Payment Systems Regulator

APP Scams - PSR Industry Engagement Session 2

10 April 2024

Purpose and agenda

Thanks for joining today's session. We will be hosting a series of fortnightly engagement sessions to support industry readiness. These sessions give in-scope PSPs the opportunity to ask questions and seek clarity on the FPS APP scam reimbursement policy.

Over the next 1.5 hours, we'll be discussing:

01 Obligations for sending and receiving PSPs including opportunity to respond | *Francesca Morphakis and Jon Williams*| 35 minutes

02 Me-to-me payments | *Jon Williams* | 20 minutes

03 Vulnerability | *Saima Hansraj* | 15 minutes

04 Repatriation | *Ben Woodside* | 15 minutes

05 Upcoming questionnaire

Given the number of attendees and the content to cover, please:

- Mute microphones unless you are speaking
- Raise hands virtually to ask questions
- Do not feel the need to echo others' views
- If you leave a comment in the chat, we will try to get to it or we will review it after the call
- A copy of these slides will be shared after this session.

Obligations for sending and receiving PSPs – Part 2

‘Advanced reimbursement’ and ‘opportunity to respond’

- We understand receiving firms are concerned that the policy as currently drafted allows a sending PSP to assess a claim as reimbursable and to require the receiving PSP to pay 50% of the liability, without the receiving PSP having the opportunity to input into the assessment process.
- We recognise this may lead to a number of disputes where receiving PSPs refuse to pay their liability contribution.

We have heard the strength of industry feeling on the need for greater clarity on:

a) how the policy operates where a firm wishes to reimburse a consumer in advance of completing the assessment

b) whether a receiving PSP has an opportunity to proactively share information with the sending PSP during the assessment process

These slides set out the PSR’s view on both a) and b), and the possible interaction between them in a series of example scenarios.

Recap of sending and receiving PSP obligations

The sending PSP must notify the receiving PSP of the claim in a time period set by Pay.UK.

Sending PSPs must complete their assessment and reimburse the victim within 5 business days of the victim making the claim if it is a reimbursable APP scam claim (subject to 'stop the clock').

The sending PSP can 'stop the clock' to pause the 5-business day assessment timeline in specified circumstances. This is at the sending PSP's discretion. This includes gathering additional information from the receiving PSP. There are benefits to the sending PSP considering all data and intelligence available to it to support its assessment of a claim.

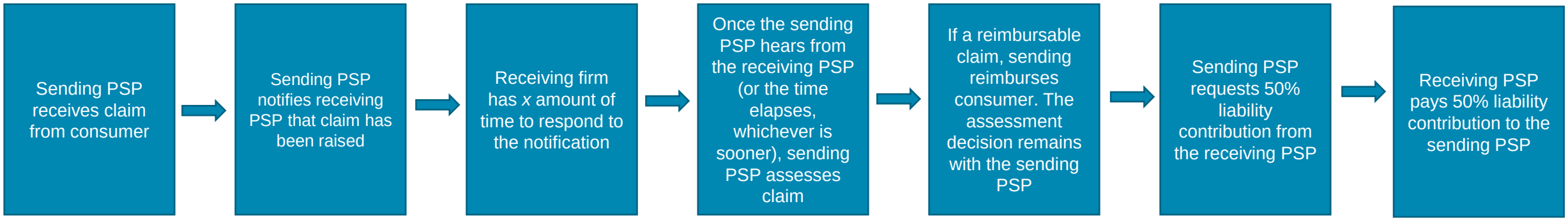
The receiving PSP must reply to information requests it receives in a timely manner. We also expect the sending PSP to give the receiving PSP an opportunity to respond.

The responsibility for deciding whether or not a claim is a reimbursable APP scam claim rests solely with the sending PSP.

The sending PSP can only request a receiving PSP to pay the reimbursement contribution if the claim is a reimbursable APP scam claim under the policy.

Opportunity for receiving PSP to respond

- PSR is engaging with Pay.UK on the potential to include in FPS rules an ‘opportunity to respond’.
- By this, we mean: a sending PSP must give any receiving PSPs *x* amount of time (to be specified by the PSO) to respond to the initial notification from the sending PSP that a claim has been raised.
- The sending PSP is not allowed to complete its assessment of the claim until either a) this period of time has elapsed or b) all receiving PSPs have responded to the notification.
- The time would start from the point when the notification was sent by the sending PSP.
- The responsibility for deciding whether or not a claim is a reimbursable APP scam claim rests solely with the sending PSP.



Advanced reimbursement and opportunity to respond illustrative scenarios

PSR OFFICIAL

Sending PSP receives claim from consumer → Sending PSP notifies receiving PSP that claim has been raised → Sending PSP reimburses consumer before 'opportunity to respond' window has elapsed → Receiving PSP responds to the notification → Sending PSP assesses the claim as reimbursable → Sending PSP requests 50% liability contribution from the receiving PSP → Receiving PSP must pay 50% liability contribution to the sending PSP

Sending PSP receives claim from consumer → Sending PSP notifies receiving PSP that claim has been raised → Sending PSP reimburses consumer before 'opportunity to respond' window has elapsed → Receiving PSP responds to the notification to state that **it does not consider the claim to be reimbursable** → Sending PSP assesses the claim as reimbursable in light of all the evidence available to it → Sending PSP requests 50% liability contribution from the receiving PSP → **Receiving PSP must pay 50% liability** contribution to the sending PSP

Sending PSP receives claim from consumer → Sending PSP notifies receiving PSP that claim has been raised → Sending PSP **reimburses consumer before** 'opportunity to respond' window has elapsed → Receiving PSP responds to the notification → Sending PSP assesses the claim as **not reimbursable** → **Sending PSP cannot request 50% liability** contribution from the receiving PSP

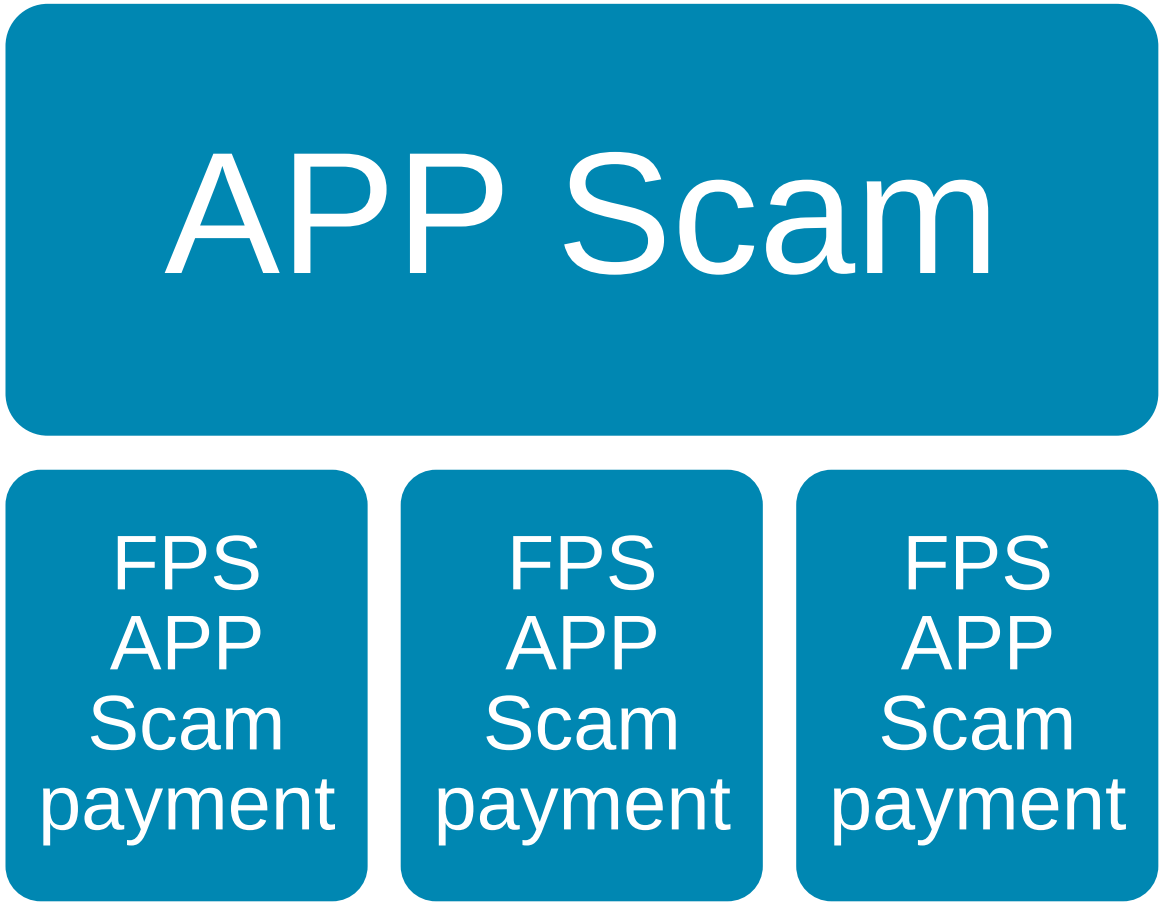
How are "Me2Me" payments treated under APP Scams Reimbursement Requirement

Me2Me – "*a payment made by a customer to another account they control*"

Relationship between the APP Scam and its payments

- **APP Scam Claims** relate to **FPS APP Scam payments** which are caused by a single **APP Scam**

- So considering whether a payment is in scope should consider if there was an APP Scam and whether the related payments meet the FPS APP Scam Payment definitions for the receiving relevant account



Key considerations – definitions

- ***APP scam (authorised push payment scam)*** *means where a person uses a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade a consumer into transferring funds from the consumer's relevant account to a relevant account not controlled by the consumer, where:*
  - *the recipient is not who the consumer intended to pay, or*
  - *the payment is not for the purpose the consumer intended*
- ***FPS APP scam payment****, for the purposes of this requirement, means an APP, authorised by a victim as part of an APP scam, that has all the following features:*
  1. *is executed through the Faster Payments Scheme.*
  2. *It is authorised by a PSP's consumer.*
  3. *It is executed by that PSP in the UK.*
  4. *The payment is received in a relevant account in the UK that is not controlled by the consumer.*
  5. *The payment is not to the recipient the consumer intended, or is not for the purpose the consumer intended*
- ***Account controlled by the consumer*** *means a relevant account that a consumer can access and make payments from. It is not sufficient for it to be in the consumer's name.*

Key considerations around whether an apparent Me2Me payment is an APP Scam

Considerations relating to the sending account

One of the key considerations during the assessment process is whether the consumer authorised the payment. Some example scenarios are:

✓ Was the payment authorised by consumer? (AUTHORISED)

x Was the payment initiated by intercepted or manipulated authentication codes or mechanisms? (UNAUTHORISED)

x Was the consumer's device taken over by remote access software? (UNAUTHORISED)

Considerations relating to the receiving account

One of the key considerations during the assessment process is whether the receiving account was in the consumer's **control**. Some example scenarios are:

x consumer account – was the account in the control of the consumer?

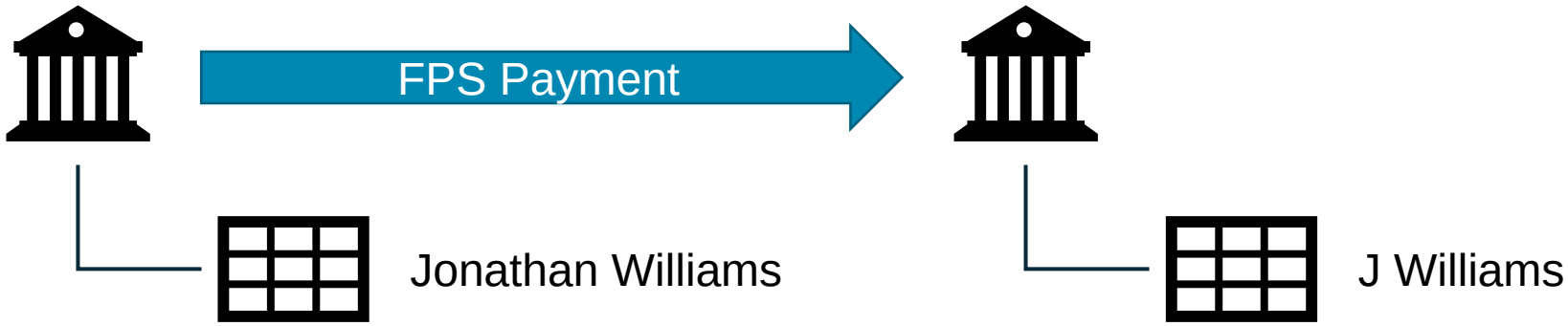
x fraudster access – was the account in control of consumer but fraudster had gained access?

✓ account takeover – was the account no longer in the consumer's control (account takeover)?

✓ fraudulent account – was the account never in the consumer's control (identity theft, manipulation, synthetic ID)?

Examples of Me2Me consideration

Example 1

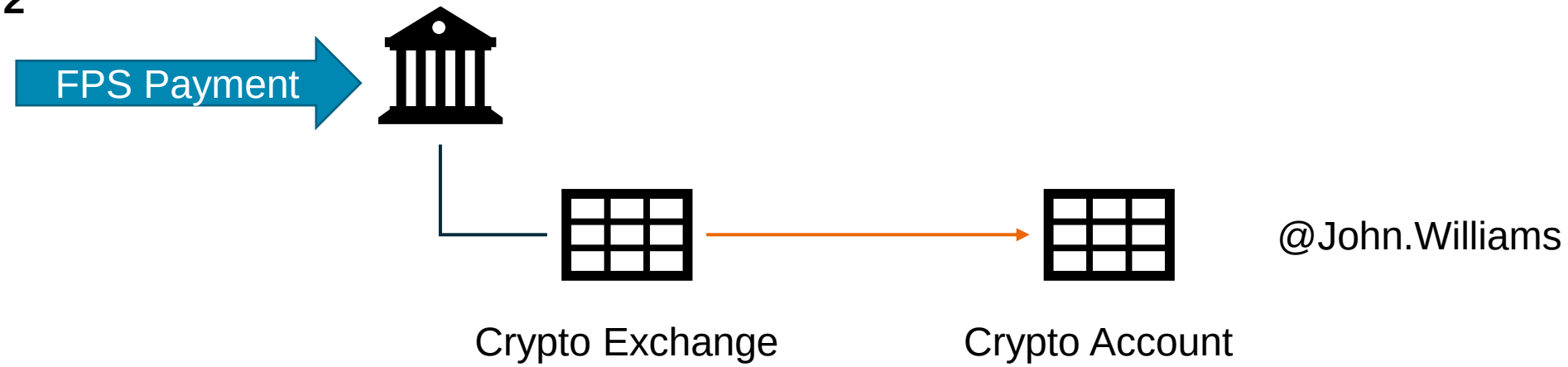


Reimbursable APP Scam payment?
Who initiated payment?
✓ Consumer
x Fraudster

Reimbursable APP Scam payment?
Is the receiving account?
x Consumer's account
x Fraudster accessed - account in customer's control
✓ Account takeover- account not in customer's control
✓ Fraudulent account

Examples of Me2Me consideration

Example 2



Reimbursable APP Scam payment?

What is the intent of the consumer in making the payment?

x Fund a crypto account in consumer's name controlled by consumer

✓ Fund a crypto account in consumer's name but controlled by fraudster

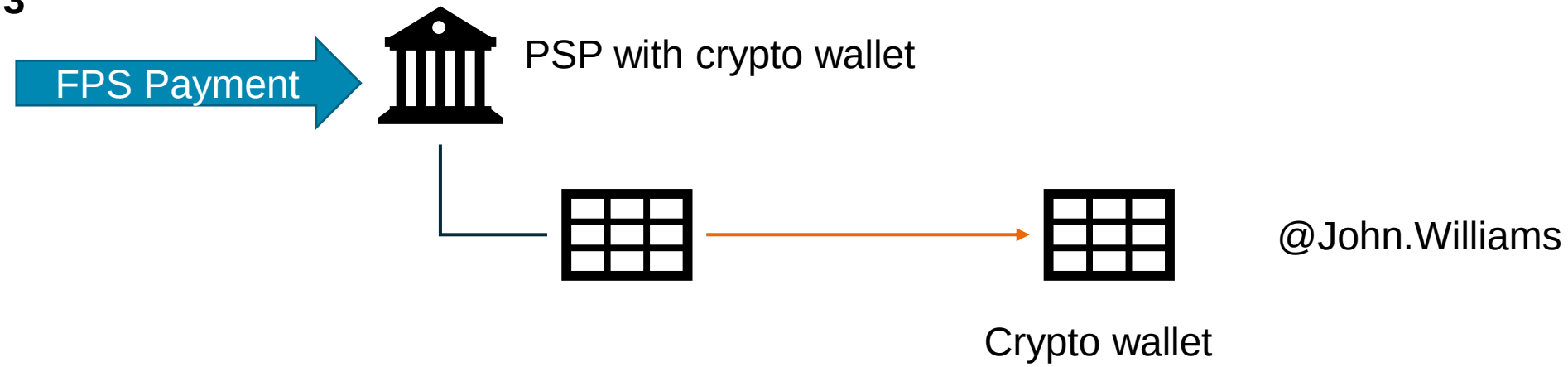
✓ Fund a fraudster's crypto account

? Fund a crypto account in consumer's name they were manipulated to open (depends on control)

? …

Examples of Me2Me consideration

Example 3



Reimbursable APP Scam payment?

What is the intent of the consumer in making the payment?

x Fund a relevant account in consumer's name controlled by consumer

✓ Fund a relevant account in consumer's name but controlled by fraudster

✓ Fund a fraudster's relevant account

? Fund a relevant account in consumer's name they were manipulated to open (depends on control)

? …

Examples of Me2Me consideration

Example 4

Reimbursable APP Scam claim?

What is the intent of the consumer in making the payment?

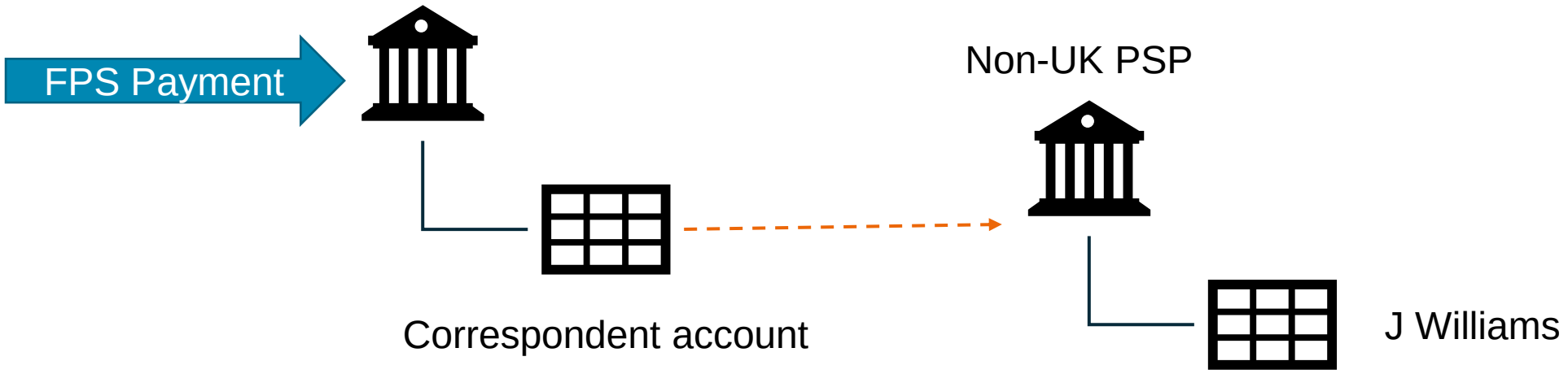
x Pay a consumer's genuine utility bill

? Pay a fraudster's utility bill e.g. romance scam

✓ Pay a utility bill that presents as the consumer's bill that is not from their utility account

Examples of Me2Me consideration

Example 5



Reimbursable APP Scam payment?

x Receiving account is outside UK, irrespective of ownership control or purpose

Vulnerability

Vulnerability

Our policy makes clear that the consumer standard of caution and the claim excess does not apply to consumers identified as vulnerable.

What do we mean by vulnerability?

We have aligned our definition of vulnerability with the FCA's so firms are working towards a single definition. *'A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.'*

***This is not a blanket exception for all customers who show characteristics of vulnerability**. For the purposes of reimbursement, Sending firms should assess the extent to which the customers vulnerability (whether temporary or enduring) led them to be defrauded. This is a subjective assessment. We expect Sending Firms to evaluate each customers circumstances on a case by a case basis.*

Assessing vulnerability

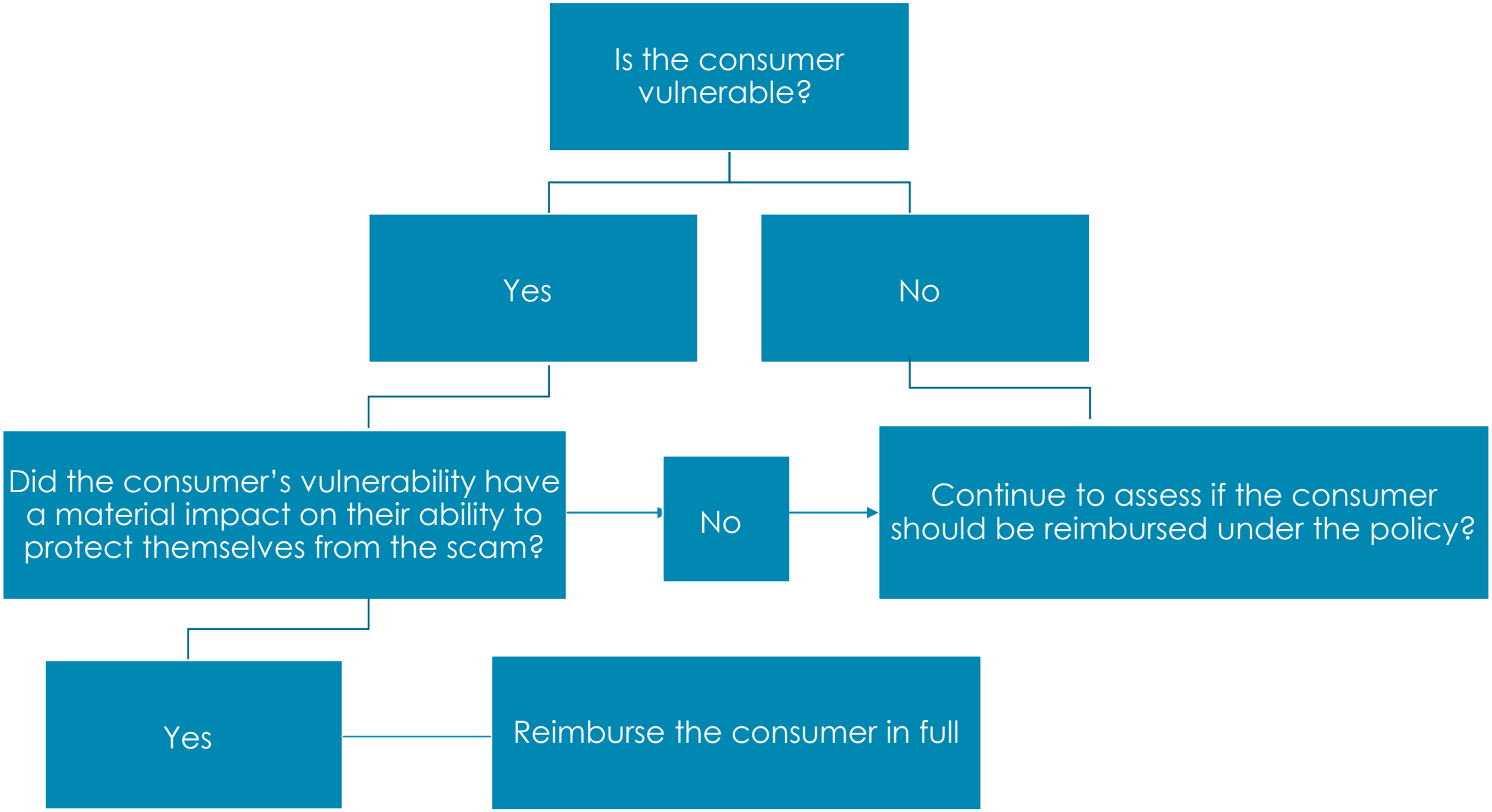
When assessing vulnerability, sending firms should consider whether the customers circumstance had **a material impact on their ability to protect themselves from the scam.** If their assessment concludes that it does, then the excess and consumer standard of caution do not apply, and the customer should be reimbursed in full. If the assessment concludes that it does not, the firm should continue to assess the claim under the reimbursement requirement.

The maximum a consumer can be refunded under the policy is £415,000. This applies irrespective of whether or not the customer is vulnerable.

The 13 month time limit to report a claim is a key parameter of the policy, it applies whether or not the customer is vulnerable. In practice this means that the vulnerability exemption cannot be used by a consumer to bring a claim outside of the 13 month timeline. This is separate to the prompt reporting requirement, set out in the consumer standard of caution. If a consumer is considered vulnerable, and the vulnerability has a material impact on their ability to protect themselves from the scam, the consumer standard of caution does not apply.

In our December policy statement we made clear that Sending firms should consider the financial impact of levying an excess on consumers with low financial resilience, and exempt consumers from the excess where there is evidence that this will lead to financial stress.

Considering vulnerability



Repatriation

APP scams reimbursement requirement and repatriation

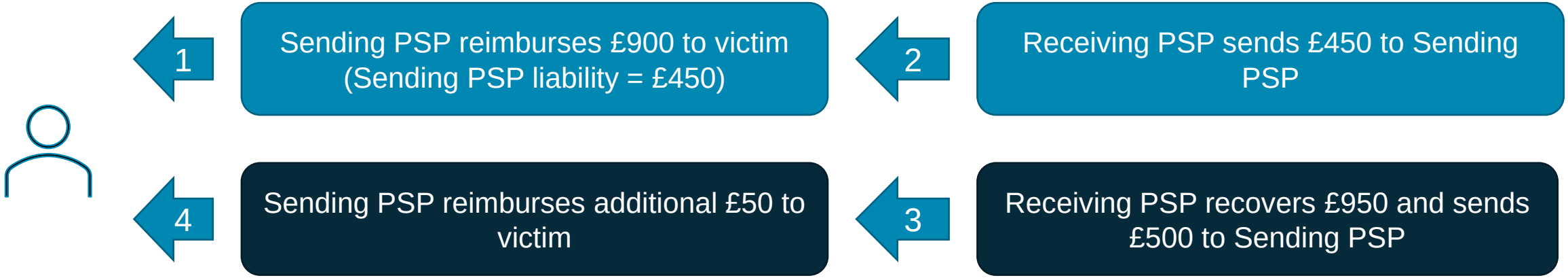
Repatriated funds – General principles

- Reimbursing the consumer is **not conditional** on the sending PSP receiving recovered funds.
- Consumer is always credited **funds by their own PSP**.
- **If 100% of funds are recovered**, the victim should be reimbursed any excess they have been charged by the sending PSP (victim should not be reimbursed more than 100% of their loss).
- **If only a portion of the funds are recovered**, the sending PSP and receiving PSP divide the funds between them (in the proportion they contributed to the reimbursement) and then pay any funds remaining back to the consumer. This is to encourage receiving PSPs to recover funds and incentivise repatriation.
- Receiving PSP would only be able to keep the maximum of its reimbursable contribution amount.
- We are **working with Pay.UK** to explore the best way of providing clarity to industry where there are complex repatriation scenarios (e.g. setting out the calculation into FPS rules).

Examples with one sending and one receiving PSP

Scenario A - Consumer loses £1,000; Sending PSP applies £100 excess; Receiving PSP recovers full amount

Scenario B - Consumer loses £1000; Sending PSP applies £100 excess; Receiving PSP recovers £950

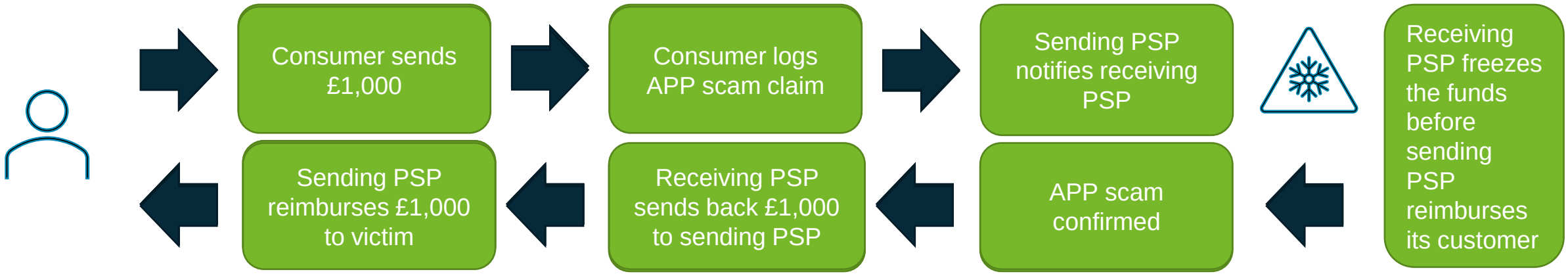


Examples with one sending and one receiving PSP

Scenario C - Consumer loses £1,000; Sending PSP applies £100 excess; Receiving PSP recovers £500

Repatriation before reimbursement

If the receiving PSP freezes all the funds and repatriates them before the sending firm reimburses its customer, the victim gets the full amount back (and no excess is levied).



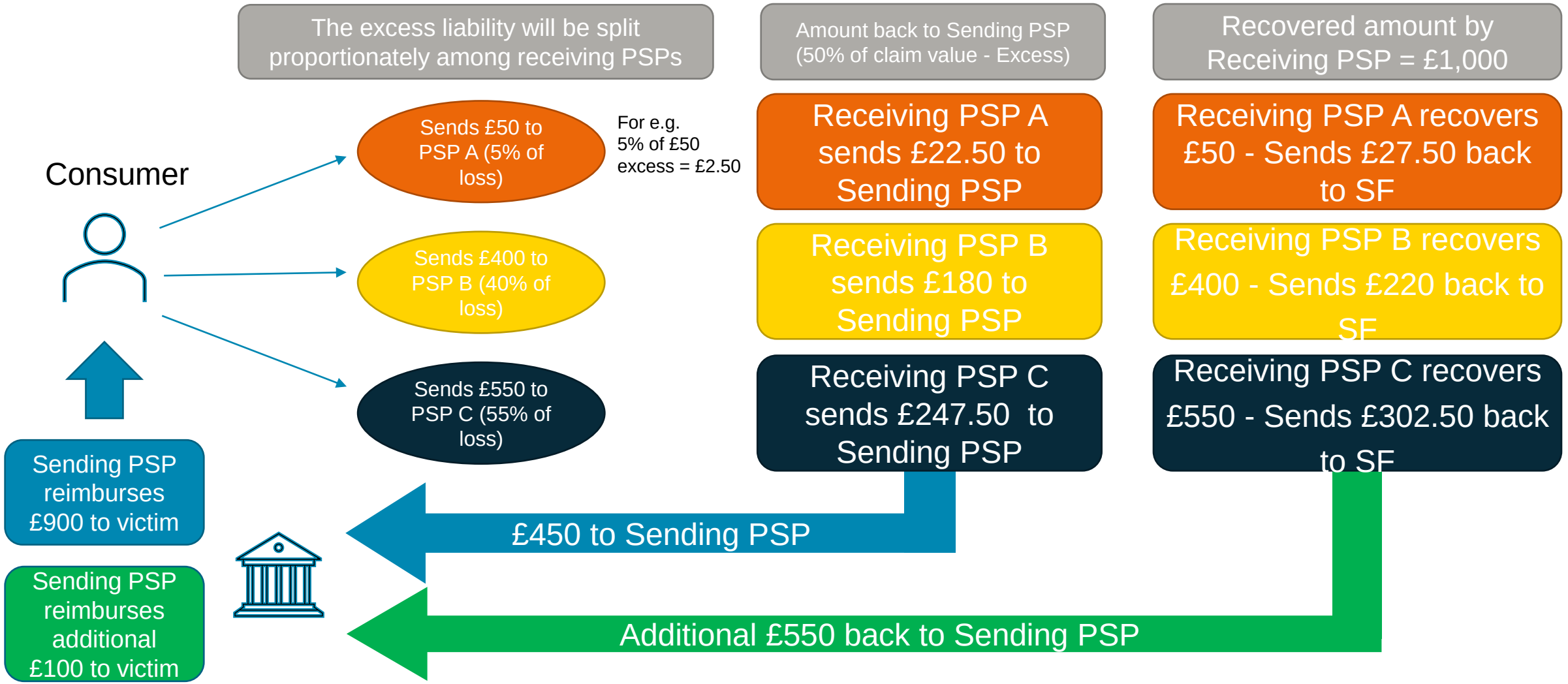
Repatriation and multi-receiving PSPs

Principle: the same principle as when there is a single receiving PSP apply.

- To confirm, we expect a **sending PSP to treat each receiving PSP separately in each repatriation journey** – SF should treat repatriation from each separate receiving PSP as a separate and independent activity.
- The victim would not receive any additional money back to cover the excess if the recovered amount from each receiving PSP is less than or equal to the value reimbursed to the victim.

Scenario D: One sending and multiple receiving PSPs

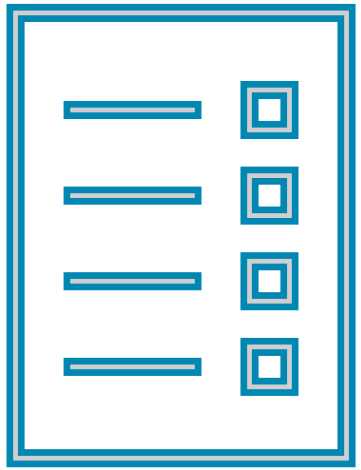
Consumer loses £1,000; Sending PSP applies £100 excess; all receiving PSPs recover full amount (£1,000)



Questionnaire

Questionnaire

We would like to hear from you – we will soon share a very brief questionnaire to understand the level of industry readiness at this stage and whether there are any critical issues in the lead up to implementation



Payment Systems Regulator

Next session will take place on 24th April 2024. Please register online on our website. Details and registration form will be uploaded soon.