their Practitioners Guidance (and/or the CRM Code) to clarify that effective warnings, as defined in the CRM Code should: these transactions, but should be applied to the other category of PISP transactions:

    i) ***should not*** be applied to Merchant Initiation via PISP payment journey

    ii) ***should not*** be applied to Transferring money between accounts in the same name

    iii) ***should*** be applied to P2P Initiation via PISP

3. OBIE develop appropriate technical Standards to enable PISPs to identify the sub-category that a PISP payment falls in so that the ASPSP is able to refrain from applying CoP and CRM warning interventions when making the payment that has been initiated by the merchant.

Consultation Questions:

Question 1: Do you agree with our analysis of the susceptibility of each of the 3 PISP use case categories to APP fraud? Please give reasons for your answer.

Question 2: Do you agree with our preliminary conclusions and recommendations as to the effectiveness and necessity for CoP in each of the 3 PISP use case categories? Please give reasons for your answer.

Question 3:

(i) Do you agree that there should be specific requirements relating to the onboarding and validation of payee accounts by PISPs offering Merchant Initiation via PISP?

(ii)Do you agree with the proposed requirements? Are there any additional requirements that should be included? Please give reasons for your answers.

5. Effective CRM Warnings

5.1 Evaluation Objectives

As set out above , our preliminary conclusions are that in two categories of PISP transaction, CoP and CRM warning interventions do provide a benefit and should, where well designed have a positive appreciable effect on the incidence of fraud. A key objective of the current Evaluation is to explore the extent to which these interventions can be optimised so that they increase consumer attention, reduce fraud, and improve the overall consumer experience.

A recent thematic review of effective warnings undertaken by the LSB concluded that there was scope for improvement and that many firms were in the process of reviewing the warnings they have in place and many had change programmes underway with a view to improving the design and impact of warnings. The thrust of this evolution is intended to create more dynamic and targeted warnings. They noted that good progress was generally being made, but that there is still work to be done to meet all the requirements of the Code and reach a situation where all firms are displaying warnings which are effective in making a customer stop to carefully consider whether the payment should be made. The LSB noted firms should attempt to find a balance between displaying impactful warnings and not having too much friction in the payment journey for genuine transactions.

In that context, we considered that it would be informative to commission consumer research based on behavioural science principles, the objective of which would be to identify improvements to warning interventions that are likely to increase consumer attention, identification of fraud and improve the overall consumer experience. These warnings were tested in a large-scale online randomised controlled trial, designed to provide robust evidence as to what works. We engaged Professor John Gathergood, a leading expert in the field of Behavioural Science who has undertaken extensive research for the FCA, CMA and others, to oversee the research design and peer review the results.

The intention is to distil the findings of this piece of research and provide relevant recommendations to the LSB to inform development of the Code addressing effective warnings. The LSB's work in this area has not involved the commissioning of consumer research. Instead, their approach to the Thematic Review was to assess the systems, processes and controls in place relating to the creation and implementation of warnings, how the effectiveness of the warnings were evaluated and how firms

have tailored warnings to the specific nature of the scam , which is a requirement of the Code. One of the primary conclusions of the Review was that "The content of warnings still requires further development across all nine firms. Firms are at different points in the evolution of warnings, but all require some element of improvement. Firms are not always using the data and MI available to help enhance and improve warnings."[8] We anticipate that the robust empirical findings provided by this research exercise will be useful to inform the enhancements to warning interventions that Code participants are embarked on and potentially to enable the LSB to develop relevant elements of Practitioner Guidance.

5.2 Experimental Design Summary[9]

Two separate experiments were undertaken. Both involved recruiting subjects to take part in an online survey in which they were presented with information about several hypothetical payments and were asked to complete payment journeys via an app that was accessible within the survey. Participants were incentivised to behave as they would in the real world. They maximised their earnings if they made 'legitimate' payments and earnings were reduced if they made 'fraudulent' payments.

In the first experiment, participants were able to make these payments using a fictitious mobile banking app. Subjects were presented with various payment scenario descriptions together with associated evidence (e.g., email receipts, invoices), and invited to make the payment using the mobile banking app. Participants were randomly allocated to groups that were shown different types of warning interventions. Each participant was shown the same warning intervention in each of the payments they were asked to make.

The "control" group was shown a hybrid version of current CMA9 effective warnings. There were 7 other groups who were exposed to modified warning interventions that incorporated various combinations of the following elements:

1. A risk-based approach involving presenting warnings only when they were considered higher risk . These groups were further subdivided into:
    a. high accuracy, meaning that the risk-based approach did not misclassify high-risk scenarios as low-risk or vice versa.
    b. low accuracy, meaning that the risk-based approached produced some false positives (i.e., classified legitimate scenarios as being risky).
2. Inclusion of opportunity for Calls to Action (CTAs); this involves including more 'buttons' within the app that let participants cancel a payment, save the payment for later, or make a call to the bank.
3. Inclusion of 'behavioural interventions' (e.g., the app includes text that leverages loss aversion by stating that they might *lose* a given amount of money if they proceed).

We recruited 10,000 participants for this experiment. The sample was nationally representative of the adult UK population.

[8] Lending Standards Board Contingent Reimbursement Model Code for Authorised Push Payment Scams Thematic review of provision SF1(2) – Effective warnings Summary Report December 2020

[9] see Research Report for details

In the second experiment, participants were able to make these payments using a PISP app. Participants were randomly allocated to groups that were exposed to three distinct variants :

Variant 1: A version where COP and CRM appear when authorising the payment using the bank app

Variant 2: A version where COP appears in the PISP app, and CRM appears when authorising the payment using the bank app

Variant 3: A version where COP and CRM appear in the PISP app

We recruited 3,000 participants for this experiment, nationally representative of the adult UK population. Subjects were presented with the control journey used in the first experiment.

5.3 Experimental Results Summary[10]

The experimental design allowed us to isolate and identify the efficacy of the warning variants while also measuring whether there are interactive effects (e.g., whether the combination of certain variants works better). The principal measure was the extent to which participants completed fraudulent and legitimate payments. Secondary outcomes of interest include whether participants liked the app, and the time it took to complete a payment and whether there was evidence of fatigue etc.

The results are as set out in the table below

Table: Preliminary results of effectiveness

	Share that made a fraudulent payment (& increase/reduction)	Average share of legitimate payments made (increase/reduction)
Average in the control group	22%	57%
Control + behavioural	18% (-18%)	51% (-11%)
Control + CTA	10% (-55%)	43% (-25%)
Control + behavioural + CTA	8% (-64%)	37% (-35%)
Risk-based	23% (+5%)	65% (14%)
Risk-based + behavioural	23% (+5%)	67 (18%)
Risk-based + CTA	4% (-82%)	50% (-12%)
Risk-based + behavioural + CTA	6% (-73%)	49% (-14%)
Observations	8507	8507

The key findings are that several of these treatments (7) had a statistically significant effect on the share of subjects that made a fraudulent payment. The size of these effects is large, which provides some confidence in the results . The 'Risk-based + CTA' group had the largest effect, reducing the number of fraudulent journeys made by 82% relative to the control group. This means that only 4% of participants in this group fell for fraud. The second-most successful intervention was the 'Risk-based + behavioural + CTA' group (73% reduction). Introduction of the 'CTA' element seems to have a major impact on the share that fall for fraud, regardless of whether it is placed in context with a risk-based approach or in an app with behavioural interventions. This was supported in some of the qualitative data collected during the experiment, which suggested that typically when consumers are embarked on a payment journey, they have some sense of urgency and commitment to complete the task. There is rarely any obvious route to abandon or defer a payment journey once it is commenced and PSUs are hesitant to do so, particularly where they have some uncertainty as to the status of the payment if

[10]please see Research Report for details

the break away from it mid-point. Saving payment details was the most utilised CTA (10%) compared to cancelling or contacting the bank (1-3%).

The objective of warning messages is to encourage consumers to better consider the risks associated with the transaction that they are undertaking . We have heard effective warnings described as the mechanism by which the spell cast by fraudsters can be broken. The provision of a clearly defined and permitted "escape route" , where the payer starts to have some doubts relating to the payment seems to be a highly effective mechanism to decrease the extent to which the payer makes a fraudulent payment.

An interesting observation is that in addition to being the most effective treatment from a fraud detection perspective, the 'Risk-based + CTA' group was also the most preferred option when subjects were asked for their qualitative feedback on the journeys that they had undertaken. 72 percent of users said they would prefer the 'Risk + behavioural + CTA' journey to their existing bank payment journey. It is helpful in this context that there is no trade off required between effectiveness and customer experience, this approach achieves both.

As noted above the research was also designed to provide a more nuanced understanding of the impact of accuracy in the presentation of risk-based warnings. We fully appreciate that in a live environment it would be impossible to accurately risk-assess every transaction and present an appropriately tailored intervention.

The groups presented with risk-based warnings were subdivided. One group was presented with highly accurate warnings in which fraudulent transactions were properly classified as high risk, while the other group were presented with misclassified fraudulent scenarios as low-risk or vice versa. The research found little evidence that varying the accuracy of the risk-based approach has a significant effect on the share of fraudulent journeys that participants completed. However, we did find that the accuracy of the risk-based approach influenced the likelihood that people completed legitimate journeys (i.e., if it was less accurate, they completed around 3 percentage points fewer legitimate journeys).

We did not find that the treatments had any significant effects on the amount of time that it took for participants to complete the payments. The 'Risk + behavioural + CTA' version of the intervention also scored the best on customer satisfaction and usability metrics. However, there was some evidence in some of the experimental arms that the repeated overuse of warnings, in the absence of a risk based approach led to process fatigue that over the course of the experiment led the subject paying less attention to the warnings and reducing their effectiveness. Individuals may be 'desensitised' to the warnings conveyed in the payment journey after having gone through the same warnings in preceding scenarios, making the warnings less effective if fraud appears in a subsequent scenario.

Further analysis including an interactivity analysis to understand if the efficacy of the treatments depended on whether participants were exposed to fraud in the first, second, or third scenario is being undertaken. We intend to publish the results of this in the second phase of consultation.

We note that while the CTA interventions generated large reductions in the share that fall for fraud, they also had an unintended side effect: they reduced the share of legitimate payments that individuals complete. Further in-depth analysis is also being undertaken to analyse this effect, which will be presented in the next phase of our consultation. However, we would urge caution in interpretation of the data. The very nature of the experimental design necessarily involved presentation of payment scenarios that would be perceived as " high risk". The results are therefore likely to be directional but would not necessarily reflect impacts where used in a broader range of more typical payment types that customers would undertake in reality.

The results of the second experiment are set out in the table below.

Table: PISP variants

	Share that made a fraudulent payment	Average share of legitimate payments made
Average in the Variant 1 group (bank only)	20%	65%
Variant 2 (CoP by PISP)	26% (30%)	64% (1.5%)
Variant 3 (CoP & CRM by PISP	21% (5%)	62% (5%)
Observations	1478	1478

We found that 20% of participants in the Variant 1 group (COP and CRM in the bank app) fell for fraud. This statistic is similar to the share that fell for fraud in the control group in experiment 1 (22%). Further, we find that individuals completed around 65% of legitimate payments in the Variant 1 group (this statistic is slightly larger than the average in the control group in experiment 1).

Variant 2 increased the share of individuals that fell for fraud by approximately 6 percentage points. In other words, more participants fell for fraud when the responsibility for COP was assigned to the PISP, rather than the bank. We did not find that ***Variant 3*** (when both COP and CRM were assigned to the PISP) had a significant effect relative to ***Variant 1***.

Our preliminary conclusion is that it is detrimental for CoP and CRM warnings to be presented separately in the bank and PISP environments , although it makes little difference whether they occur in either environment. Neither variant had a significant effect on the share of legitimate payments that participants completed.

Both Variant 2 and 3 performed slightly worse than ***Variant 1*** in terms of participants' subjective usability scores (e.g., whether it was easy to cancel payments, whether the app felt safe, and whether the app felt intuitive to use). However, participants were equally likely to say that they would use ***Variant 1 as Variants 2 and 3*** if given the chance.

The results from experiment 2 should, however, be treated with a degree of caution as at the time of writing , we have not yet analysed the full results from the entire sample. Further analysis will be presented in the second phase of consultation.

5.4 Preliminary observations

The results of this research demonstrate that enhancements to warning interventions have potential to significantly increase PSU detection of APP fraud. The largest effects are achieved when introducing CTAs that offer PSUs the opportunity to cancel and defer payments.

We note that this finding is consistent with an observation made by the LSB in the context of their Thematic Review who found varying approaches to how customers were able to abort transactions following the provision of warnings within digital channels. Their recommendation is that options "should both be clear and prominent, ensuring a customer is able to make an informed choice about whether to proceed or not". We found that a separate option to save payment details but to defer payment, potentially allowing the PSU time to investigate the authenticity of the transaction was a preferred CTA. Our view is that PSUs may be more inclined to take this action on the basis that the effort they have expended on inputting payment details is not wasted, which would be the case if the transaction is cancelled or abandoned.

We also note that there is some evidence that a risk-based approach, which provides more targeting of interventions such that warnings are presented more sparingly is likely to improve their effectiveness. Even when the risk-based approach is used in isolation from other treatments, there is no statistical meaningful degradation in detection, while participants completed a much higher proportion (65%) of legitimate payments. It should be noted in this context that the approach to risk-assessment within the context of the hypothetical scenarios presented in an experimental context are necessarily much less refined than would be possible in a live environment, where a wealth of additional data relating to customer and payee transaction profiling would be important components of any risk assessment. It should also be noted that the nature of the payment transactions, even for legitimate payment journeys, presented in the experiment were high risk.

We note that this finding sits somewhat at odds with the LSB's provisional findings that emerged from their Thematic Review. They identified the approach that some firms were taking in setting a threshold payment amounts, below which no effective warning is given, as potentially resulting in " a lack of protection for victims of lower value fraud and to inconsistency in customers receiving warning messages which in turn may result in unfair customer outcomes". Transaction value, in our view is likely to be a significant, although not the only, indicator of APP fraud risk. We have presented these findings to the LSB and committed to engaging in more detailed discussion with them.

As noted above, furthermore detailed analysis of this piece of research is currently underway and we will publish more extensive conclusions in the course of our consultation. We will also study the generalisability of the results, conduct benefit cost analyses, and will and provide more detailed recommendations.

This will inform the recommendations that we ultimately make. It is our intention to consult further on these.

The preliminary results of experiment 2 suggests that it does not make a big difference if the responsibility for COP and CRM are allocated to a bank or a PISP. However, it does suggest that it is detrimental to split the responsibility between the two parties. Further analysis is also taking place in relation to any recommendations flowing from these finding. Nevertheless, our provisional conclusion is that there is likely to be benefits from a fraud reduction perspective in enabling PISPS, to play an autonomous role in the presentation of CoP and CRM messaging. The possible approaches to achieving this are discussed in more detail below.

Consultation Questions:

Question 4: Do you have any observations on the preliminary conclusions of this research? Are they corroborated by any proprietary research or review of the design and impact of warnings?

Question 5: Do you have views on the feasible of introducing Call to Action features in the payment process ? Please give reasons for your answer.

Question 6: Do you have views as to whether it would be constructive to include key conclusions of the research as recommendations to the LSB to add as good practice guidelines within the CRM Code & Practitioners Guidance? Please give reasons for your answer.

6.Direct Participation of PISPs in CoP

6.1 Option Evaluation

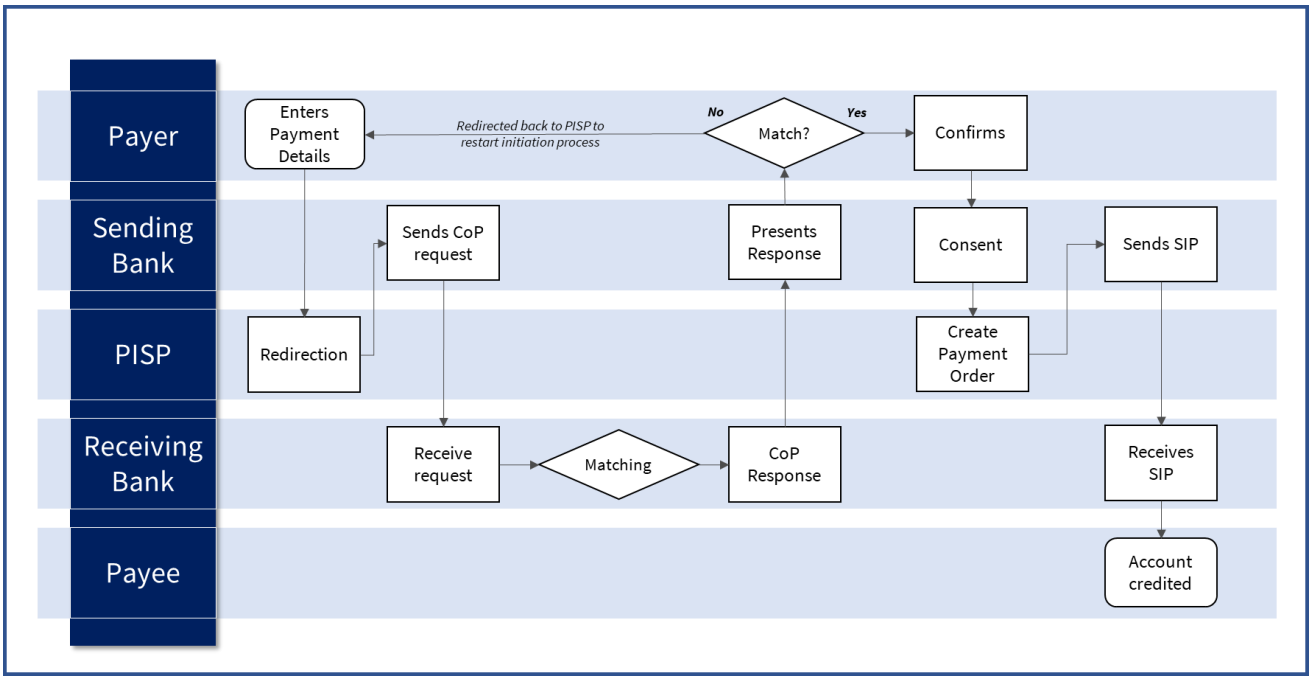
Enrolment and participation in CoP is currently limited to FCA regulated firms who are :

- An ASPSP with its own allocated sort code allocated with its own sort-code in the Extended Industry Sort Code Directory (EISCD)
- Existing participants of Open Banking

Currently, ASPSPs that do not have a sort code allocated to them and non-ASPSPs e.g. PISPs are not eligible to participate. Pay.UK will be developing an extended CoP proposition for these types of firms in the course of 2021, within the scope of Phase 2.

There are three possible approaches to incorporating CoP requests in PIS journeys as set out below:

Option 1: CoP call by Sending Bank after authentication



In this model the Payer's ASPSP always makes the CoP request and processes the API Request and Response.

Step 1 : The PSU confirms payment details with PISP.

Step 2: The PSU is redirected to the ASPSP to authenticate

Step 3: The Sending Bank makes a CoP call to the Receiving Bank.

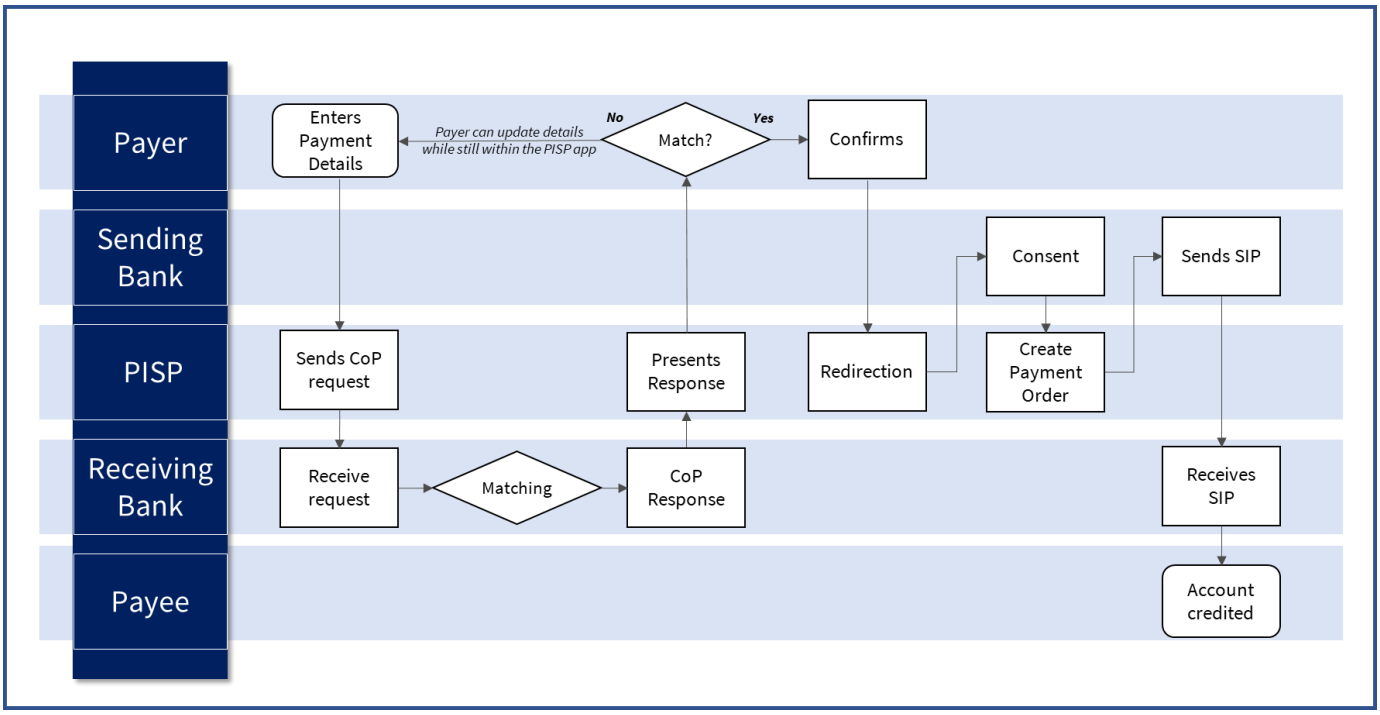
Step 4: The ASPSP displays the results of the CoP to the PSU, with options to proceed or cancel.

Step 5: If PSU confirms, they are directed to PISP for confirmation that payment has been made , if the PSU cancels, they are redirected to the PISP to edit the payment details.

Key features :

- The PISPs does not need to become a CoP participant
- Liability for APP fraud remains entirely with ASPSPs
- CoP is performed on each PISP initiated transaction in line with the proposed requirements set out in Section 4 above.

Option 2: CoP call by PISP



In this model the PISP always makes the COP request directly to Payee ASPSP Payer's

Step 1 : The PSU confirms payment details with PISP.

Step 2: PISP makes the CoP call directly to the Receiving Bank

Step 3: PISP displays the CoP response to the PSU with option to proceed or cancel.

Step 4: If PSU confirms, they are directed to the Sending bank to authenticate . If the PSU cancels, they are able to edit payment details in the PISP app and resubmit a CoP call .

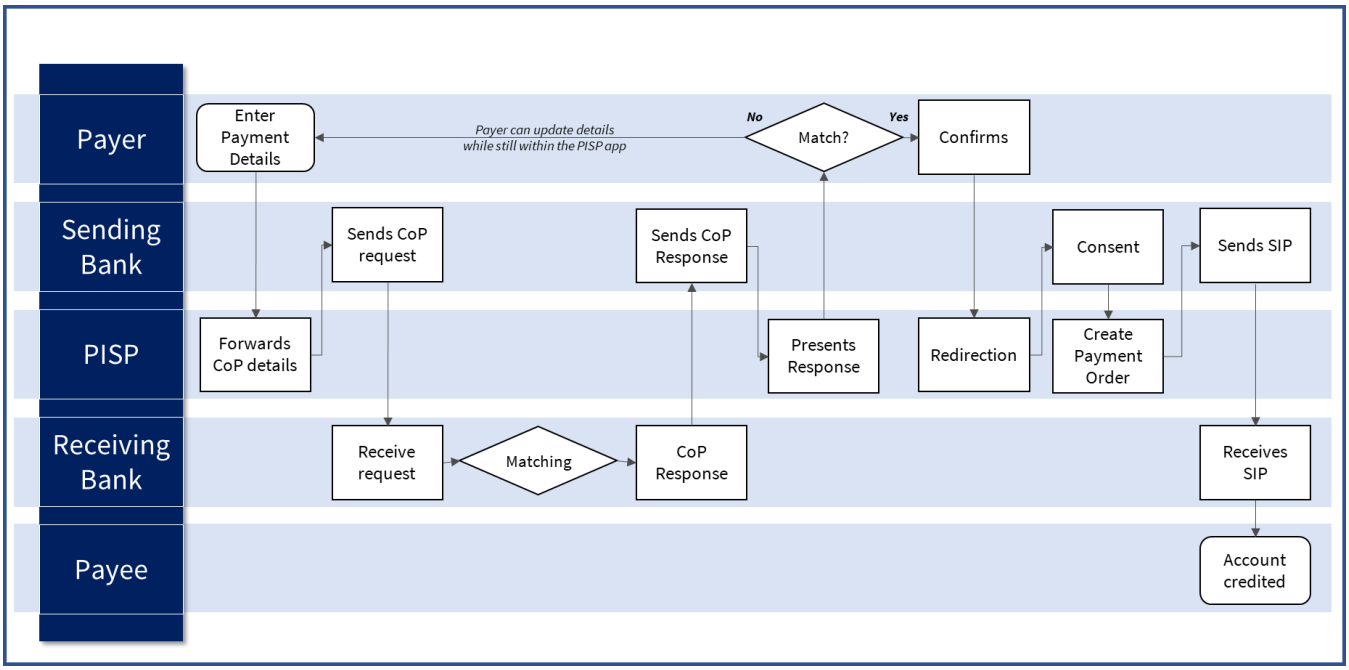
Step 5: PISP confirms payment made.

Key features :

- PISPs would potentially be liable if they present the CoP response incorrectly to the PSU

- PISPs would be liable for APP fraud arising from the failure of a PSU to act on warning interventions provided in the payment message relating to CoP mismatch, subject to the provisions of the CRM Code.
- PISPs must sign up as CoP participants
- PISPs must be signatory to the CRM Code at least to the extent that APP fraud that is preventable by CoP.
- PISP needs to build, test and maintain CoP technical integrations

Option 3: CoP call by Sending Bank before authentication



In this model the PISP always makes the COP request directly to Payee ASPSP Payer's

Step 1 : The PSU confirms payment details with PISP.

Step 2: Sending Bank makes the CoP call to the Receiving Bank and responds to PISP with CoP message (in the response to POST payment-order-consent).

Step 3: PISP displays the CoP response to the PSU with option to proceed or cancel.

Step 4: If PSU confirms, they are directed to the Sending bank to authenticate . If the PSU cancels, they are able to edit payment details in the PISP app and resubmit a CoP call .

Step 5: PISP confirms payment made.

Key features :

- The CoP request is completed by the Payer ASPSP before redirection.

- Customer only transferred to ASPSP after completing the CoP request.
- Liability is less easy to apportion as PISP handles customer messaging, but ASPSP processes the API Request and Response. Liability potentially split between PISP and ASPSP.
- PISPs may not need to become full CoP participants

6.2 Observations

The purpose of this consultation is to assess the extent to which the three options outlined above should be progressed by Pay.uk . It is envisaged that the first option - CoP call by Sending Bank after authentication should be an available option. It is envisaged that the other alternative options that involve the transfer of liability to the PISP may be attractive to some, but not all, PISPs. This option is therefore an appropriate fall-back mechanism that enables the integration of CoP messaging into relevant PIS journeys that have been identified as susceptible to APP fraud and would benefit from the introduction of CoP. This will require the development of new Pay.uk standards rules and procedures. It will also require existing CoP participants to undertake development work to embed the required changes to support PISPs.

The other two options are more complex to implement as the Pay.uk standards and rules will also need to be modified to define liability between various parties, notably :-

- Between the PISP and other CoP participants in situations where a party does not fully comply with the applicable rules and standards in a way that exposes one of the parties to potential or actual loss.
- Between the PISP and the Sending Bank, where the Sending Bank is relying on the PISP to undertake the CoP call and present the results to the PSU, where each has existing contractual relationships with the PSU.
- Between the PISP, Sending Bank and the PSU, where APP fraud arises that could have been prevented by the effective application of CoP.

It is acknowledged that the associated issues are complex to resolve.

Options 2 & 3 will also require :

- Pay.uk to admit and accredit a new participant type and address contractual considerations, including Data Protection.
- The development of technical Standards that enable the Sending Bank to identify that a CoP has been made by the PISP so that it is unnecessary for the Sending Bank to replicate that activity.

As previously noted, the PSR's Specific Directions relating to the application of CoP do not currently extend to PISP payments, on the basis that Pay.UK rules and standards have not been developed to cater for these transaction types. It is likely that the issue of the Scope of SD10 for the Directed participants will need to be revisited in the event that several of these options are introduced. This is particularly relevant if their introduction is phased. The current view is that introducing any new requirements for certain PISP journeys, would have implications across the entire spectrum of PISP transactions.

Consultation Questions:

Question 7: Do you agree with our conclusion that there are 3 possible approaches to incorporating CoP requests in PIS journeys? Are there alternative options that could be considered?

Question 8: Is there commercial appetite to use each of these potential solutions to justify their development? Please give reasons for your answers.

7. Direct Participation of PISPs in CRM Code

The provisional conclusions arrived at in the preceding sections of this document suggest that that it would be beneficial to include Effective Warning Interventions in certain types of PISP payments. Furthermore, the research into effective warnings suggests that where these were presented in the PISP domain they tended to result in a higher level of customer attention to the warnings, which resulted in greater number of subjects identifying APP fraud. On this basis , we can see a credible case for PISPs to play an autonomous role in the provision of effective warnings in defined transactions. We concluded from previous discussions with the PISP community that there was interest from some PISPs who had the capability to identify APP Scam risk indicators in developing a model that would enable them to provide appropriate customer fraud warnings in preference to relying on the ASPSP, in order to avoid increased risks of disruption to customer journeys. However, this was not a universally held view and there was recognition that this may result in consequences for liability for any APP fraud.

Participation in the CRM Code is voluntary. At its introduction, and prior to it falling under the remit of the LSB, eight banks were signatories of the Code. A further bank has joined. Extending participation in the Code is a key activity for the LSB and supports the PSR's key objective to ensure that as many customers as possible have access to the protections afforded by the Code.

The LSB is currently consulting on potential revisions to the Code as part of a first post-implementation review. This includes consideration of challenges or barriers which specifically may exist that would prevent PISPs from becoming a signatory to the Code, for example because they are unable to meet the requirements of the Code as it currently stands. The specific needs and constraints of PISPS were not considered within the original development of the Code. As the LSB looks to extend participation within the Code to a wider range of participants, including PISPs, there is an increasing need to identify and address components of the Code that may act as potential barriers to PISP participation.

A fundamental requirement of the Code is that, with a number of exceptions (where the customer has not heeded warnings or has been grossly negligent), , firms should reimburse the Customer when he/she has been the victim of an APP scam. We note that PISPs are not required to validate customer's identities in the same way or to the same extent as the Sending Bank. The authentication process in the PIS payment flow is intended to provide the reassurance as to the authenticity of the PSU. Consequently, in some business models the PISP may not be able to identify the customer and validate a claim. We consider that where the PISP is in this situation it is unlikely to be able to reliably fulfil this component of the Code. Our provisional view is this would be a significant impediment that will preclude the PISP from participation as a direct subscriber to the Code.

OBIE has reviewed the current version of the Code and has identified a number of current provisions that it recommends components, that in our view would be difficult for PISPs to conform with. These are set out below.

Code Component	Constraints
GF1. Firms should participate in coordinated general consumer education and awareness campaigns .	This a desirable objective but has been formulated within the Code on the basis that the original signatories of the Code are large organisations with a significant reach – 95% of PCA customers and are suitably resourced and skilled to deliver undertake a variety of financial education initiatives. It is noted that the relevance of APP fraud for PISP transactions differs across different business models and that for some PISPs a key element of the proposition, which will be part of their marketing message, is how their approach minimises APP fraud. The messages applicable to their customers may need to be specifically tailored to find an appropriate balance between warning messages where the PISP is developing a new payment channel, unfamiliar to customers. It is **recommended** that the LSB revise this requirement of the Code so that the focus is on the firm providing relevant information to customers to educate customers of the risks that are relevant to the business model of the participating firm. There may be opportunities for industry -level customer awareness activities to be co-ordinated via relevant trade associations , rather than by individual TPPs.
GF2. Firms should collect and provide statistics on APP scams to their relevant trade bodies.	It is envisaged that PISPs who become signatories to the Code should collate relevant data, where they are potentially handling incidences of APP fraud from transactions initiated on behalf of their customers. The requirements of the Code currently envisage that data will be provided to UK Finance, who currently collate APP fraud MI. PISPs may not be members of UK Finance. They may be members of other Trade Associations e.g. FDATA, EMA or EPA. None of these currently plays a role in the collation and reporting of APP fraud. It is **recommended** that the LSB agree the role that UK Finance will play in the collation and reporting of APP fraud data and how that can extend to firms operating in the payment sector, but who are not members of UK Finance. Alternatively, the PSR and/or FCA might usefully look at how data can be effectively collated across a broader range of participants. Furthermore, it is **recommended** that the LSB in conjunction with UK Finance and regulators develop reporting requirements for PISPs to ensure that APP fraud reported by PISPs is not simultaneous reported by the ASPSP. As the PISP is not involved in the settlement of transactions, it possible that the PSU will contact the ASPSP if APP fraud occurs. The LSB Practitioners Guidance should set out the key processes and responsibilities of both the PISP and ASPSP in these circumstances.
GF3 (a). Firms should take reasonable steps so that Customers who have been victims of an APP scam, can better to protect themselves.	We note in the context of Merchant Initiation via PISP models the PISP has the contractual relationship with the payee (merchant) rather than the PSU. However, even in other PIS models the nature of the relationship between PSU and PISP is likely to be very different to the relationships between the PSU and their bank. It is probable that they will undertake transactions less frequently with individual PISPs . Our view is that PISPs do not have the capability to reliably do this because of the limited information that they hold on the PSU and their overall payment behaviour. There is no current process for ASPSPs to communicate concerns to PISPs re particular customers.

	It is **recommended** that the LSB revise this requirement of the Code so that the requirements on PISPs is to advise customers of the risks inherent in particular transactions that they are undertaking rather than their previous behaviour.
SF1. Firms should take appropriate action to identify Customers and payment authorisations that run a higher risk of being associated with an APP scam	As previously noted, the nature of the relationship between PSU and PISP is likely to be very different to the relationships between the PSU and their bank. It is by its nature an entirely on-line relationship with a narrower purpose than the provision a broader range of financial services . Our view is that PISPs will not necessarily have the capability or customer behaviour analytics to reliably identify customers who are at a greater risk of susceptibility to APP fraud, because of the limited information that they hold on the PSU and their overall financial situation. TPPs also have less access relevant data to inform an extensive risk assessment. For example, they don't see customer's typical spending patterns that would enable identification of abnormal behaviour. PISPs will typically rely on relatively simple velocity monitoring to identify fraud, absent other relevant data. Currently ASPSPs are not sharing "real-time" risk analysis from their fraud monitoring systems, which would contribute to a risk assessment. It is **recommended** that the LSB revise this requirement of the Code and/or the Practitioners Guidance to clarify that there are reduced requirements on PISPs in relation customer susceptibility, and instead their primary focus should be on risk-based assessment of the transaction itself. In this regard the LSB should clarify that it is a requirement for PISPs to monitor customer activity, which will include identification of abnormal activity, but this is limited due to the PISP having only a sub-set of the spending behaviour.
SF1(4).Firms should apply additional measures to protect Customers that are, or may be, vulnerable to APP scams	As previously noted, the nature of the relationship between PSU and PISP is likely to be very different to the relationships between the PSU and their bank. It is by its nature an entirely on-line relationship with a narrower purpose than the provision a broader range of financial services . Many models are based on obtaining minimal information on PSUs in line with data privacy / GDPR constraints. It is unlikely that ASPSPs would be able to legitimately communicate data that would be needed to identify vulnerability. It is **recommended** that the LSB revise this requirement of the Code and/or the Practitioners Guidance so to recognise these constraints and acknowledge that the nature of the PIS product makes the identification of vulnerability (for the purpose of susceptibility to APP fraud) unlikely and therefore the identification of vulnerability will be the exception rather than the rule.
SF1 (5). Where a Firm has sufficient concern that a payment may be an APP scam, it should take appropriate action to delay the payment while it investigates.	The PISP able to initiate a payment order, with the PSU's explicit consent, from their online payment account held at their ASPSP. The nature of PIS does not allow. The PSUs is required to authenticate with the ASPSP to make the payment. there is no opportunity within this process (governed by PSD2) for the PISP to pend or delay the payment.

	It is **recommended** that the LSB revise this requirement of the Code and/or the Practitioners Guidance to clarify that a PISP does not require to delay the payment pending investigation and instead faces a binary decision as to proceed or not.
SF1 (6). Where an APP scam is reported to a Firm, the sending Firm should notify any UK receiving Firms in accordance with the procedure and timeframes set out in the Best Practice Standards	The PISP will not have a direct relationship with the Receiving Bank as it is not involved in the settlement of the underlying transaction . The Sending Bank has that relationship. It is **recommended** that the LSB revise this requirement of the Code and/or the Practitioners Guidance to clarify the mutual roles of the PISP, Sending Bank and Receiving Bank in this process.
R2 Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer	Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer. We note that PISPs are not required to validate customer's identities in the same way or to the same extent as the Sending Bank. The design of PIS is predicated on the authentication process in the payment flow to provide the reassurance as to the authenticity of the PSU, who has already been validated by the Sending Bank in their on-boarding process. This means that at least in some in some business models, the PISP may not be able to identify the customer and validate a claim. We **conclude** that where the PISP is unable to reliably fulfil this component of the Code, that this would preclude the PISP from participation as a subscriber to the Code.

Consultation Questions:

Question 9: Do you agree with our conclusions that there are particular aspects of the existing CRM Code that potentially act as barriers to PISP participation ? Are there others? If so, please describe.

Question 10: Do you agree that the LSB should consider modifying these barriers. Would this encourage PISPs to subscribe to the Code?

Question 11: Do you have any other comments on the Consultation?

Appendix 1 List of Consultation Questions

Question 1: Do you agree with our analysis of the susceptibility of each of the 3 PISP use case categories to APP fraud? Please give reasons for your answer.

Question 2: Do you agree with our preliminary conclusions and recommendations as to the effectiveness and necessity for CoP in each of the 3 PISP use case categories? Please give reasons for your answer.

Question 3:

(i) Do you agree that there should be specific requirements relating to the onboarding and validation of payee accounts by PISPs offering Merchant Initiation via PISP?

(ii)Do you agree with the proposed requirements? Are there any additional requirements that should be included? Please give reasons for your answers.

Question 4: Do you have any observations on the preliminary conclusions of this research? Are they corroborated by any proprietary research or review of the design and impact of warnings?

Question 5: Do you have views on the feasible of introducing Call to Action features in the payment process ? Please give reasons for your answer.

Question 6: Do you have views as to whether it would be constructive to include key conclusions of the research as recommendations to the LSB to add as good practice guidelines within the CRM Code & Practitioners Guidance? Please give reasons for your answer.

Question 7: Do you agree with our conclusion that there are 3 possible approaches to incorporating CoP requests in PIS journeys? Are there alternative options that could be considered?

Question 8: Is there commercial appetite to use each of these potential solutions to justify their development? Please give reasons for your answers.

Question 9: Do you agree with our conclusions that there are particular aspects of the existing CRM Code that potentially act as barriers to PISP participation ? Are there others? If so, please describe.

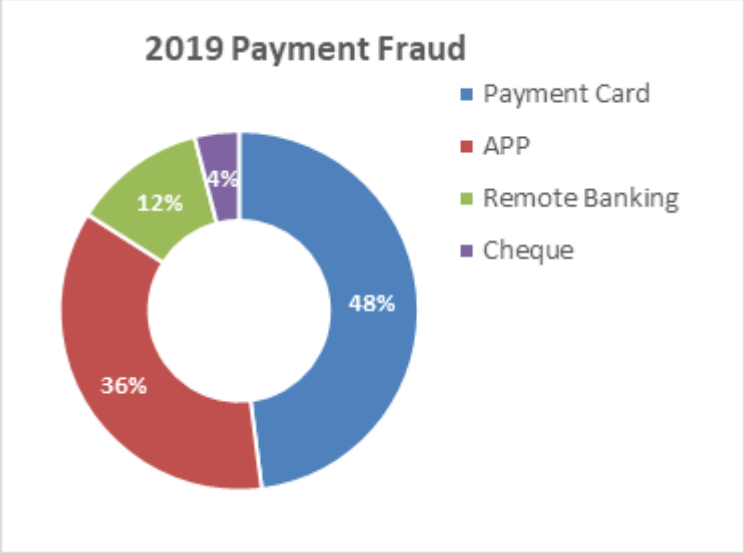
Question 10: Do you agree that the LSB should consider modifying these barriers. Would this encourage PISPs to subscribe to the Code?

Question 11: Do you have any other comments on the Consultation?

Appendix 2 Market Analysis (Source UK Finance)

In 2019 there were 122,437 incidents of Authorised Push Payment (APP) scams with gross losses of £455.8 million. 70% of APP fraud losses and over 93% of cases were attributable to personal customers. The value of losses increased by 29% between 2008 and 2019, while the number of cases rose by 45%. APP fraud now accounts for 36% of all payment fraud in the UK as set out in ***figure 5.***

Figure 5



The volume and value of APP is growing. The number of cases grew by 45% in the year to end 2019, while the total value of fraud increased by 29% as set out in ***figure 6.***

Figure 6

	2017	2018	2019
APP Fraud Cases	65,812	123,675	185,449
Value £m	236.0	354.3	455.8
Repatriation £m	60.8	82.6	116.0
Average loss per case £	**3,586**	**2,865**	**2,458**

There are two distinct types of APP fraud:

Maliciously misdirected – the payer thinks they are paying a legitimate payee but is instead deceived into transferring the funds to a different person.

Malicious Payee - The Customer transfers funds to a payee person for what they believe is legitimate purposes, but which is in fact fraudulent.

UK Finance has established 8 specific subsets of APP fraud. The value and number of fraud cases applicable to each of these categories is set out in in *figure* 7 & 8.

Figure 7

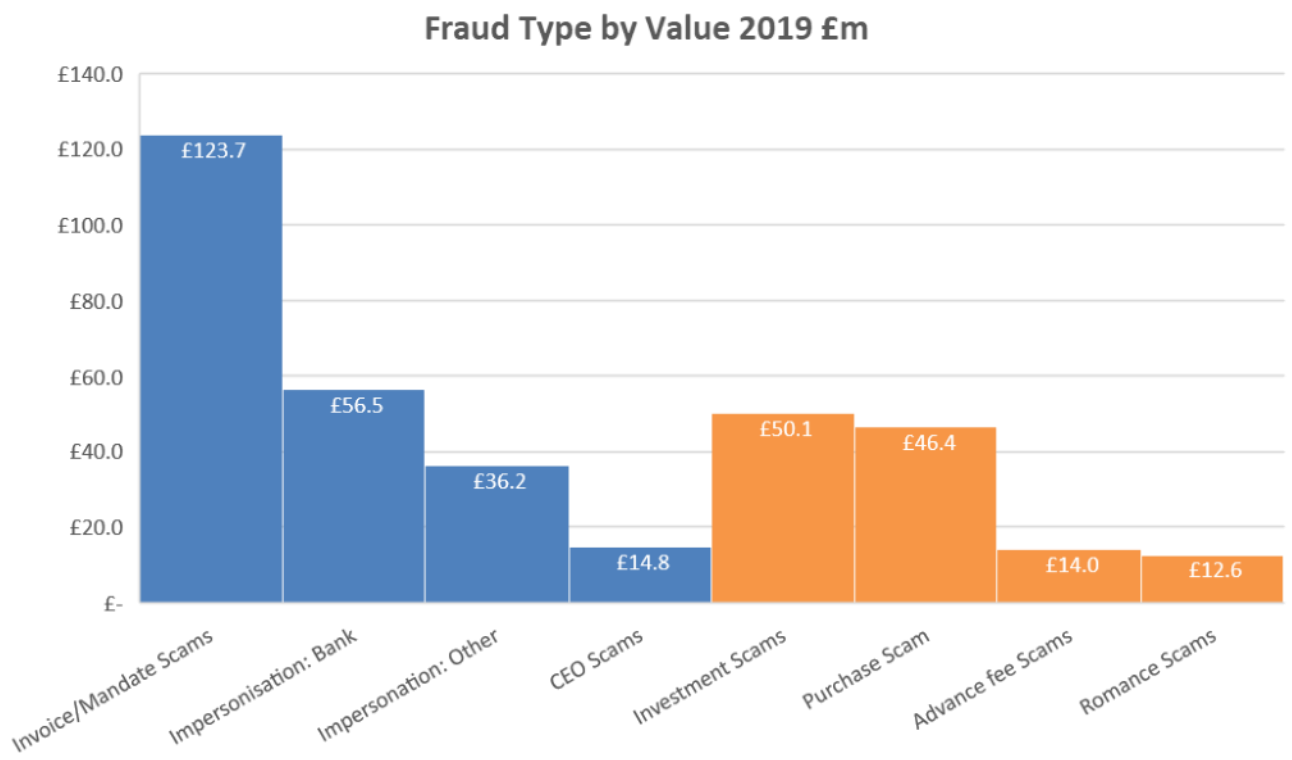


Figure 8

		Cases
Malicious Redirection	Invoice/Mandate Scams	7,544
	Impersonation: Bank	5,459
	Impersonation: Other	5,465
	CEO Scams	603
Malicious Payee	Investment Scams	3,385
	Purchase Scam	56,621
	Advance fee Scams	8,133
	Romance Scams	1,404

There is a considerable variation in the average APP fraud loss across each of these categories. The average value of each APP fraud payment and the distribution of losses by value band is set out in figure 9 & 10.

Figure 9

	2019 vs 2018		
	Volume	Value	Ave. Loss
Invoice & Mandate Scams	16%	-8%	£ 9,949.42
Impersonation : Police/ Bank Staff	156%	49%	£ 3,778.08
Impersonation : Other	75%	39%	£ 3,282.12
CEO Fraud	16%	20%	£ 18,503.12
Investment Scams	79%	90%	£ 6,707.45
Purchase Scams	39.6%	27%	£ 633.59
Advance Fee Scams	29%	23%	£ 1,005.61
Romance Scams	45%	44%	£ 1,642.92

Figure 10