

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

Draft Standards

Date : 07 07 2021
Version : 01.2
Classification : LIMITED

CONTENTS

| | | |
|-------|---|----|
| 1 | Executive Summary | 4 |
| 2 | Background | 5 |
| 2.1 | Use Cases | 6 |
| 2.2 | Confirmation of Payee | 6 |
| 2.3 | Contingent Reimbursement Model (CRM) Code | 7 |
| 3 | Proposition | 9 |
| 3.1 | Scope | 9 |
| 3.2 | Status of this draft standard | 9 |
| 3.3 | Ecosystem consultation | 10 |
| 4 | Analysis of Effective Warnings | 11 |
| 4.1 | Experiment 1 – generic anti-fraud interventions | 11 |
| 4.2 | Experiment 2 – Intervention touchpoints | 12 |
| 4.3 | Study results | 12 |
| 5 | Customer journeys | 14 |
| 5.1 | Generic Customer Journeys | 15 |
| 5.1.1 | COP Generic outcomes | 15 |
| 5.1.2 | Generic CRM outcomes | 17 |
| 5.1.3 | CoP Call by ASPSP during authentication | 18 |
| 5.1.4 | CoP Call by ASPSP before authentication | 19 |
| 5.1.5 | CoP call by PISP | 20 |
| 5.1.6 | CRM warning by PISP | 21 |
| 5.2 | Recommended Customer journeys | 22 |
| 5.2.1 | Risk specific responses | 24 |
| 5.2.2 | Alternative Calls to Action | 26 |
| 5.2.3 | Behavioural warnings | 27 |
| 5.2.4 | COP + CRM together / PISP vs ASPSP | 28 |
| 5.2.5 | Risk + CTA + Behavioural | 30 |
| 5.3 | Product Requirements for Standards | 31 |
| 5.4 | Assumptions | 33 |
| 5.5 | Dependencies | 33 |
| 5.6 | Constraints | 33 |
| 6 | Implications for API Standards | 34 |
| 6.1 | Payment sub-category | 34 |
| 6.1.1 | Proposition Statement | 34 |

| | | |
|-------|---|----|
| 6.1.2 | Required Changes | 34 |
| 6.2 | COP Check by PISP | 35 |
| 6.2.1 | Proposition Statement | 35 |
| 6.2.2 | Required Changes | 35 |
| 6.3 | PISP Request to ASPSP to carry out COP check | 36 |
| 6.3.1 | Proposition Statement | 36 |
| 6.3.2 | Required Changes | 36 |
| 6.4 | Transmission of COP result from ASPSP to PISP | 37 |
| 6.4.1 | Proposition Statement | 37 |
| 6.4.2 | Required Changes | 38 |
| 6.5 | Guidance on COP/CRM | 38 |
| 6.5.1 | Proposition Statement | 38 |
| 6.5.2 | Required Changes | 38 |
| 6.6 | Indication from PISP to ASPSP on display of CRM | 38 |
| 6.6.1 | Proposition Statement | 38 |
| 6.6.2 | Required Changes | 38 |
| 7 | Appendix | 39 |
| i. | Roadmap Reference | 39 |

1 Executive Summary

Item A2(d) of the [May 2020 CMA Order Roadmap](#) specified a need to “ensure maintenance of low-friction, no obstacle customer journeys that take account of the requirements of the Contingent Reimbursement Model (CRM) code and Confirmation of Payee (CoP)”.

There were 149,946 recorded incidents of authorised push payment (APP) scams in 2020, causing losses of around £479 million (UK Finance, 2021). Fraudsters groom and manipulate people into transferring money or divulging their personal and financial details. For example, the criminal may pose as a bank, the police, a retailer, utility company or government department.

The growing losses from APP fraud prompted the financial industry, in conjunction with regulators to launch key counter- initiatives. In February 2018, the Payment Systems Regulator established a steering group to develop an industry code now known as the Contingent Reimbursement Model (CRM). The CRM code sets out consumer protection standards related to the reimbursement of victims. Another was the introduction of Confirmation of Payee (CoP), helping customers verify the account details they enter.

The Evaluation sought to establish how CoP and CRM can be most appropriately embedded into open banking 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 overriding objective is to ensure that how CoP and CRM are implemented is proportionate and maximises their effectiveness. The output of this Evaluation was 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.

At the conclusion of the Evaluation, the Trustee instructed OBIE to develop draft technical standards and Customer Experience Guidelines to support implementation of all possible models identified in the Evaluation process. It is still too soon to determine which of these models will ultimately be required, but the existence of these draft standards will assist Pay.UK and the LSB as they progress their own work in relation to this.

In the course of the Evaluation the OBIE commissioned an extensive behavioural study to explore the impact of on-screen interventions intended to prevent APP fraud in digital payment journeys. In a randomised controlled trial of over 13k participants we tested new designs against customer journeys currently live in the marketplace. The study design was conducted by The Behaviouralist, an external agency specialising in behavioural, data science, economic theory, and strategic design.

The findings of the study demonstrate that small changes to payment apps have the potential to significantly reduce the share of individuals that fall for APP fraud. The biggest affects were achieved by presenting alternative outcomes in the app, offering users options to cancel or defer payments, alongside buttons for completing the payment. Further improvements came from a risk-adjusted response, and targeted loss-framed warnings.

This draft standard encapsulates these findings and has been developed in consultation with both the LSB and Pay.uk.

2 Background

The OBIE has completed its Evaluation of this Roadmap item and presented its Final Report including Recommendations for approval by the Trustee. These were tabled for discussion at IESG on 28 April 2021.

The Trustee noted that OBIE had consulted widely not only with the ecosystem, but also with Pay.UK and the LSB, the entities with ultimate responsibility for the development of CoP and the CRM Code. The Trustee has approved a number of Recommendations, including:

A2021/4 11. The OBIE must develop standards for publication in draft by end June 2021. These standards include:

- Technical standards to address the identified models set out in the OBIE Final Report dated April 13th, 2021. These must address the development of 'flags' to provide the ASPSP with certainty as to which model was being used, who was performing the CoP check and potentially the result of that check. This to include consideration of circumstances where a bilateral agreement may be in place between participants governing the application of effective warnings.
- Technical standards for an additional open banking payment model that incorporates a background CoP call, the result of which is provided to the TPP, but not to the PSU, which could be used in "Merchant Initiated" open banking payment journeys, where the PISP has a contractual relationship with a merchant. . (For the avoidance of doubt, these are draft standards only, and would only become final standards following the outcome of Pay.uk and LSB work and following consultation).
- Customer Experience Guidelines, supporting all identified models and the additional model described in A2021/4 12 (2), with a greater focus on unhappy paths where there is no CoP match. This will include suggested approaches to the presentation of warning interventions for both CoP and CRM that emerged from the consumer research undertaken, and to assist the LSB.

This document sets out the changes to the Standards that we consider necessary to support the various models identified in the Evaluation.

2.1 Use Cases

This table defines the key use cases, and indicates those that are covered in this document.

| ID | Description | Met |
|----|--|---------------|
| 1 | As a Merchant providing integrated checkout and payment facility to customers via PISP, I do not want to perform CoP checks of my payment account with the customer's bank every time a payment is made as the PISP has verified it as part of onboarding process. | Not addressed |
| 2 | As a PISP, providing payment facility to customers, I would like to verify the beneficiary and show appropriate CoP warnings/messages to the customer before payment is initiated with the bank. | Fully |
| 3 | As an ASPSP, I would like to receive requests from PISPs to not verify the beneficiary before executing the payment order and provide appropriate response back. | Fully |
| 4 | As a PISP, providing payment facility to customers, I would like to request the ASPSP to verify the beneficiary and show appropriate CoP warnings/messages to the customer either before or during authentication. | Fully |
| 5 | As an ASPSP, I would like to receive requests from PISPs to verify the beneficiary before executing the payment order and provide appropriate response back. | Fully |

2.2 Confirmation of Payee

<https://www.wearepay.uk/confirmation-of-payee/>

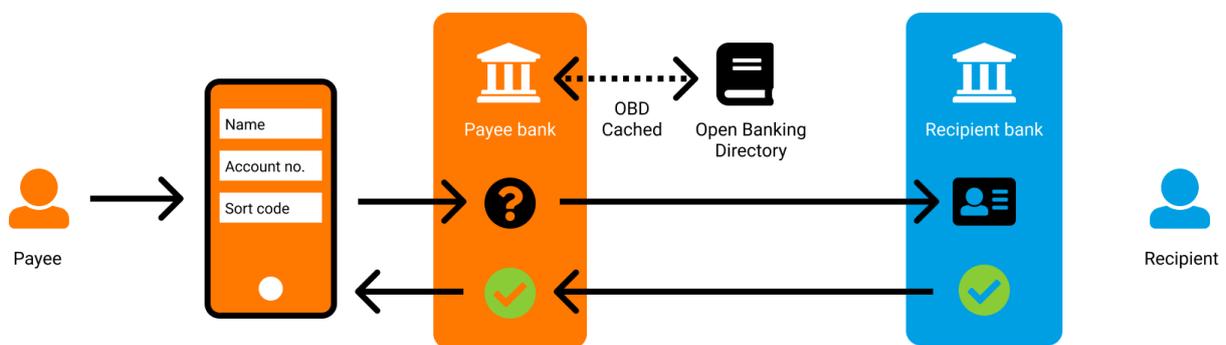
Confirmation of Payee (CoP) is a mechanism designed to give end-users assurance that they are making payments to the intended recipient. Customers setting up a new payee will now be able to confirm that the name they've entered matches the one on the account they're intending to pay. It addresses both 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.

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.

Figure 1: CoP Process Flows



2.3 Contingent Reimbursement Model (CRM) Code

<https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/#contingent-reimbursement-model-crm-code>

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'. 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. 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.

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 this year.

UK Finance 2020 Types of APP Scam

| Type of scam | Communication channel | Volume (share) | Av. Loss (share) | Overview |
|-----------------------------------|-----------------------|----------------|------------------|--|
| Invoice & mandate | Email | 7k (9%) | £16k (35%) | Victim intercepted with a request to make payment to a new account |
| Impersonation: bank staff, police | Phone/SMS | 5k (6%) | £10k (16%) | Victim urged to transfer funds to 'safe' account |
| Impersonation: HMRC, utilities | Phone/SMS | 5k (6%) | £16k (35%) | Victim asked to pay overdue tax or penalty |
| CEO | Phone/email | 600 (1%) | £24k (4%) | Impersonates victim's CEO to make urgent payment |
| Purchase | Ecommerce | 56k (64%) | £800 (13%) | Goods or services paid for, never delivered |
| Investment | Online ad | 3k (4%) | £14k (14%) | Fictitious investment scheme |
| Advance fee | Online ad | 8k (9%) | £2k (4%) | Small payment, to receive a larger sum |
| Romance | Social media | 2k (2%) | £9k (4%) | Emergency loan after romantic relationship is established |

3 Proposition

Roadmap item definition

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

The objective of this Roadmap item is to develop standards for the CMA9 to implement Confirmation of Payee (CoP)ⁱ and Contingent Reimbursement Model (CRM)ⁱⁱ in their PIS customer journeys and provide customer experience guidance to ensure low friction journeys consistent with the regulatory requirements of CoP and CRM Code.

3.1 Scope

This proposition is to develop standards that enable:

- a. PISPs to notify the ASPSP that they have verified the payee directly so that it is unnecessary for the payer's ASPSP to replicate the verification by making a CoP call to the payee's ASPSP.
- b. PISPs to request the payer's ASPSP to verify the payee and provide a response prior to making a payment.
- c. PISPs to notify the ASPSP that they have done their own risk-based evaluation and shown appropriate CRM warnings to the PSU as part of the payment initiation, or if they have not.

The proposition will present multiple options in which this can be done and provide recommendations for low friction customer experience journeys based on learnings from the behavioural consumer research study conducted by OBIE.

3.2 Status of this draft standard

The Roadmap item envisaged that Final Standard would be published with mandatory implementation by the CMA9. In the course of the evaluation it has become apparent that concurrent activities are being undertaken by the LSB, Pay.UK and the PSR that are considered likely to have implications for the standards that OBIE develop. The timings and inter-dependencies between these related activities mean that it would be premature for OBIE to implement standards for mandatory implementation at this time.

We noted in the Final Report that it is still too early to fully assess the extent to which PISPs may choose to implement CoP, if they were able to. Further evaluation of this will be required for the possible models of CoP integration into open banking journeys. Similarly, further work is being undertaken to address integration of CRM effective warnings to inform the considerations of the LSB in this area.

The Trustee has agreed the following approach to the further development of the Final Standard :

- **A2021/4 12.** When the activities being undertaken by the Lending Standards Board to review the CRM Code are finalised, OBIE should consult on revisions to the standards (including Customer Experience Guidelines) to enable the CMA9 to implement customer warnings in such a way that does not create obstacles to the provision of payment initiation services.
- **A2021/4 13.** The OBIE must work with Pay.UK and PSR to agree timeline for the enablement of inclusion of open banking payments within Confirmation of Payee rulebook, following which the OBIE must modify the draft standards following consultation so that they are consistent and compatible with the CoP rulebook, and do not create obstacles to the provision of payment initiation services. Final standards will then be published. Implementation requirements must consider the outcome of Roadmap Item A10 (Sweeping).

3.3 Ecosystem consultation

Refer to [CoP-CRM Consultation Paper 20210201 Final.pdf](#) for details on analysis and research on CoP and CRM.

4 Analysis of Effective Warnings

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 this year.

The conclusion of the LSB's thematic review was that there was scope for improvement in the use of warning interventions intended to act as a countermeasure to APP fraud. They noted that 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 commissioned 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.

Together with John Gathergood of Warwick University, and The Behaviourist we conducted a wide study of the effects of anti-fraud interventions in digital payment journeys.

We recruited nationally representative samples of UK adults and allocated them randomly to different experimental conditions. Participants were asked a number of questions defining their demographic and use of online banking. Each was presented three payment scenarios, described in detail with supporting assets like email and text communications. They conducted the payments using a prototype payment app and had the choice to complete or abort each.

Participants understood that the payment requests might not all be legitimate. To simulate real-world caution, they lost part of their fee if they made a 'fraudulent' payment and earned more if they completed legitimate ones.

Individuals were randomly allocated to groups that would see different variants of the payment app. Those allocated to the control group saw fraud interventions that mirrored current approaches in the market. The other groups saw the same app, with the addition of new tactics to encourage critical thinking around the details of the payment scenario.

The study comprised two online experiments that separately tested key dimensions of the solution.

4.1 Experiment 1 – generic anti-fraud interventions

This concerned the design of generic Confirmation of Payee (CoP) and Contingent Reimbursement Model (CRM) interventions in payment initiation journeys. It was designed so that the findings could apply equally to any payment journey, whether pure-play banking journey, or end-to-end fintech app.

Around 10,000 participants took part in this study, and were randomly allocated to the following cohorts:

Group 1 – Control

An aggregation of interventions that occur in current payment journeys. These present the same journey for every payment and tend to depend on a copy-heavy approach, with few interactive options.

Group 2 - Behavioural (Loss aversion and social norms.)

This variant closely resembled the ‘control’ variant, but with the addition of messaging that emphasises the possible losses the consumer might incur.

Group 3 - Call to Action (CTA)

Here we added salient calls to action (or buttons) that offered users alternative options to cancel or postpone payments.

Group 4 Behavioural and CTA combined

Showed an app that combined the features of the behavioural messaging and CTA .

Group 5-8 Risk appropriate

These groups repeated variants of the previous groups, with the addition of a risk-based response. This meant that apparently legitimate payments presented minimal interventions, but warnings were triggered when payments were calculated as particularly suspicious by the PSP.

4.2 Experiment 2 – Intervention touchpoints

Participants in the second experiment were randomly allocated one of three conditions. These were designed to test where the interventions were most effective: local to the third party PISP app, or in the ASPSP bank app where the user authenticates the payment.

Group 1 – Current state control

Those in the first condition were asked to complete payments using a prototype journey, with CoP and CRM placed on the bank side as they authenticated their payments.

Group 2 – Split across PISP and ASPSP

Those in the second condition were shown the CoP warnings in the PISP app, and the CRM warnings in the bank app.

Group 3 – CoP and CRM PISP side

Finally, those in the third condition were shown both the CoP and CRM warnings in the PISP app.

4.3 Study results

The empirical analysis of the experimental data yielded a number of key findings.

Alternative calls to action

The CTA intervention had dramatic effects on the share that fell for fraud. Those in group three (the CTA group) were 54% less likely to fall for fraud than those in the control group. The CTA intervention did not update individual's beliefs regarding the probability a payment scenario was fraudulent - suggesting that it changed behaviour by simply making it easier for individuals to act on their suspicions. This intervention also improved participants perceptions regarding the user-friendliness of the app.

Behavioural warnings

The loss framing and social reinforcement reduced the share of participants that fell for fraud to 18%, where 22% fell for fraud in the control group. However, these effects likely decay with time; the warnings successfully prevented fraud when they occurred in the first and second scenario but did not impact if the third scenario was fraudulent. Individuals seem to get used to the warnings and start ignoring them, suggesting that such warnings should be used sparingly (i.e. risk appropriate).

Combined CTA and behavioural messaging

While the CTA and behavioural interventions successfully reduce APP fraud, they might do so at a slight cost--both intervention types made participants less likely to complete legitimate payments within the experiment. However, the legitimate payments presented in the experiment were what could be described as 'high risk' payments - by design so it was not straight forward for the subject to ascertain whether they were suitable to complete. So, we have reasonable confidence that the interventions would not negatively impact the completion of straight forward day-to-day banking transactions.

Risk appropriate responses

The risk-based approach did not significantly influence the likelihood that individuals fell for fraud. That said, the risk-based approach did make individuals significantly more likely to complete legitimate payments. This result makes intuitive sense, as the main feature of the approach was to remove warnings when they were deemed unnecessary. It suggests that the ideal approach may be to combine the CTA intervention with a risk-based approach, to reduce APP fraud without impacting the completion of legitimate payments.

Intervention touchpoints

Finally, the second experiment shows that it does not make a meaningful difference if the responsibility for CoP and CRM occurs in the banking app or the PISP. But it did suggest that it is detrimental to split the responsibility between the two parties, i.e. the CoP warning on the PISP side and the CRM in the bank. Splitting the interventions in this way made participants around 37% more likely to fall for fraud.

In summary, the results showed the number of scams detected during payment journeys dramatically increased when Call to Action (CTA) interventions were presented, offering users more opportunities to cancel or defer transactions throughout the payment journey. The largest effects were achieved when a combination of risk-based and CTA warnings were implemented, without negatively impacting the completion of legitimate payments. The targeted use of interventions using a risk-based approach also prevented a decay in their effectiveness over time.

5 Customer journeys

This section contains a series of guidelines for the deployment of anti-fraud measures in digital payment journeys. As the OBIE we are primarily concerned with open banking journeys which are characterised by a third party connecting to the customer's bank to verify identity and authorise payment. However, our research was designed first to identify generic anti-fraud measures that could be applied in any APP scenario (experiment 1) and then to optimise specific open banking journey touchpoints (experiment 2).

These user journeys are focused on the two key screens required to initiate a standard push payment: new payee account details and payment details (amount, reference). Around these two pillars the mechanisms of CoP and CRM are arranged in the standard patterns found in the market. These patterns effectively represent the scope of the interactivity provided by the underlying schemes.

The graphic execution of the anti-fraud measures are indicative only, colours being used to indicate the degree of urgency of a given warning. In practice these warnings and countermeasures would be styled to fit the brand design system.

5.1 Generic Customer Journeys

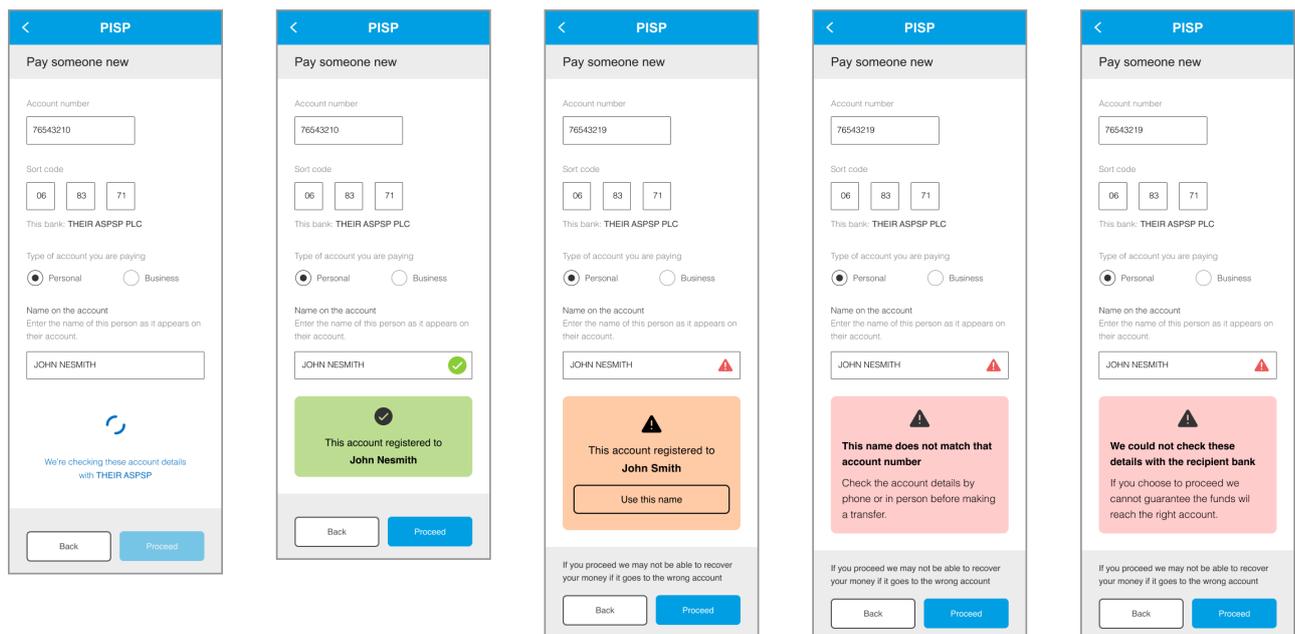
These generic customer journeys show standard deployment of CoP and CRM mechanisms, with textual responses refined to communicate with highest impact in the lowest word count.

5.1.1 COP Generic outcomes

This array all standard responses to account details entered for a new payee. Different PSPs will handle the interactive options a variety of executions. We're seeing a possible trend away from the partial match option as it might compromise personal information. Where CoP is not supported by the receiving bank, the last option is displayed – ‘we could not verify these details’.

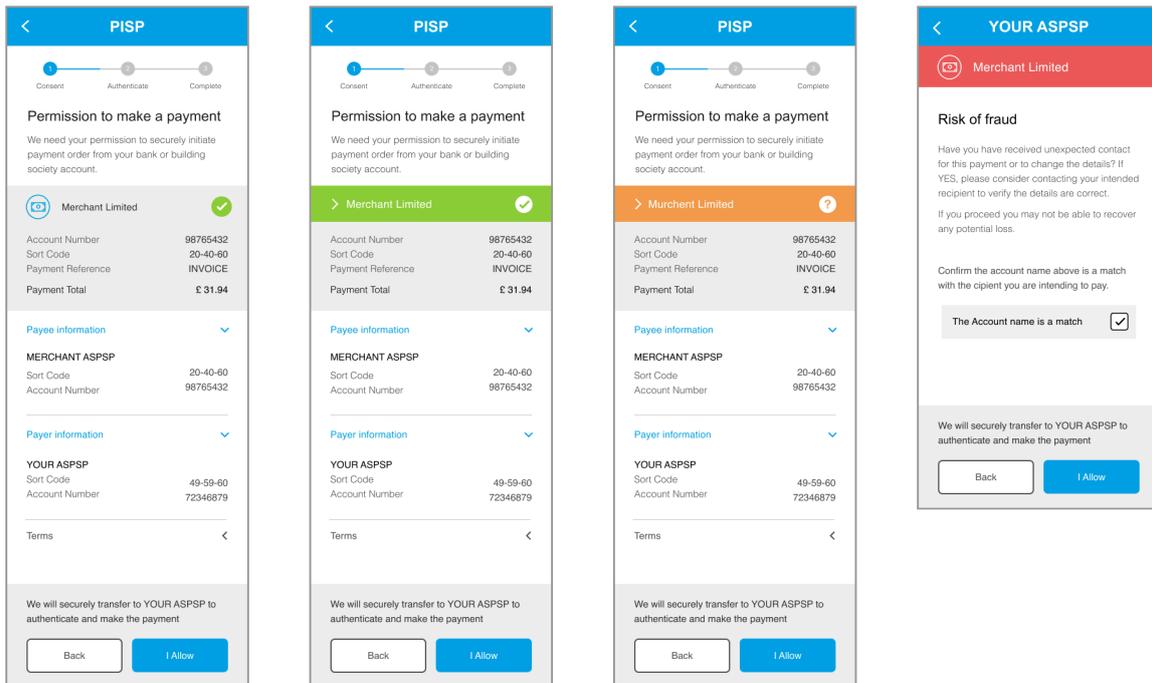
Standard display dialog

These responses are represented here in two different visual modes. The first is a standard display dialog box approach.



Progressive disclosure

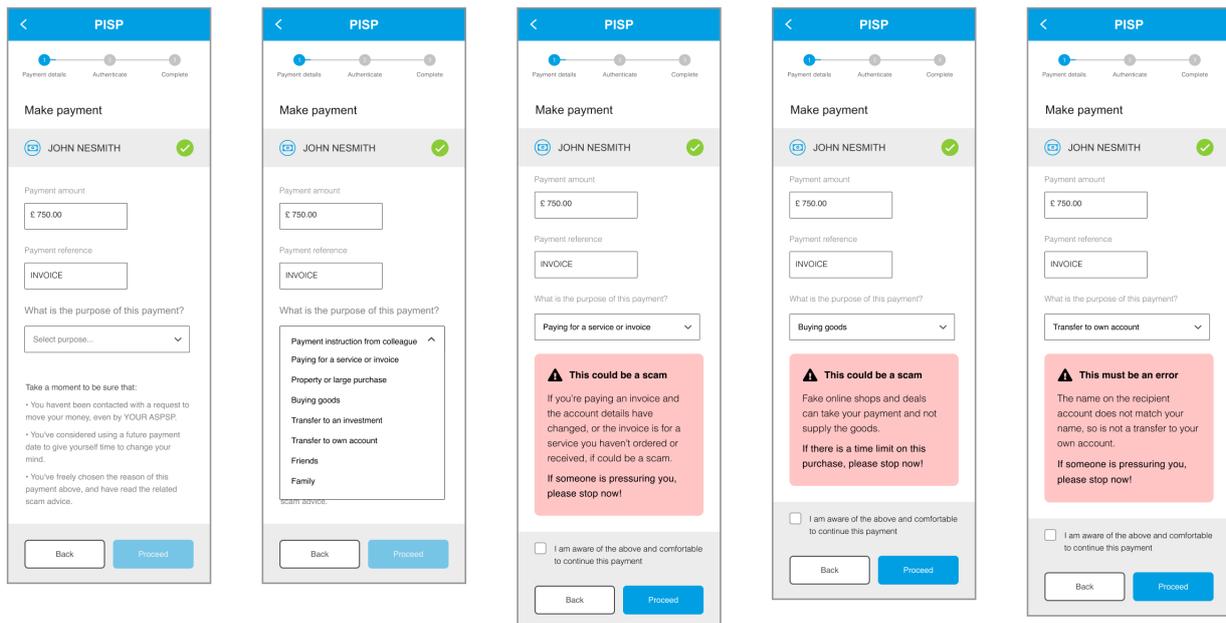
This variant favours rapid user comprehension and offers progressive disclosure – the chevron encouraging the user to drill-down to a more detailed explanation. Once the definition is understood, the icon, colour and title becomes a placeholder for the underlying concepts.



5.1.2 Generic CRM outcomes

CRM presents as a menu of ‘payment purposes’. Each menu item represents a category of scam strategies. Choosing an option is mandatory, and simply displays a tailored warning.

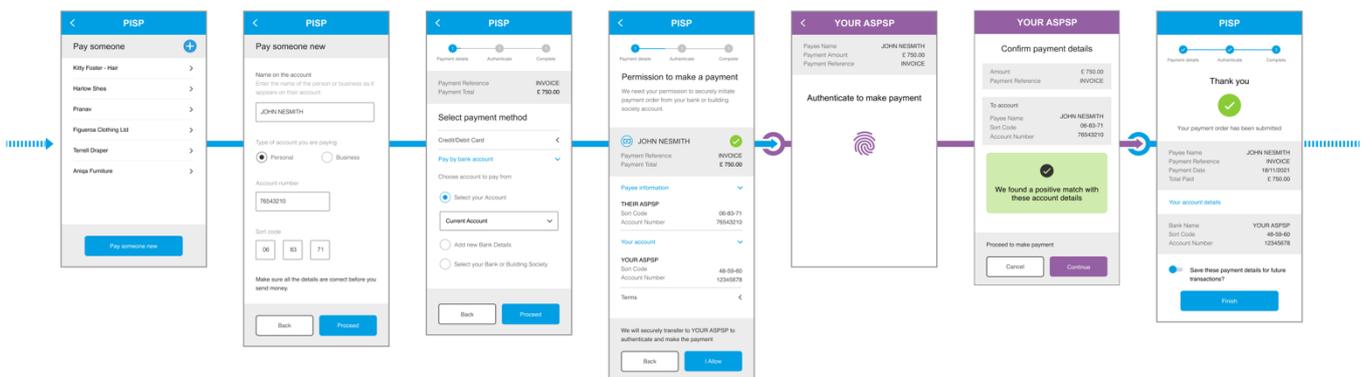
E.g. **Buying goods**: Criminals make fake adverts and shopping websites that take your payment, but do not supply the goods.



5.1.3 CoP Call by ASPSP during authentication

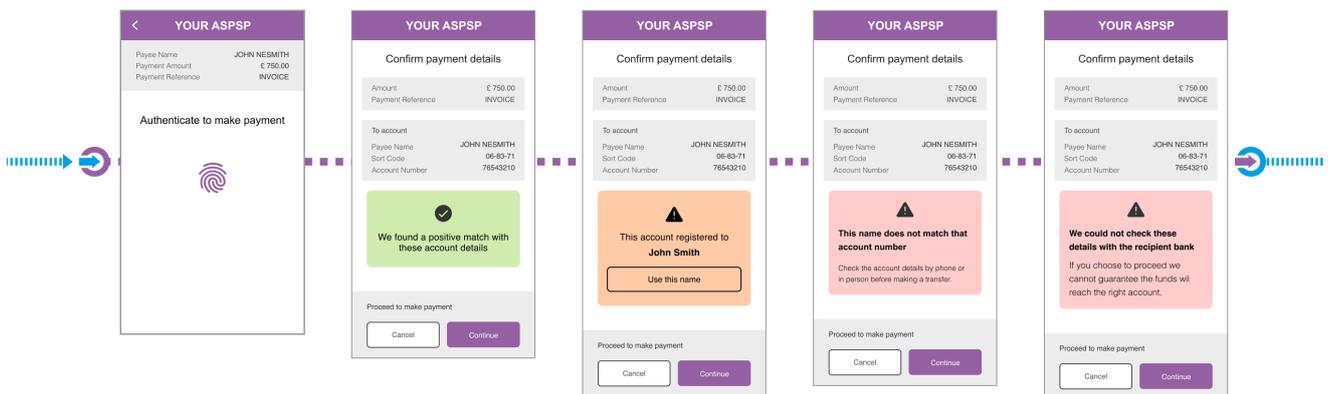
In this standard implementation the PISP is not signed up to the CoP scheme, so the user enters the payment details in the PISP app and is handed-off (redirected) to their default banking app to verify identity and authorise the payment. Here the ASPSP confirms the payee details (CoP) and displays the result locally, in their app.

This implementation suffers from the disconnection between the input controls (account name, number and sort code) and the CoP response, particularly as the user has an inconvenient journey back to the payee details to amend mis-keys etc.



CoP call by ASPSP during authentication - standard outcomes

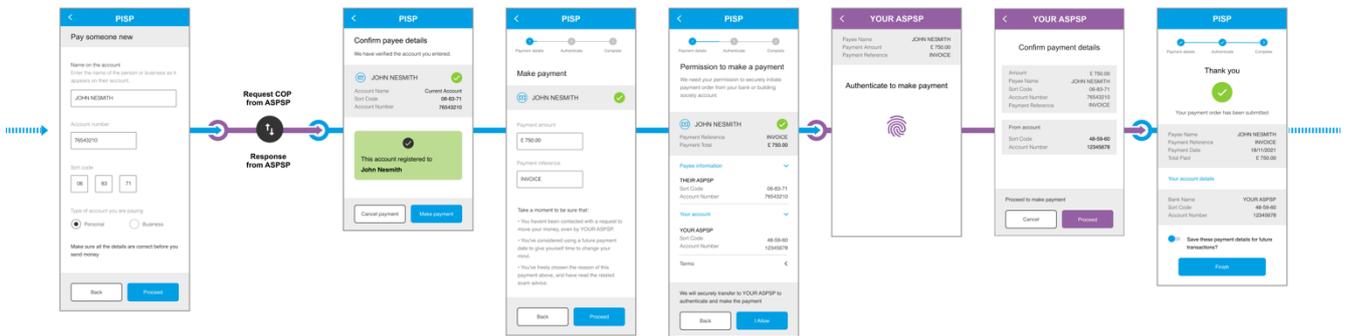
The array of typical CoP response options are displayed here. As discussed above, the partial match is less common, and where the recipient's ASPSP does not support CoP, the last option is to report 'unable to verify'.



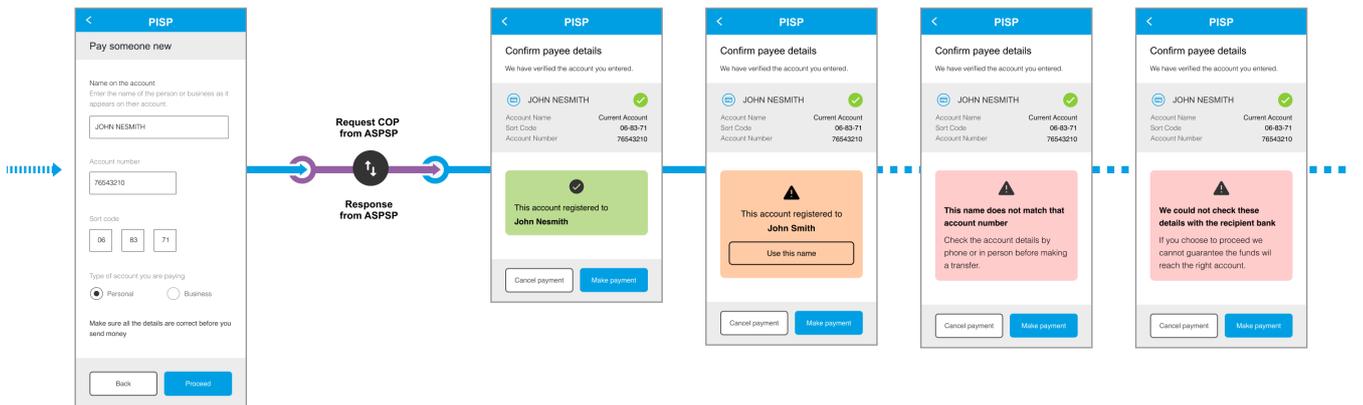
5.1.4 CoP Call by ASPSP before authentication

In early qualitative testing, users demonstrated higher comprehension of the CoP message when it was displayed adjacent to the input controls. From a user experience perspective this is a more sophisticated implementation, where the PISP is able to receive a CoP response from the payee's ASPSP before the user authenticates at their banking app, thus displaying the response in-app.

This journey presents the CoP response on an interstitial page, equally this could appear inline / in-page.

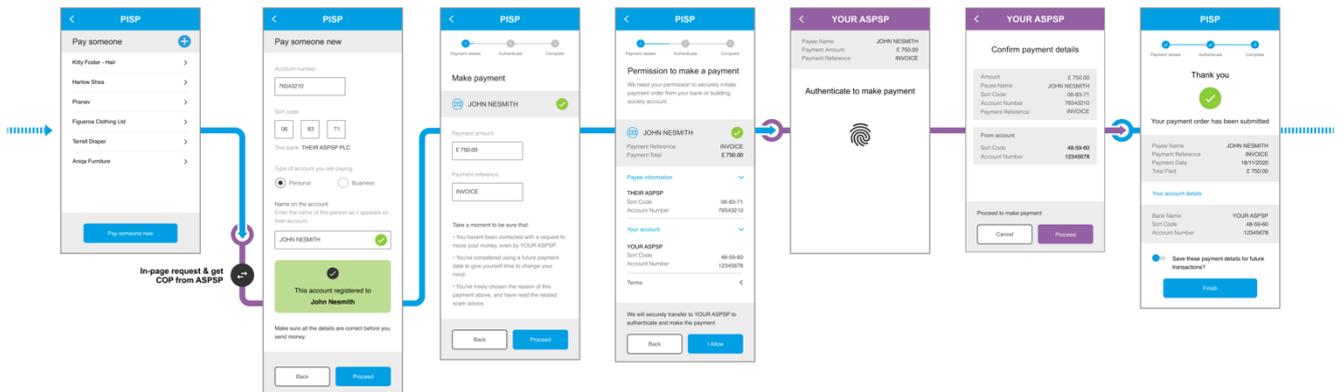


CoP call by ASPSP before authentication - standard outcomes

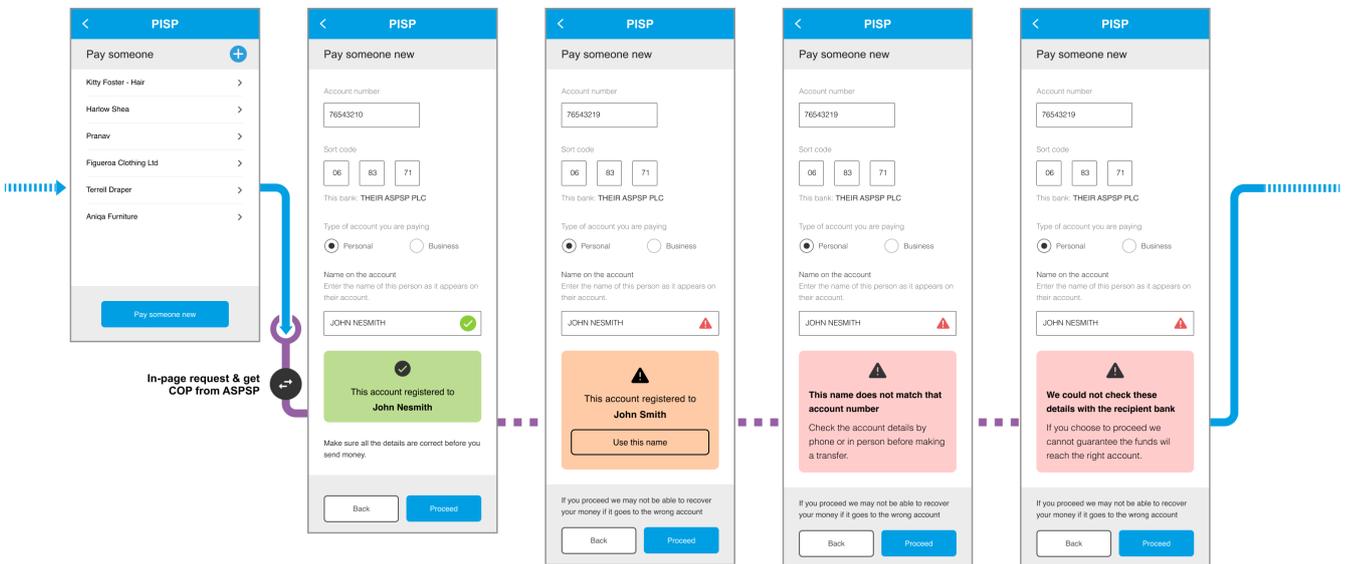


5.1.5 CoP call by PISP

This journey show a CoP response requested by PISP app and displayed inline with the new payee input controls. Here the CoP call is triggered when the user completes account detail input and displays below. This is the ideal arrangement since the user gets immediate feedback and can easily amend the details - often the account name needs adjustment to the form it is recorded: first name / surname, initials, title.

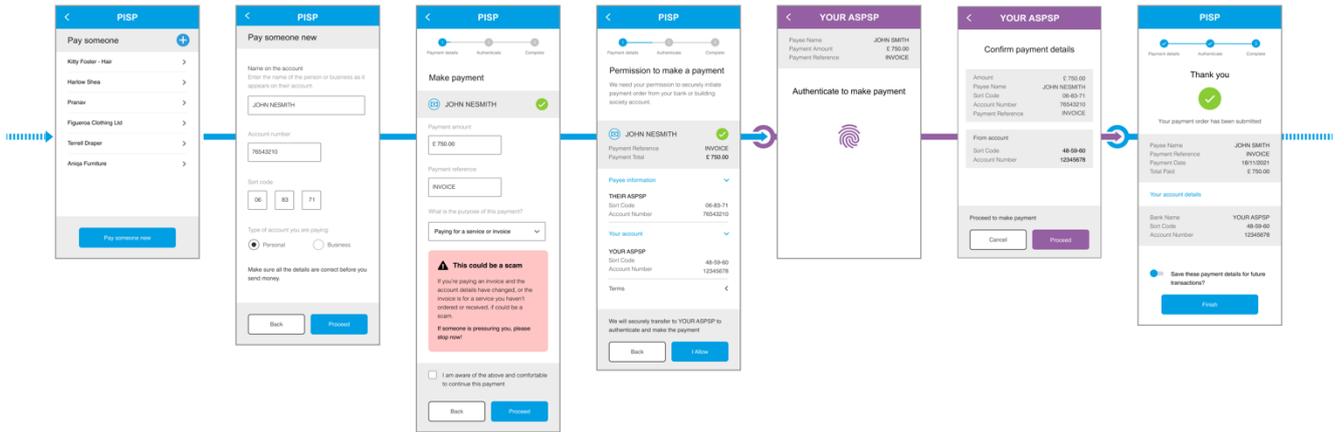


CoP call by PISP - standard outcomes

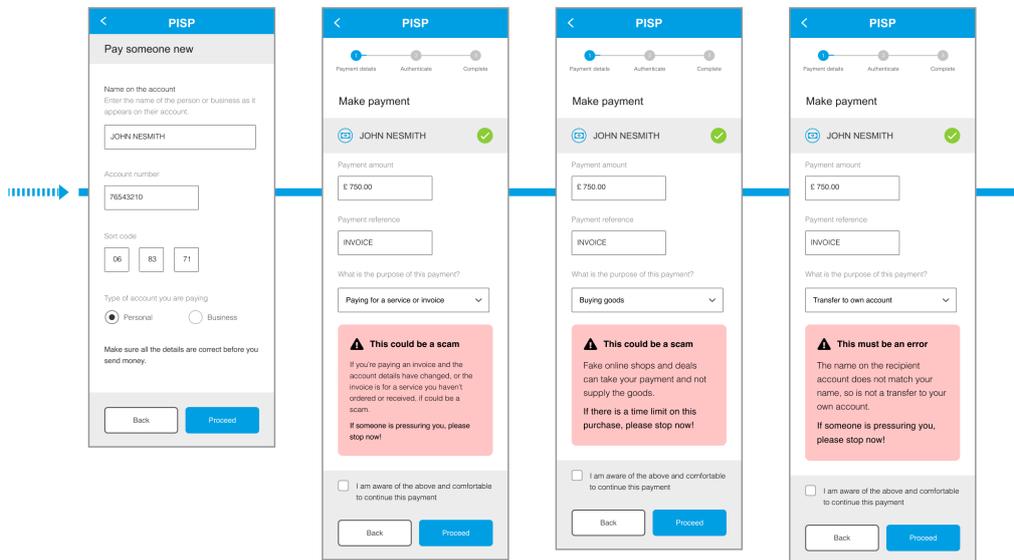


5.1.6 CRM warning by PISP

As with the CoP lessons above regarding the positioning of response inline with input control, this journey shows the CRM response below the ‘payment purpose’ menu. This is the most common pattern in the field and makes sense technically since CRM requires no external call (like CoP).



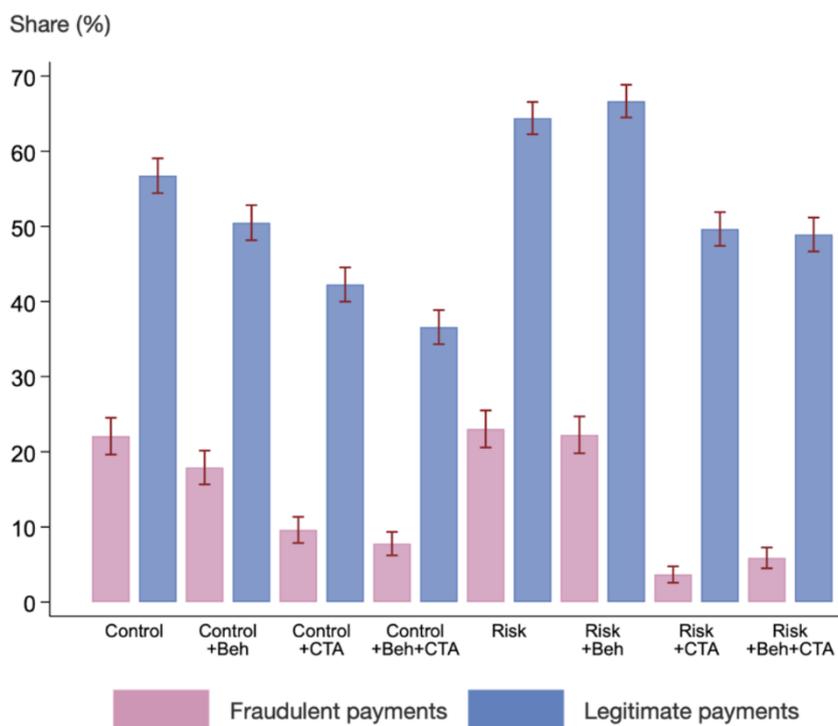
CRM warning by PISP - standard outcomes



5.2 Recommended Customer journeys

Analysing the outcome of our big APP fraud study, we began by examining the share of participants that made fraudulent and legitimate payments in each experimental group. As it shows below, around 22% of participants made a fraudulent payment in the control group (existing measures in market). Those in the control group on average completed 57% of the legitimate payments. With two legitimate payments presented to each participant, this means on average they completed 1.14 of these payments.

Treatment effects on payment behaviour



Five of the seven treatments had a statistically significant effect on the share that made a fraudulent payment compared to the control group. The 'Risk-based + CTA' group had the largest effect - an 18% decrease relative to the control group. This means only 4% of participants in this group fell for the fraud. We conclude that the 'CTA' element has the biggest impact, regardless of whether it is deployed by a risk-based mechanism or in an app with behavioural messaging. [See below for definitions].

While the CTA interventions generated large reductions in the share that fell for fraud, they also reduced the conversion of non-fraudulent payments. The addition of 'behavioural' text reduced the share of fraud by 4% over the control group but had little effect in the risk-based group. The 'risk-based' approach on its own had no significant effect on fraud. However, both 'risk-based' and 'risk-based + behavioural' increased the legitimate payments that participants completed by up to 10%.

The inability of the risk-based approach to reduce fraud on its own may suggest that individuals do not need more words warning them about the prevalence of, or risks associated with, fraud. While the risk-based approach might not be suitable on its own, it mitigates the potential downside of alternative CTA's. It does so without negatively affecting the extent to which the CTA intervention combats fraud.

Thus, brands face a trade-off when deciding which variants to pursue. The strategies that avoid unintended consequences are the 'risk-based' and 'risk-based + behavioural' groups, as they reduce the friction for legitimate payments. However, these groups do not have a significant effect on fraud.

Finally, we found that 72% of users said they preferred the 'risk + behavioural + CTA' journey to their existing bank app (although 68% said the same about the control group). The 'risk + behavioural + CTA' version also scored best on other customer satisfaction and usability metrics such as in the percentage that said that the app felt intuitive (4% higher than in the control group), and the share that said it felt safe (5% higher than the control group), and scored second highest on the share that said it was easy to cancel payments (8% higher than in the control group). We also find that across all groups participants were more likely than in the control group to state that they read the text and warnings presented in the app.

5.2.1 Risk specific responses

Current payment journeys tend to present an overwhelming amount of detail about online fraud which compromises its effectiveness (*Cross and Kelly, 2016*).

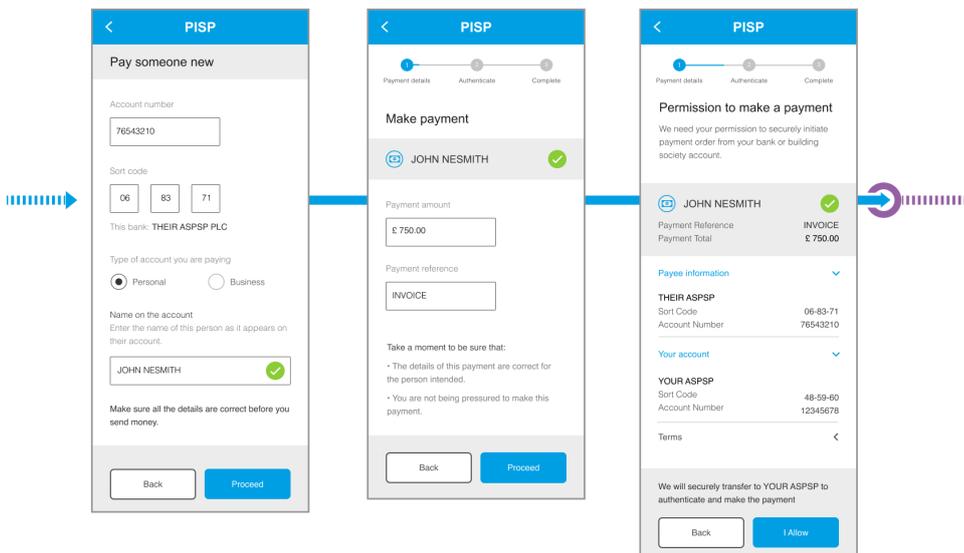
The concept here is to assess the level of risk in a transaction and present a proportionate response. The risk assessment is conducted through background AI pattern analysis, and through direct question and answer in the payment journey. This strategy has the dual advantages of ramping up the urgency of warnings when the evidence of fraud looks strong and reducing the friction for the many low risk transactions.

Step 1 Customer enters payee details and payment amount. These responses determine the first tier of risk assessment. Low value payments, trusted recipients, positive CoP checks flag the payment as low-risk and the user journey unfolds in a low-friction configuration with minimal anti-fraud interventions.

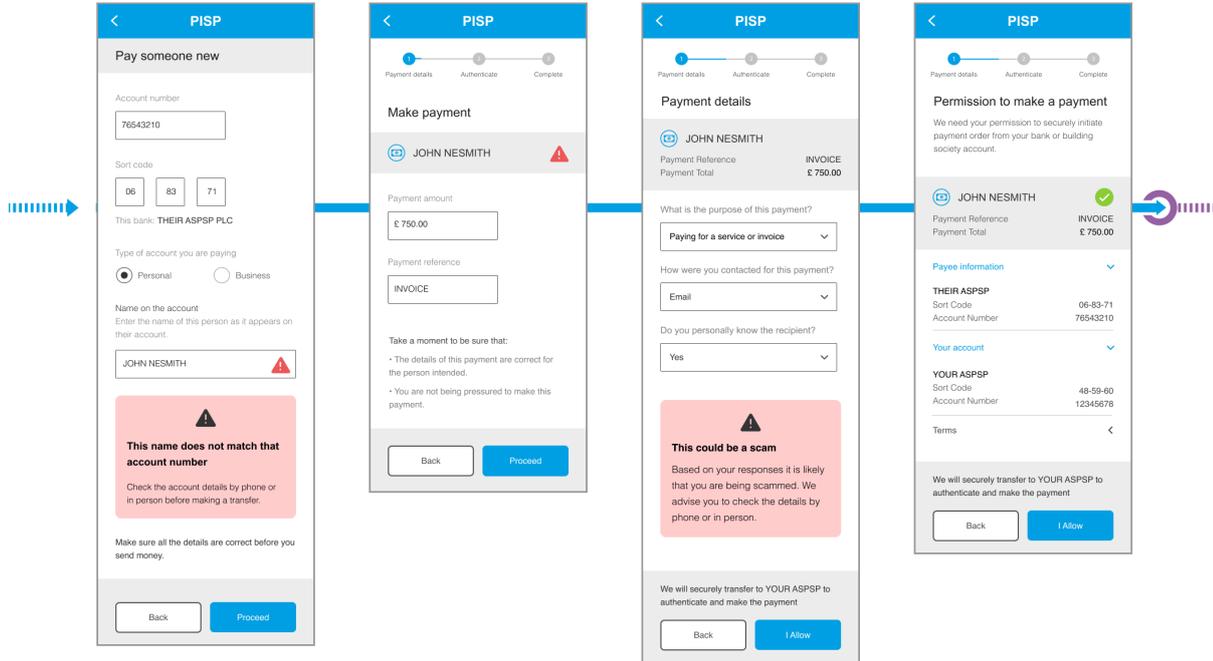
Step 2 If the payment is flagged as medium to high-risk, the customer is presented with a few more questions, page elements that the low risk payment hides.

Step 3 Based on the user responses, a new risk assessment provides salient advice to the customer e.g., “We advise you to cancel this transaction” or “We advise you to speak to the recipient before going ahead with this transaction”.

Low-risk payment anti-fraud measures omitted



High-risk payment anti-fraud measures



5.2.2 Alternative Calls to Action

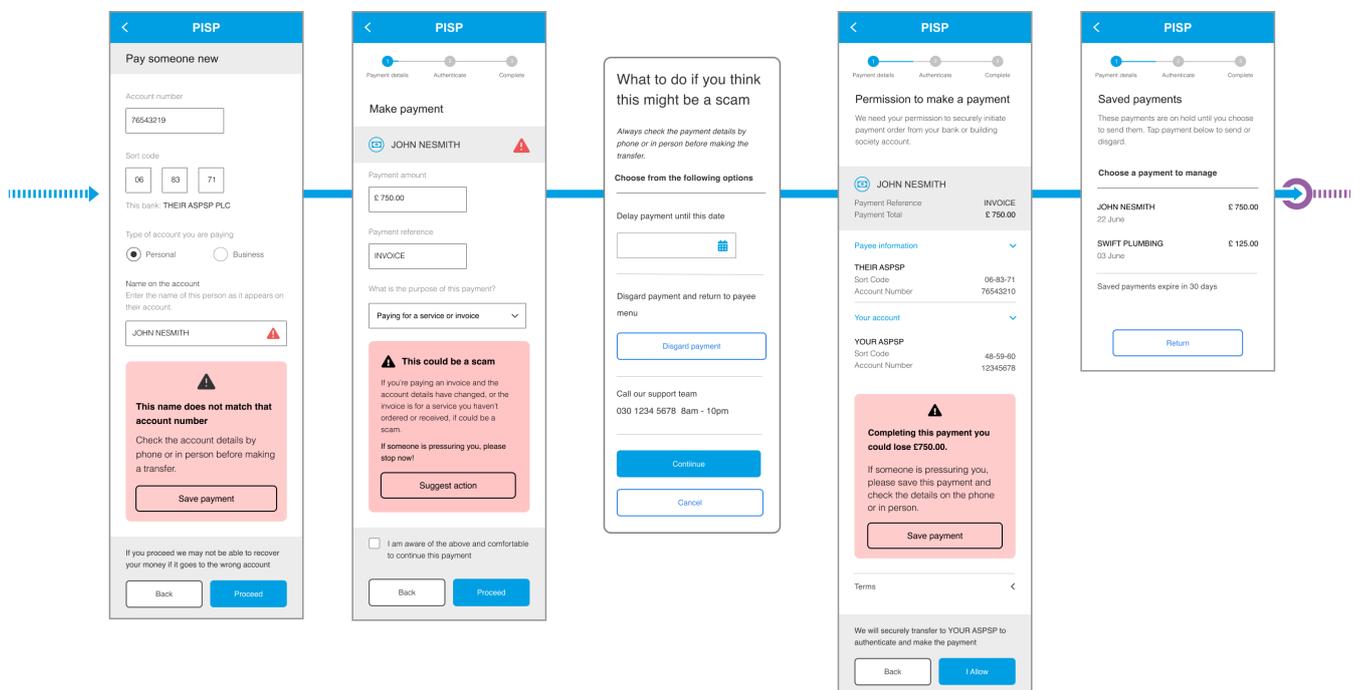
Research suggests it is effective to recommend customers call their bank if they receive a suspicious payment request (*Jansen and R. Leukfeldt, 2015*).

Scheduling payments for the future gives customers time to reflect on the payment before they execute (*Jansen and Leukfeldt, 2015*).

This approach presents the customer with alternative CTAs rather than more copy to read. When customers feel a payment is suspicious their uncertainty is compounded by the absence of explicit options other than complete payment or quit out of the browser tab. Alternative actions can be presented at each stage of the journey, and relevant to the level of risk and recommended user response.

Alternative calls to action include:

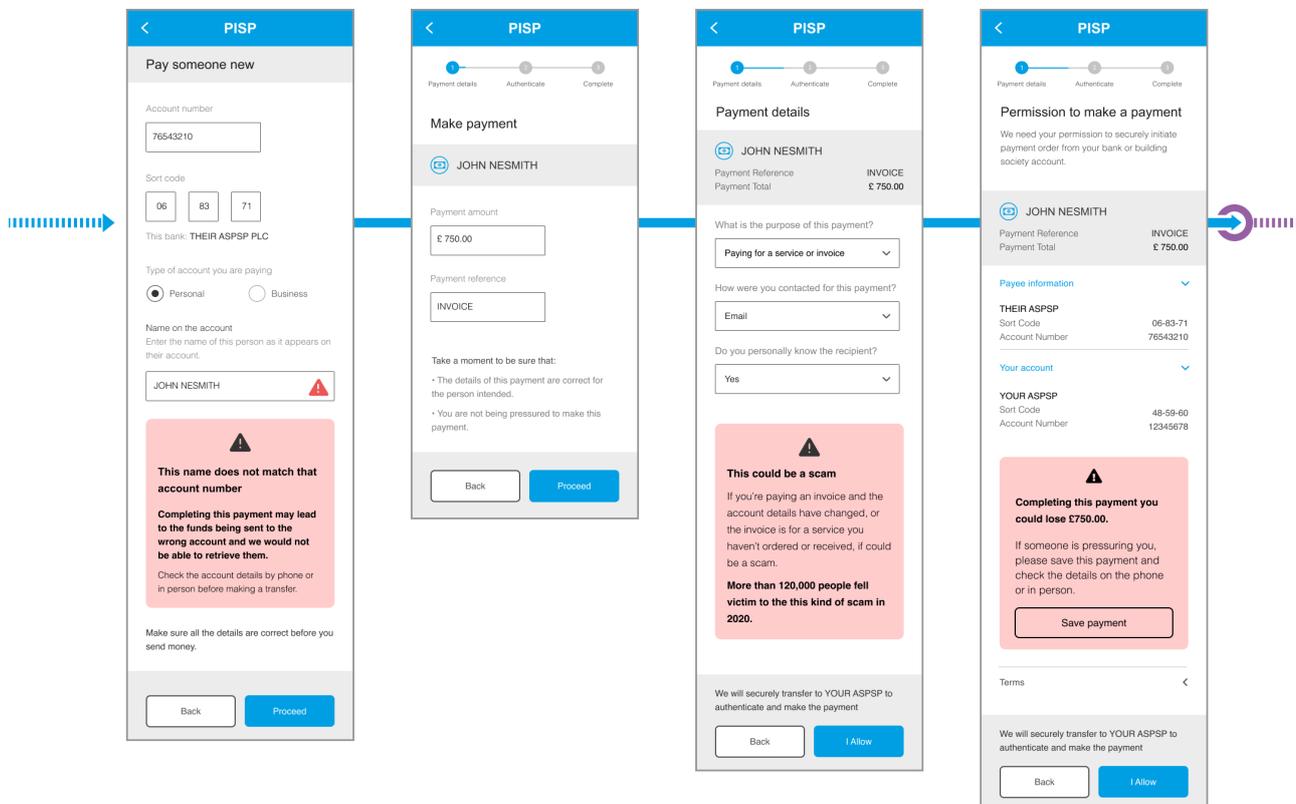
- Contact us,
- Save payment for a later date,
- Change payee details,
- Discard payment.



5.2.3 Behavioural warnings

People are more likely to stop accessing suspicious web pages when warnings describe personal risks (Kauer et al. 2012; Cross and Kelly, 2016).

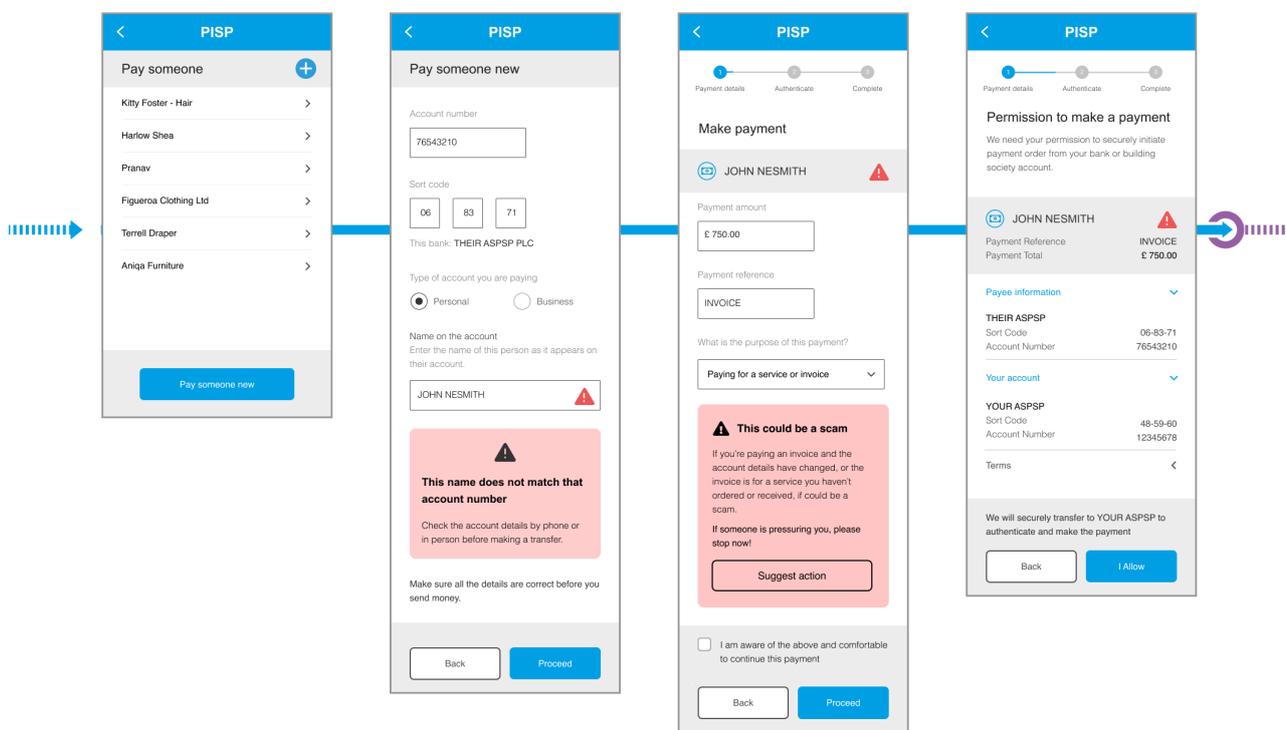
In a fraudulent payment scenario customers often fail to grasp the risk they face and assume existing warnings do not apply to them. Studies have shown that fear-based appeals are more effective in changing customers' online security behaviours. Triggering 'loss aversion' makes customers more careful, as the pain of loss is found to have more impact than messages couched in more positive terms like 'safety' or 'security'. Based on participant responses, we explain why the payment has been flagged as risky and emphasise the money they could lose.



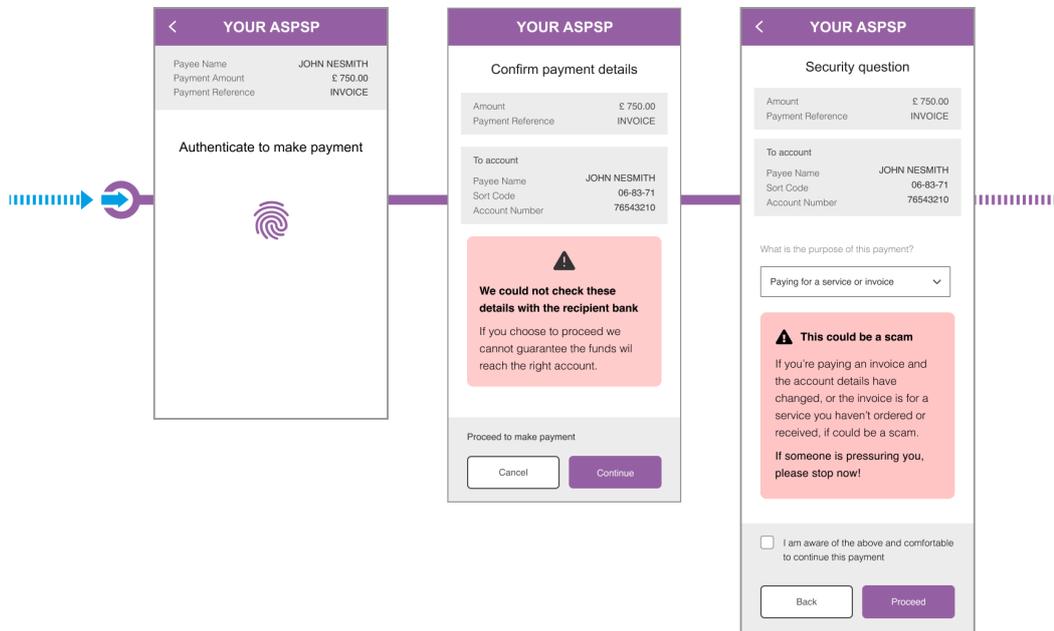
5.2.4 COP + CRM together / PISP vs ASPSP

Experiment 2 of the research explored the relative positioning of CoP and CRM mechanisms, the effect of presenting them in the PISP app or the ASPSP app, or both. The main finding was that user comprehension suffered if 1/ CoP and CRM were split across PISP and ASPSP, or 2/ the response was separated from the input controls (fields, menus). Therefore, the ideal is that both CoP and CRM are presented together, whether in the PISP or banking app.

CoP / CRM combined in PISP app

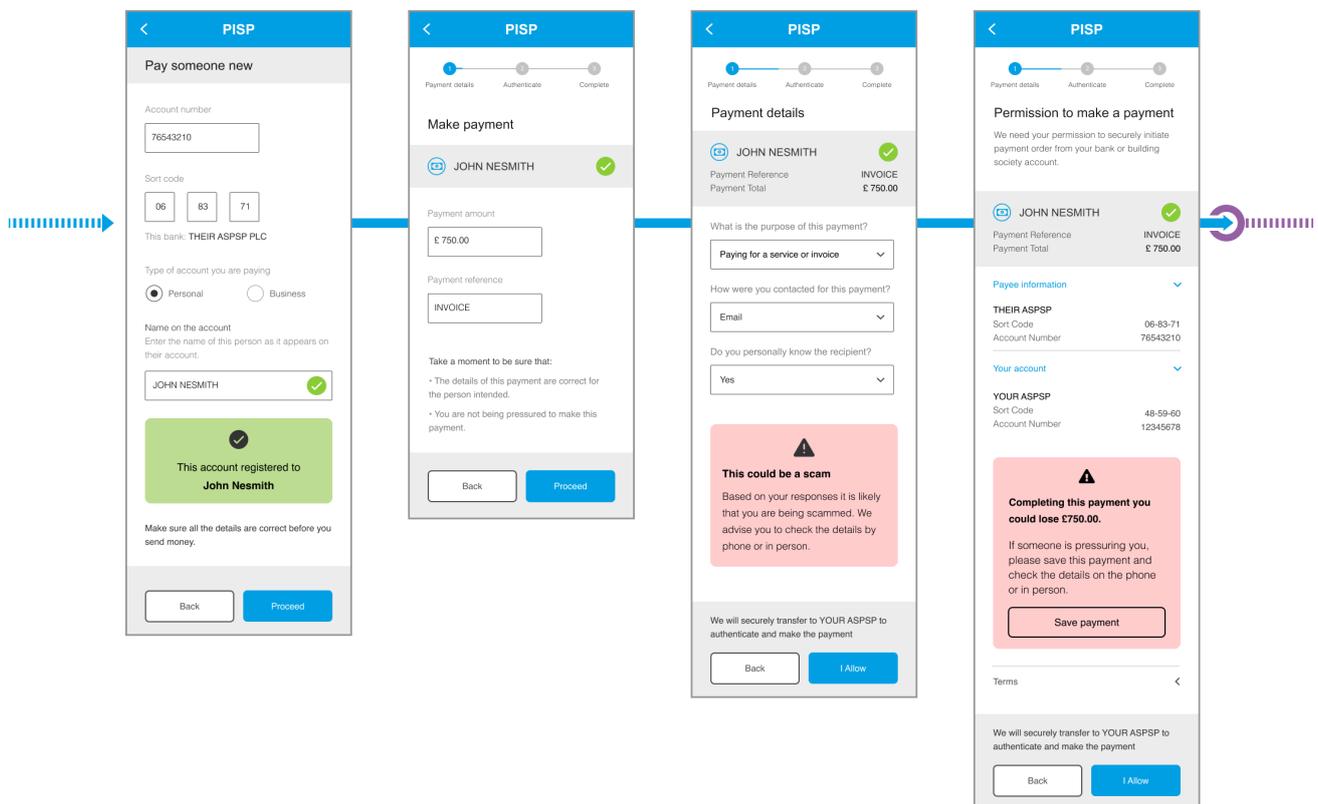


CoP / CRM combined in ASPSP app



5.2.5 Risk + CTA + Behavioural

The risk-based approach reduces the presentation of anti-fraud measures for payments assessed as low risk (low value, trusted recipient, purpose and supplementary questions). This is found to have less impact on fraud but reduces friction for the benign majority of payments. In the research the most effective counter-fraud group combined a risk-based approach with alternative CTA's (e.g. save payment) and behavioural messaging.



5.3 Product Requirements for Standards

These are stated as requirements of the OBIE solution to provide a standard for CoP and CRM. Requirements marked as 'M'(Must) are in the scope of the OBIE solution. All other requirements are listed for future consideration. Each requirement below is 'optional' for implementation by ASPSPs and/or TPPs. These terms are defined in the document “Categorisation of requirements for standards and implementation”

The product requirements below would address the technical aspects of the three Trustee Actions referenced above. Additionally, an assessment of the technical changes that would be required to address these requirements (and by extension the Trustee Actions) has been completed and is documented in Section 6 below). These changes can be incorporated into the OBIE Read-Write standards following the normal governance processes at a point in time when there is an industry demand for these capabilities.

The following requirements only apply to:

- Domestic payments
- Future dated domestic payments
- Standing Orders

| ID | Description | MoSCoW | Rationale | Implementation by ASPSP |
|----|--|--------|-----------|-------------------------|
| 1 | The OBIE Solution(s) must enable the PISP to provide a sub-category* associated with each payment as part of payment consent request to the ASPSP. *sub-category – BillPayment, EcommerceGoods, EcommerceServices, Other PartyToParty | M | Customer | Optional |
| 2 | The OBIE Solution(s) must enable the PISP to carry out a CoP check and then communicate the result to the ASPSP as part of the payment consent or payment submission request. | M | Customer | Optional |
| 3 | The OBIE Solution(s) must enable the PISP to request the ASPSP to perform a CoP check as part of the payment consent or payment submission request. | M | Customer | Optional |
| 4 | The OBIE Solution(s) must enable the ASPSP to perform a CoP call and respond indicating the entire response of the CoP check to the PISP, as part of the payment consent response or payment submission response. | M | Customer | Optional |

| ID | Description | MoSCoW | Rationale | Implementation by ASPSP |
|----|---|--------|-----------|-------------------------|
| 5 | The OBIE Solution(s) must provide guidance to ASPSPs where it is recommended, to not perform CoP check and display additional CRM warnings where the sub-category of the payment is identified as Merchant Initiated or Me2M by the PISP. | M | Customer | Optional |
| 6 | The OBIE Solution(s) must enable the PISP to provide to the ASPSP an indicator to show whether or not the CRM warnings were displayed to the PSU prior to payment consent request. | M | Customer | Optional |

5.4 Assumptions

- Where PISP and ASPSP both are participant of CRM Code, a contractual agreement between the two parties may likely be required to determine responsibility of appropriate CRM warnings, CoP checks and liability.
- PISPs have a mechanism to carry out CoP check with the beneficiary bank either directly or via a third party.
- Merchant details are verified (CoP check done) by the PISP as part of their merchant onboarding process and hence a CoP check for payments made to the merchant by PSUs is not required.

5.5 Dependencies

- Implementation of CoP in PISP journeys by CMA9 is required in order to meet the objectives of the CMA Order, however it is subject to pay.uk incorporating and extending the current rules to cover PISPs as anticipated in their planned Phase 2 (Q2 2021) activity.
- Implementation of CRM in PISP journeys by PISPs is required in order to meet the objective of the CMA Order, however it is subject to LSB enabling the PISPs to enrol and participate in CRM Code.

5.6 Constraints

- None

6 Implications for API Standards

This section discusses the changes that would be required to the OBIE RW API Standards in order to line up with the COP Proposition

6.1 Payment sub-category

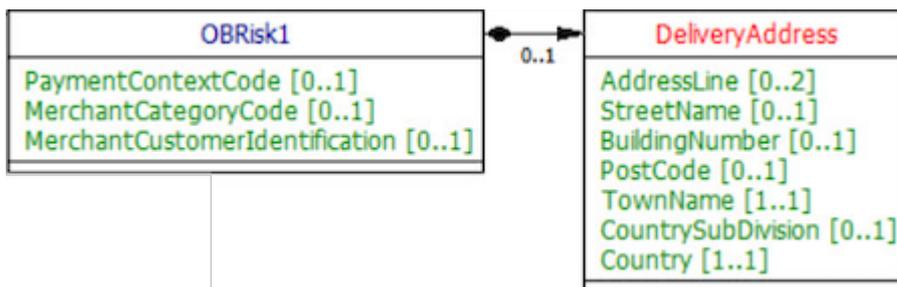
6.1.1 Proposition Statement

The OBIE Solution(s) must enable the PISP to provide a sub-category* associated with each payment as part of payment consent request to the ASPSP.

6.1.2 Required Changes

All the payment payloads currently have a Risk block. This includes a PaymentContextCode that can take on the values:

- BillPayment
- ECommerceGoods
- ECommerceServices
- Other PartyToParty



Recommendation 1

The Risk.PaymentContextCode field should be used to indicate the sub-category of the payment to the ASPSP.

If the current enumeration is insufficient, new enumerated values should be added to the enumeration

6.2 COP Check by PISP

6.2.1 Proposition Statement

The OBIE Solution(s) must enable the PISP to carry out a CoP check and then communicate the result to the ASPSP as part of the payment consent or payment submission request.

6.2.2 Required Changes

The payment - consent and payment request bodies should be modified to cater to this requirement.

In order to provide complete context of the COP confirmation, the PISP should be able to transmit:

- Body of the COP request that was made
- COP response that was received
- Signature for the COP response that was received.

The standard should have the flexibility to accommodate various COP service providers and versions of the service without leading to continuous changes in the OBIE standards.

The following fields should be added to the Data block of the request and response objects:

| Name | Path | Definition | Type |
|----------------------------|--------------------------------|--|-----------------------------|
| COP (0..1) | Data . COP | A block for holding COP information | OBCOP1 |
| Requestor (1..1) | Data . COP . Requestor | The PSP that carried out the COP request | Enumeration: ASPSP, PISP |
| Result (0..1) | Data . COP . Result | The result of the COP check | OBCOPResult1 |
| Provider (1..1) | Data . COP . Result . Provider | The organisation providing the COP service | Namespaced Enumeration |
| Version (1..1) | Data . COP . Result . Version | The version of the COP service that was used by the PISP | Max140Text |
| Request (1..1) | Data . COP . Result . Request | A copy of the COP request that was sent to the COP provider | Object |
| Response (1..1) | Data . COP . Result . Response | A copy of the COP response that was received from the COP responder. | Object |

| | | | |
|------------------------------------|--------------------------------------|--|------|
| ResponseSignature (1..1) | Data. COP. Result. ResponseSignature | The signature received from the COP responder along with the COP response. | Text |
|------------------------------------|--------------------------------------|--|------|

Recommendation 2

Add the Data. COP block defined above to the request and response payloads for:

- domestic-payment-consents
- domestic-payments
- domestic-scheduled-payment-consents
- domestic-scheduled-payments
- domestic-standing-order-consents
- domestic-standing-orders

6.3 PISP Request to ASPSP to carry out COP check

6.3.1 Proposition Statement

The OBIE Solution(s) must enable the PISP to request the ASPSP to perform a CoP check as part of the payment consent or payment submission request.

6.3.2 Required Changes

A flag should be included in the payment and payment consent requests to request the ASPSP to carry out a COP check.

Since this is an indicator of possible risk, we suggest that the OBRisk1 object is enhanced to include an indicator.

| Name | Path | Definition | Type |
|-----------------------|------|--|---------|
| Risk (0..1) | Risk | An enhanced block for holding risk information | OBRisk2 |

| | | | |
|--|--|--|---|
| <p>COPRequestedIndicator (0..1)</p> | <p>Risk. COPRequestedIndicator</p> | <p>A flag to request to the ASPSP that the ASPSP should carry out a COP check</p> | <p>Enumeration: RequestedByPISP: The PISP has requested the ASPSP to carry out the check CompletedByPISP: The PISP has carried out the COP check Not Required: The PISP has indicated that a COP check is not required</p> |
| <p>CRMDisplayIndicator (0..1)</p> | <p>Risk. CRMDisplayIndicator</p> | <p>A flag to indicate whether the PISP displayed CRM messaging or to request the ASPSP to display it</p> | <p>Enumeration: DisplayedByPISP: Indicates that the PISP has already displayed a CRM message to the PSU Not Required: The PISP has indicated</p> |

Recommendation 3

Create a new OBRisk2 class that includes an additional indicator.

Modify the relevant payment request and response blocks to use OBRisk2 instead of OBRisk1

6.4 Transmission of COP result from ASPSP to PISP

6.4.1 Proposition Statement

The OBIE Solution(s) must enable the ASPSP to perform a CoP call and respond indicating the entire response of the CoP check to the PISP, as part of the payment consent response or payment submission response.

6.4.2 Required Changes

No further changes are required. The 0BC0P1 block specified above can be used to transmit COP results in either direction.

Recommendation 4

Use the new 0BC0P1 class to transmit COP results from the ASPESP to PISP.

6.5 Guidance on COP/CRM

6.5.1 Proposition Statement

The OBIE Solution(s) must provide guidance to ASPSPs where it is recommended, to not perform CoP check and display additional CRM warnings where the sub-category of the payment is identified as Merchant Initiated or Me2M by the PISP.

6.5.2 Required Changes

No impact on technical standards.

6.6 Indication from PISP to ASPSP on display of CRM

6.6.1 Proposition Statement

The OBIE Solution(s) must enable the PISP to provide to the ASPSP an indicator to show whether or not the CRM warnings were displayed to the PSU prior to payment consent request.

6.6.2 Required Changes

No further changes are required. The 0BRisk2 block specified above can be used to transmit CRM indicators.

Recommendation 5

Use the new 0BRisk2 class to transmit CRM results from the ASPSP to PISP.

7 Appendix

i. Roadmap Reference

The following table is taken 'as-is' from the published [Roadmap](#):

| Reference | Roadmap Scope Item | Original Roadmap Item | Objective | Description & Work Activity |
|-----------|---|-----------------------|--|---|
| A2 (d) | Evolving Open Banking Standards re Confirmation of Payee and CRM Code | P19 | The Standards need to ensure that customers experience low friction journeys that are consistent with the regulatory requirements of CoP and CRM Code. | <p>OBIE Preparatory Activity: to complete by end of October 2020.</p> <ul style="list-style-type: none"> Develop the OB Standards (including CEG and OG), in conjunction with Pay.UK, the Lending Standards Board and the Payment Systems Regulator, to ensure maintenance of low-friction, no obstacle customer journeys that take account of the requirements of the Contingent Reimbursement Model (CRM) code and Confirmation of Payee (CoP). <p>Industry Consultation (to include CMA9 participation):</p> <ul style="list-style-type: none"> Industry consultation (including CMA9 Participation): for two months, to commence four months after the end of the Crisis Impact Period. <p>Final Standards:</p> <ul style="list-style-type: none"> Final Standard: to be published seven months after the end of the Crisis Impact Period. The CMA's expectation is that the CMA9 will not implement CoP into any PIS customer journeys until the OB Standards specified in this Roadmap item have been developed and published. <p>CMA9 Implementation:</p> <ul style="list-style-type: none"> Mandatory CMA9 implementation of the new OB Standard to be completed within 13 months after the end of the Crisis Impact Period. |

ⁱ CoP – Confirmation of Payee - <https://www.wearepay.uk/confirmation-of-payee/>

ⁱⁱ CRM – Contingent Reimbursement Model Code - <https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/#contingent-reimbursement-model-crm-code>