PSR Payment Systems Regulator

APP Scams - PSR Industry Engagement Session 1

26 March 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 two hours, we'll be discussing:

01 An overview of the policy | *Ben Woodside* | 10 minutes

02 Scope of the policy | *Daniel Spencer / Jon Williams* | 35 minutes

03 Obligations for sending and receiving Payment Service Providers (PSPs) | *Ben Woodside* | 40 minutes

04 Treatment of excess by sending PSPs | *Paola Crosetta* | 10 minutes

05 Reporting boundary for compliance monitoring | 5 minutes

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
- A copy of these slides will be shared after this session.

Policy overview

A new reimbursement requirement for fighting Authorised Push Payment fraud

We are taking bold action against Authorised Push Payment (APP) scams. As outlined in our June 2023 policy statement PS23/3, we are introducing a new reimbursement requirement within Faster Payments to improve fraud prevention and focus firms' efforts on protecting customers. The new reimbursement sets consistent minimum standards to reimburse victims of APP fraud.

01

We want firms to take responsibility for protecting their customers at the point that a payment is made. In doing so, we expect firms to look to innovate and develop effective, data driven interventions to change customer behaviour.

02

By taking such measures to combat fraud, our aim is to boost customer confidence throughout the UK payment ecosystem

03

Central to the new reimbursement requirement working is having a central body leading the way in how we actively improve the rules of governing Faster Payments to tackle fraud.

The policy has been shaped by your feedback

The new reimbursement requirement is the result of extensive engagement with industry, consumer groups and wider stakeholders and we have refined some of the key proposals to develop a balanced final package of policies. Below is a snapshot of some of the recent steps that have been taken and a brief look into what is to come.

Q2 2023

Published our initial policy statement

Q3 2023

Publication of consultation on draft legal instruments

Publication of consultation on claim excess and maximum level of reimbursement

Industry consultation on customer standard of caution (gross negligence) guidance

Q4 2023

Publication of final policy statement

2024

Policy goes live 7th October

2024 onwards

Publication of our post implementation review within two years (likely 2026)

The reimbursement policy will go-live on 7th October 2024

Below is a high level overview of the reimbursement policy.

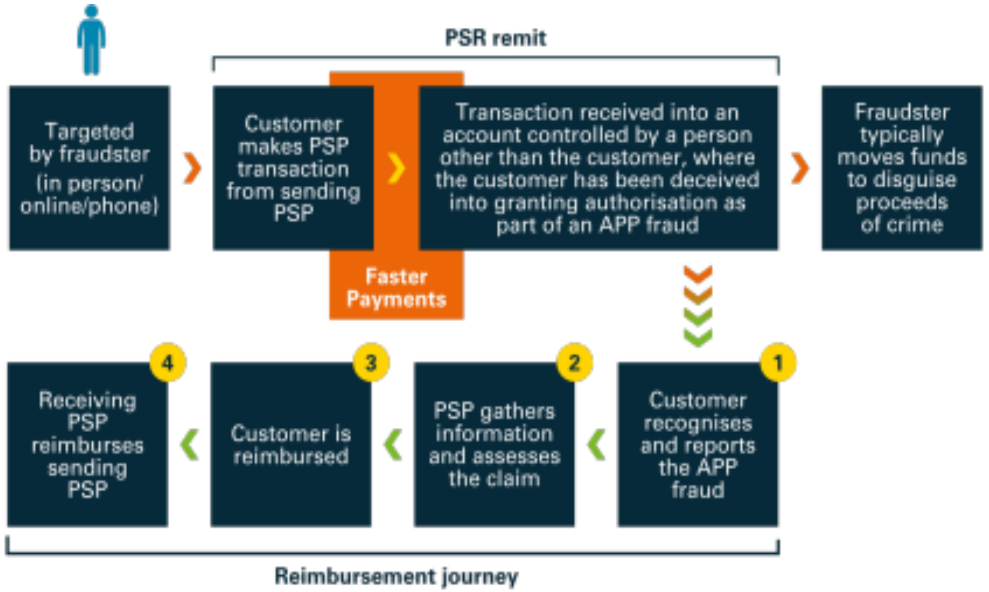
1. **Customer reports fraud** by notifying the sending PSP. The sending PSP acknowledges this and starts the process by investigating the claim and notifying the receiving PSP (the sending PSP has five business days to complete the assessment but may use the 'stop the clock' provision).

2. **PSPs should reimburse the consumer within five business days of the APP scam being reported**. But PSPs can 'stop the clock' (for a max of 35 days) to allow them to request information from the consumer, law enforcement or other relevant parties and/or receiving PSP.

3. **Sending and receiving PSPs are equally responsible** (50:50 liability split) for the cost of refunding the consumer to incentivise both sending and receiving firms to take steps to invest in fraud prevention.

4. **We've included a claim excess (£100) and a maximum level of reimbursement (£415,000)** to try and limit moral hazard and cushion the impact on PSPs. The claim excess does not apply to vulnerable customers.

5. **There are two exceptions** to reimbursement under the policy:
    1. If a consumer is grossly negligent (the Consumer Standard of Caution)
    2. First party fraud



The policy is broad and complex and we would suggest that it is reviewed in detail

Below are 10 key requirements to the APP scams policy. More information about this policy can be found at this link: https://www.psr.org.uk/our-work/app-scams/

Reimbursement requirement
Sending PSPs to reimburse victims of APP fraud

Sharing the cost of reimbursement
50:50 sending/receiving PSP

Exceptions
Gross negligence and first party fraud

Time limit to reimburse
Five business days, with the stop the clock provision

Claim excess
£100

Maximum level of reimbursement
£415,000

Time limit to claim
Thirteen months from last payment

Treatment of vulnerable customers
Gross negligence and excess will not apply to them

Payment initiation service providers
All PSPs that handle funds are in scope

Time limit to claims
A time limit of 13 months will apply to the last payment in the case

If you have any questions about the policy, please contact us on Appscamspolicyclarifications@psr.org.uk where we have set up a dedicated channel to respond to any clarifications that are raised.

Scope of the policy

Policy scope

The scope of the policy is set in SD20. In summary, it applies to **all** PSPs participating in FPS that provide relevant accounts

We have received several questions about the definitions or limits in the legal instruments of the APP scams reimbursement policy. Broadly, these

‘Consumer’	• This is defined in the legal instruments to include individuals, microenterprises or charities. • This only applies to the sending, not the receiving account.
Time limits	• To be in scope of the reimbursement policy, the FPS APP scam payment must have been made after 7 October 2024. • The time limit for a FPS APP scam claim is 13 months from the date of the final FPS APP scam payment of the claim. • Payments made before 7 October 2024 are out of scope of the reimbursement policy. • FPS APP scam claims made more than 13 months from the data of the final FPS APP scam payment of the claim are out of time, but the PSP can reimburse these as voluntary reimbursements, or subject to any other relevant regulation, legislation or code.
‘On us’ payments	• For a payment to be a “FPS APP scam payment” it needs to be executed through the Faster Payments Scheme. Where a payment is not executed through FPS, it is not in scope of the reimbursement requirement policy. • We expect some ‘on us’ payments will be made within a PSP. Some of these may be executed through FPS. For example, where PSPs are part of a group. These payments are in scope of the reimbursement requirement, provided they meet the rest of the criteria for an FPS APP scam payment.
Jurisdiction	• For a payment to be a “FPS APP scam payment”, it must be executed in the UK and received in a relevant account in the UK. UK is defined as England and Wales, Scotland and Northern Island (but not the Channel Island or the Isle of Man). Anything beyond this is outside the geographical jurisdiction of the policy. • This means, the “start” and “end” of the payment journey must be in the UK for payment to be in the geographical scope of the policy.

Key considerations for the application of the policy

Relevant account

- "*an account that is provided to a service user, is held in the UK and can send or receive payments using the Faster Payments Scheme, but excludes accounts provided by credit unions, municipal banks and national savings banks*"

Sending PSP

- "*a PSP that provides a relevant account for a consumer from which the FPS APP scam payment was made*"

Receiving PSP

- "*a PSP providing a relevant account into which APP scam payments are received*"
- customers include any type of service user (non-participant)

In scope transactions, account and PSPs

- Each PSP is accountable for determining whether Specific Direction 20 applies to it and its transactions. In determining whether a transaction is in scope of our policy, it is helpful and important to consider the sending and receiving accounts.
- In our Specific Requirement 1 and Specific Direction 20, these are defined as *'relevant accounts*' (also set out on the previous slide for ease of reference).
- Accounts which send or receive an APP scam payment are accounts provided to service users (see SR1 and SD20), not participants in the payment system. ‘Participant’ includes payment service providers, so an account which is provided to a PSP - for example as part of their access to the Faster Payments Scheme - is not a relevant account.
- PSPs which do not provide relevant accounts are unlikely to be caught by the FPS reimbursement requirement because they neither send, nor receive, Faster Payments related to the accounts they provide.

Examples of relevant accounts

- **Head Office Collection Accounts provided to service users**
  - These UK accounts are almost certainly relevant accounts because they can receive (and possibly make) Faster Payments and are provided to service users.
  - Examples could include:
    - the collection account of a UK utility provider used to receive bill payments
    - the account used by a crypto exchange to receive credit payments to a crypto wallet
- **Head Office Collection Accounts provided to PSPs**
  - These accounts are provided to PSPs, and not service users, and therefore are unlikely to meet the definition of relevant account.
  - Examples could include:
    - a collection account used by a building society to receive payments for its savings account customers (identified by a reference or roll number)
    - a collection account for a credit card issuer, used to receive payments to credit the account at that issuer

Example of not relevant accounts

- **Correspondent banking accounts** or **accounts used to send or receive FPS payments for foreign accounts which are provided to service users**
  - Where a Faster Payments transaction is addressed to a UK account (and this account is provided to another PSP), but the payment is received by a service user's account located outside the UK, this transaction is likely to be outside the geographical scope of the policy.
  - An example of this is a foreign bank using a UK Head Office Collection Account to receive payments for foreign accounts. These are unlikely to be within scope of the policy.

Payment Initiation Services and the policy

Policy statements do not mention PSPs other than sending or receiving PSP, except in Annex 2 June statement

- "*Payment initiation service (PIS) transactions are in scope of the new reimbursement requirement*"
- "*We apply the new reimbursement requirement to PIS transactions in the same way as with other types of Faster Payments. The obligations on sending and receiving PSPs are unchanged*"
  Policy statement, June 2023, Annex 2

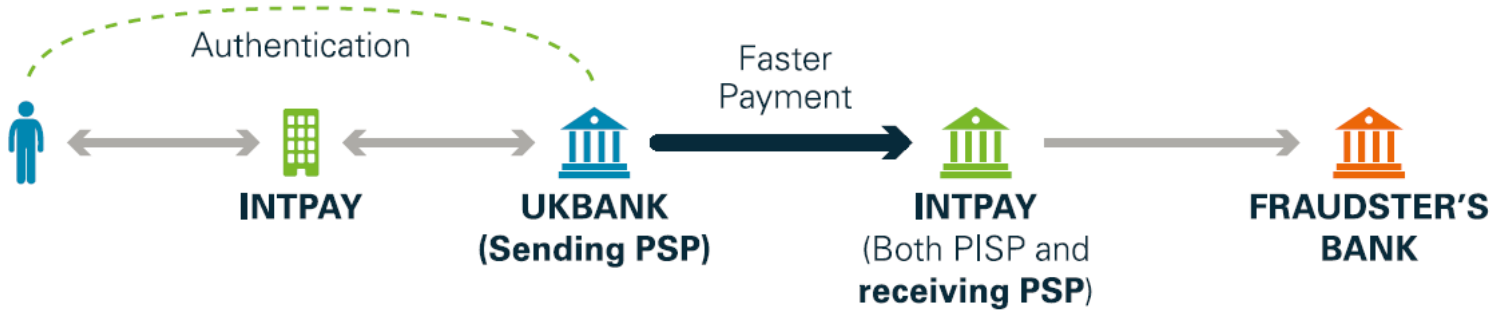
Specific Direction 20 in relation to reimbursement and FPS rules

- mentions only sending and receiving PSPs
- is silent on how the consumer initiates the payment(s)

PIS-initiated payments

Model A PISP has **no** access to funds during payment journey

Model B PISP operates as the receiving PSP
It has access and holds funds during the payment journey



In-scope transaction

Model A and B are PSR terms covering many business models

Sending and receiving PSPs obligations

Information sharing between sending and receiving PSPs

An APP scam claim is made once victim tells the Sending PSP that it has happened with details of the claim.

The Sending PSPs 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 an APP scam

The Sending PSP can stop the clock to pause the 5-business day assessment timeline in specified circumstances. This includes gathering additional information from the receiving PSP

The Sending PSP is responsible for reimbursing the victim. Its decision is final.

- We recognise that there may be circumstances where the Sending PSP requires information from the Receiving PSP to make a more informed assessment of the victim's claim.
- **Our legal instruments permit the Sending PSP to 'stop the clock' to gather information from the Receiving PSP.** This is at the Sending PSP's discretion. There are benefits to Sending PSPs 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.

Information sharing between sending and receiving PSPs

An APP scam claim is made once victim tells the Sending PSP that it has happened with details of the claim.

The Sending PSPs 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 an APP scam

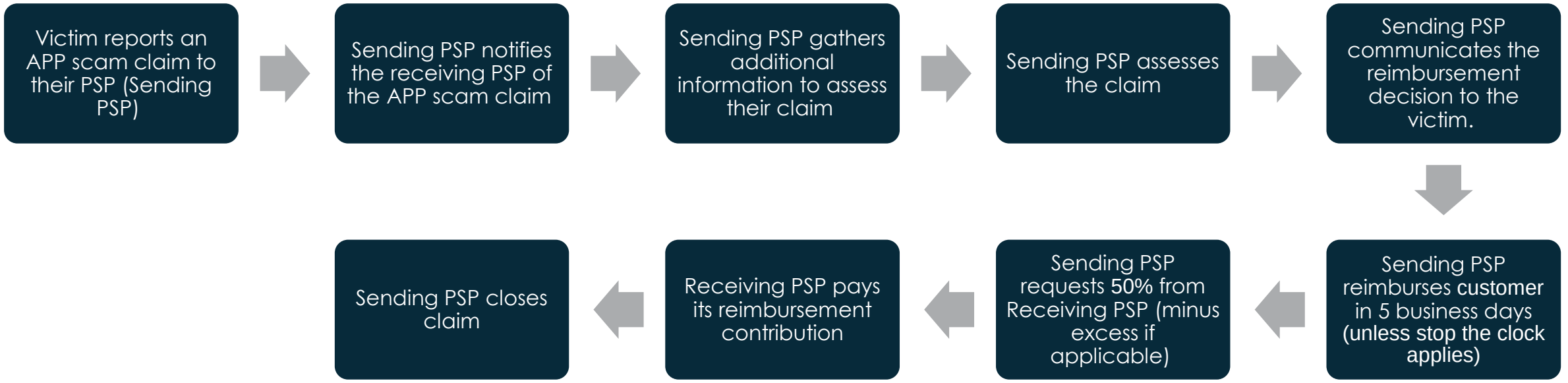
The Sending PSP can stop the clock to pause the 5-business day assessment timeline in specified circumstances. This includes gathering additional information from the receiving PSP

The Sending PSP is responsible for reimbursing the victim. Its decision is final.

- We recognise that there may be circumstances where the Sending PSP requires information from the Receiving PSP to make a more informed assessment of the victim's claim.
- **Our legal instruments permit the Sending PSP to 'stop the clock' to gather information from the Receiving PSP.** This is at the Sending PSP's discretion. There are benefits to Sending PSPs 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.

APP scams reimbursement journey

When the victim reports a scam, the Sending PSP should gather as much information as possible at the first point of contact. The information gathered from the victim should allow the Sending PSP to assess whether: the claim is in scope of the reimbursement requirement, there is evidence of first party fraud, the customer's vulnerability, if there is evidence of gross negligence.



'Auto-reimbursement'

We have heard industry refer to a number of scenarios as 'auto-reimbursement'. This is not a term the PSR uses.

We have set out here scenarios we are aware of, and how we consider the policy applies in these cases.

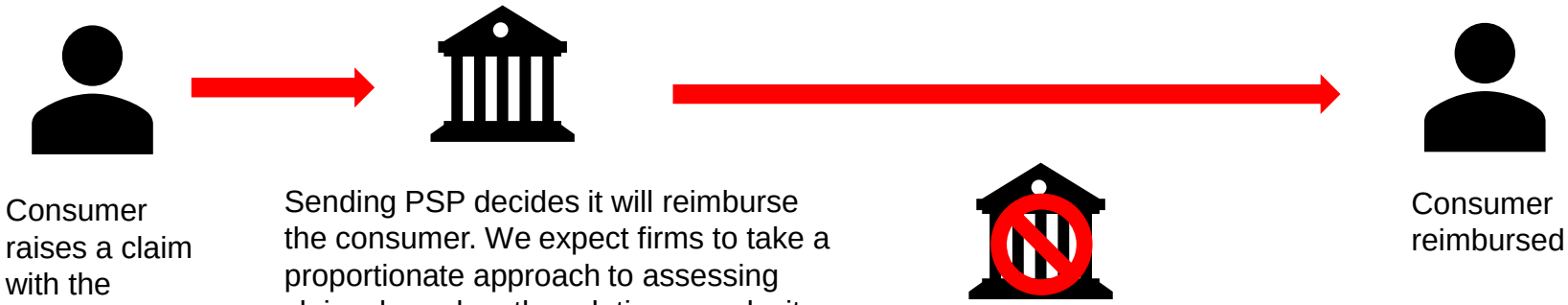
Consumer raises a claim with the sending PSP

Sending PSP notifies receiving PSP that a claim has been raised

Sending PSP decides it will reimburse the consumer. We expect firms to take a proportionate approach to assessing claims based on the relative complexity and value of the fraud.

Consumer reimbursed

In this example, the sending PSP is following the policy requirements by notifying the receiving PSP. This will support better fraud prevention across the industry.
The receiving PSP is liable to pay the sending PSP 50% of the reimbursable contribution amount.



Consumer raises a claim with the sending PSP

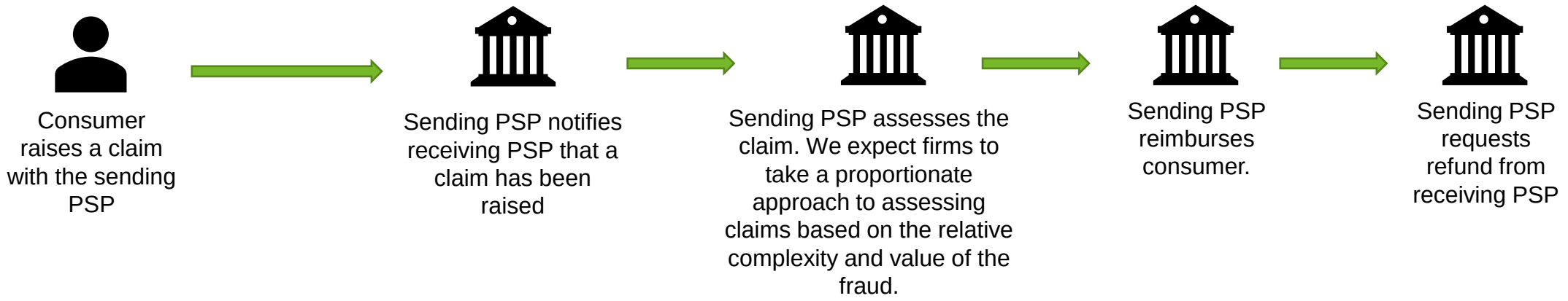
Sending PSP decides it will reimburse the consumer. We expect firms to take a proportionate approach to assessing claims based on the relative complexity and value of the fraud.

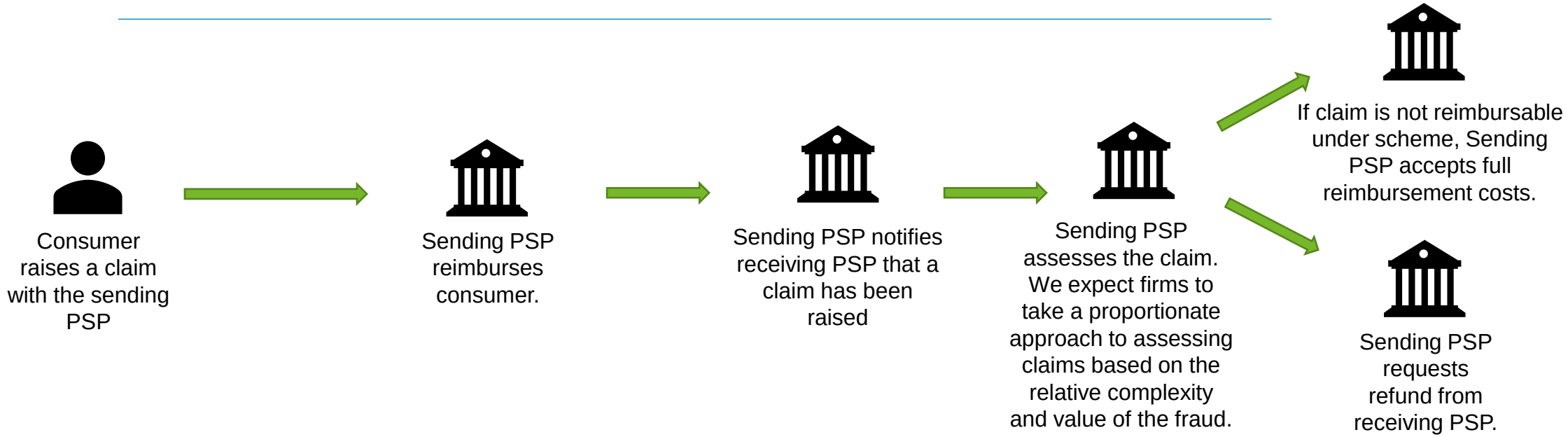
Sending PSP does not notify receiving PSP that a claim has been raised

Consumer reimbursed

In this example, the sending PSP is not following the policy requirements by notifying the receiving PSP. This will not support effective fraud prevention.
This is non-compliant with the reimbursement requirement

Advanced reimbursement





'Stop the clock'

The sending PSP must reimburse a victim of a reimbursable FPS APP scam claim within five business days. The sending PSP may ‘stop the clock’ if it has asked for information to assess the claim and is waiting for a response.

- Gather information from the victim (or their agent) to assess whether the claim is reimbursable or to assess the victim’s vulnerability
- Gather information from the receiving PSP to assess whether the claim is reimbursable
- Verify that a claims management company is submitting a legitimate claim
- Where the sending PSP has evidence of first-party fraud, gather additional information from the receiving PSP, law enforcement or other relevant parties
- For multi-step scams, to gather additional information from the other PSPs involved

The sending PSP may ‘stop the clock’ for these reasons

- Only the sending PSP can stop the clock.
- If the sending PSP is still awaiting information to assess a claim by the 35th business day, it must assess the claim based on the information it has.
- The clock is only stopped while the sending PSP is awaiting information.
- The clock restarts once the sending PSP has received the response.

Illustrative example of stop the clock where there are multiple queries

DAY 1	DAY 3	DAY 6
Sending PSP stops the clock to gather information	Sending PSP only receives information from Query 1. Clock remains stopped.	Sending PSP receives information from all queries. Clock re-starts.
Query 1	✓	✓
Query 2	✗	✓

Steps after reimbursing the consumer

Disputes

- We recognise there may be disputes between sending and receiving PSPs. Where disputes arise, we consider PSPs are best placed to determine how to resolve these, such as through independent external arbitration or the courts as with any other commercial dispute.
- Pay.UK may also introduce additional dispute resolution processes in their role as PSO.

Fund recovery

- We expect PSPs to make best endeavours to detect, freeze and return funds stolen as part of APP fraud.
- Where a receiving PSP recovers funds after the victim has been reimbursed, the firm should share these with the sending PSP (and vice versa).
- Any repatriated funds remaining after the PSPs have fully covered their costs must go to the victim: e.g. the victim should be reimbursed their claim excess by the sending PSP.
- In no case should the victim receive more than 100% of their original claim.

Treatment of the excess

Optional excess of maximum £100

Sending PSPs can apply a maximum excess of £100. Any future changes to this value will be subject to PSR review. This could be an appropriate mechanism to incentivise customer caution.

Application of the policy

- **The sending PSP can decide whether to apply the excess at the maximum value (£100),** or a lower excess (at any value up to the maximum) to a reimbursable APP scam claim. The sending PSP also has the option to not apply an excess at all.

- **If a sending PSP chose not to apply an excess, or to apply an excess below the maximum of £100, it cannot claim the amount not levied** from the receiving PSP as part of the 50-50 liability split between sending and receiving PSPs. **All 50-50 liability splits must be calculated on the assumption that a £100 claim excess has been applied**. **The receiving PSP is only liable for 50% of an in-scope claim less the maximum claim excess.** The table below sets out an illustrative example:

Excess levied on £1,000 scam	Amount reimbursed	Sending PSP liability	Receiving PSP liability
£0	£1000	£550	£450
£50	£950	£500	£450
£100	£900	£450	£450

Following slides provide use case examples of how the excess could be applied.

How the excess liability works

The excess is applied at claim level, not transaction level

Vulnerability (note the definition of vulnerability)

- PSPs can't deduct the excess with a claim involving vulnerable consumers – E.g.: For a loss of £150 the sending PSP will request £75 from the receiving PSP
- ~~If the receiving PSP disagrees on the assessment of vulnerability made by the sending PSP – it could take the dispute to independent external arbitration or the courts~~

Repatriated funds and excess

- If 100% of funds are recovered, the victim should be reimbursed their claim excess by the sending PSP
- 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 (e.g. the consumer loses £1,000, gets back £900 and the receiving PSP recovers £950, the sending PSP will get £450 from the receiving PSP and the customer will get additional £50 back). The sending PSP is in charge of what the consumer receives.

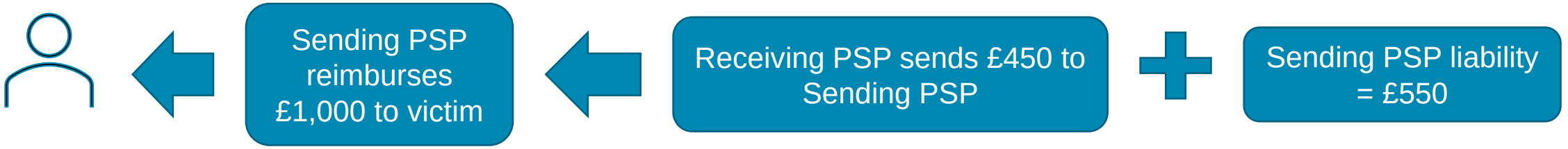
The excess liability will be proportionate to the value of the reimbursable (in-scope) APP scam claim – The liability will be split proportionately among receiving PSPs:

- Day 1 - Sending PSP will do the calculation
- Day 2 - Pay.UK single system will provide this capability

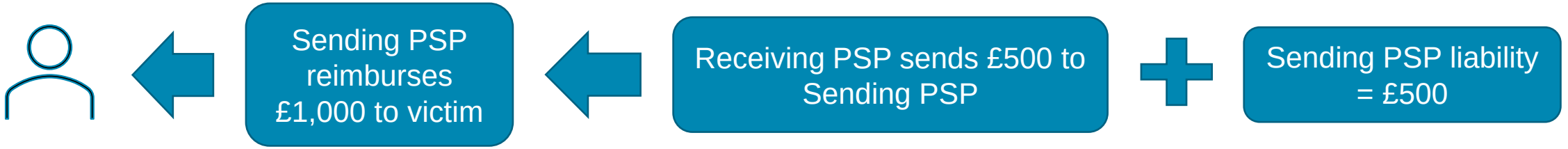
Examples with one sending and one receiving PSP

Scenario A - Consumer loses £1,000; Sending PSP applies £100 excess

Scenario B - Consumer loses £1,000; Sending PSP **doesn't apply the excess as business choice**

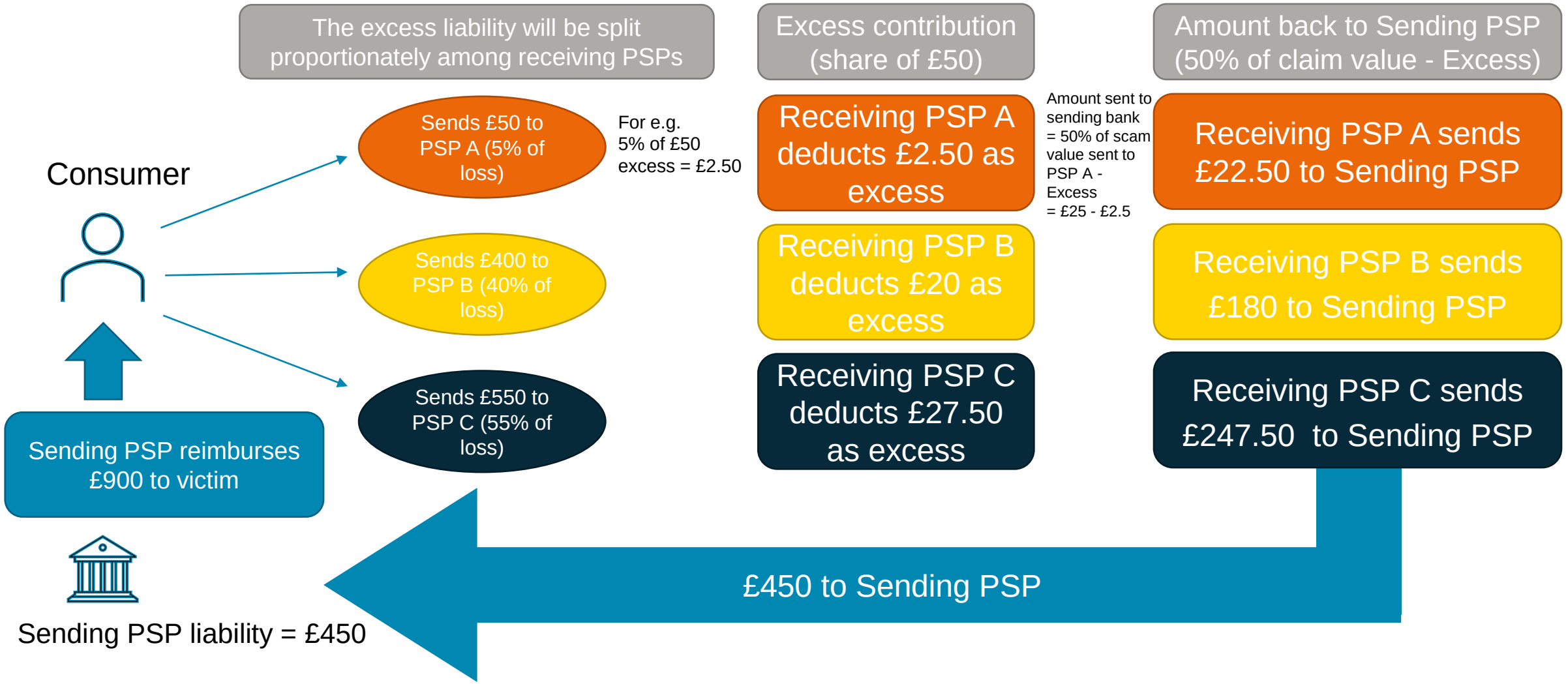


Scenario C - Consumer loses £1000; Victim is classified as **vulnerable customer**



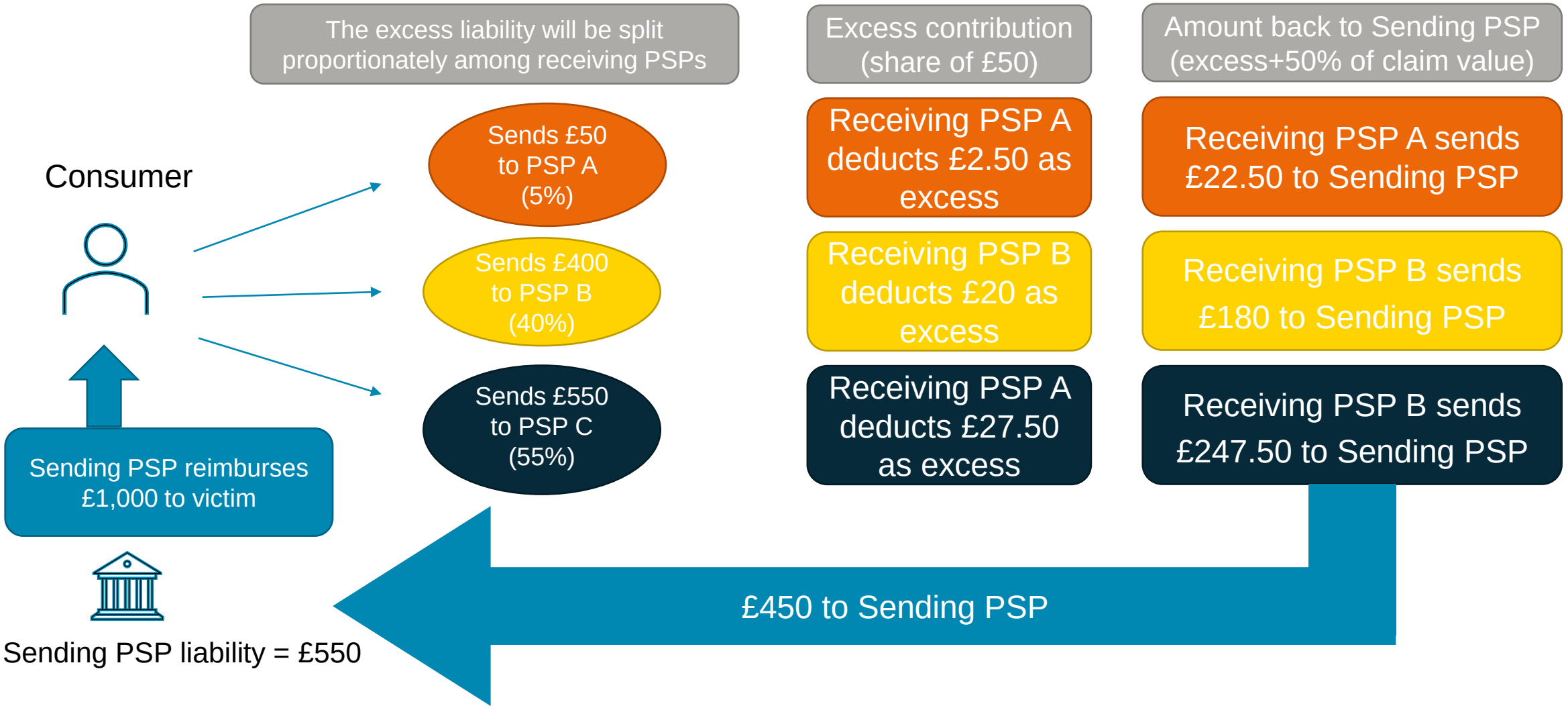
Scenario D: One sending and multiple receiving PSPs

Consumer loses £1,000; Sending PSP applies £100 excess



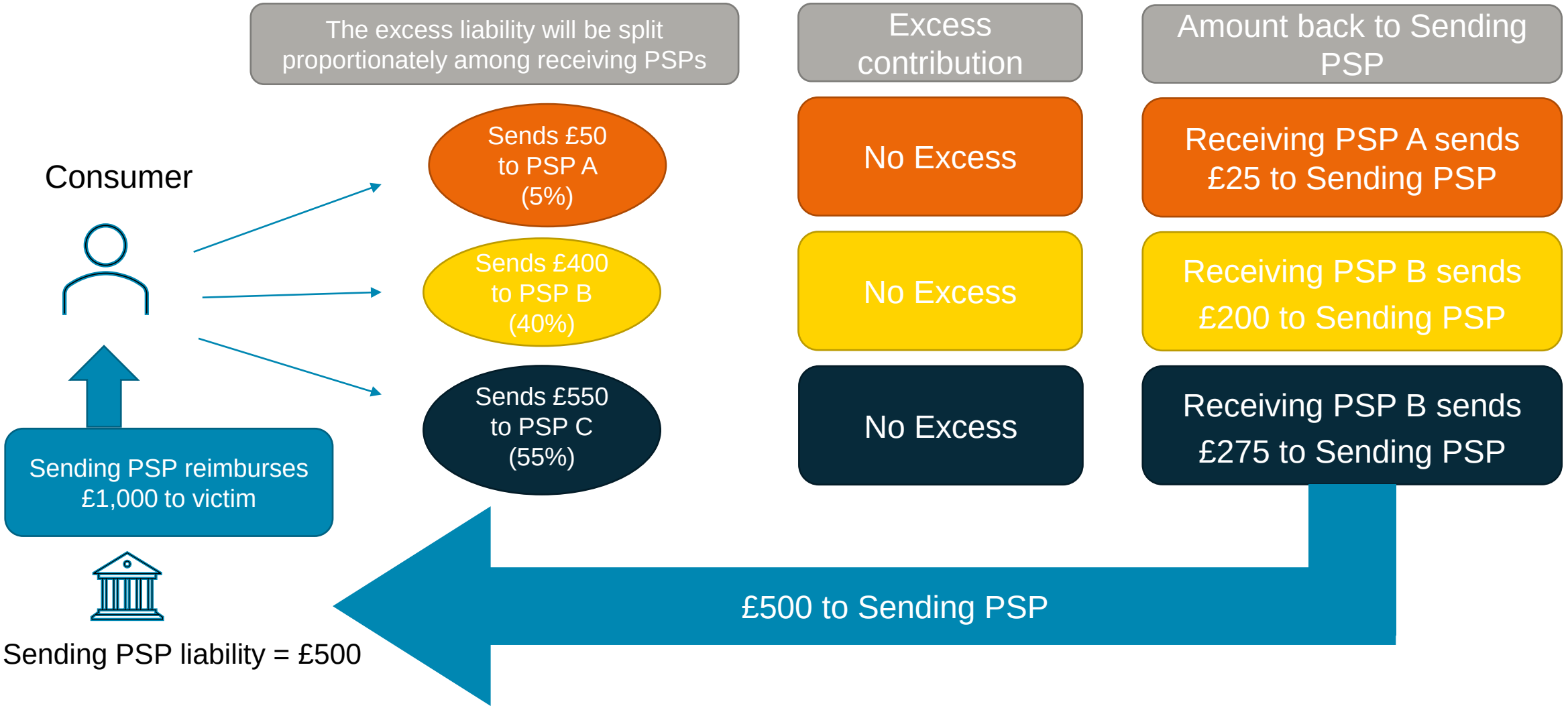
Scenario E: One sending and multiple receiving PSP, no excess applied

Consumer loses £1,000; Sending PSP **doesn't apply the excess** as **business choice**



Scenario F: One sending and multiple receiving PSP, vulnerable consumer

Consumer loses £1,000; Sending PSP doesn't apply the excess as consumer classed as **vulnerable**

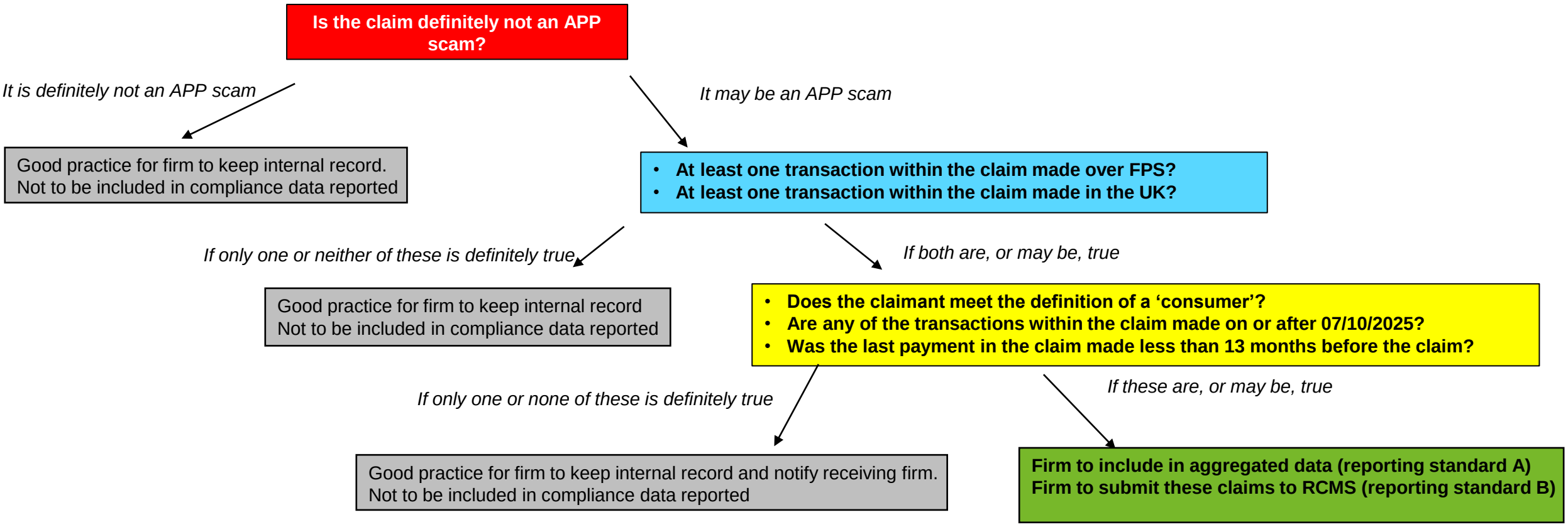


Compliance monitoring reporting boundary

Background

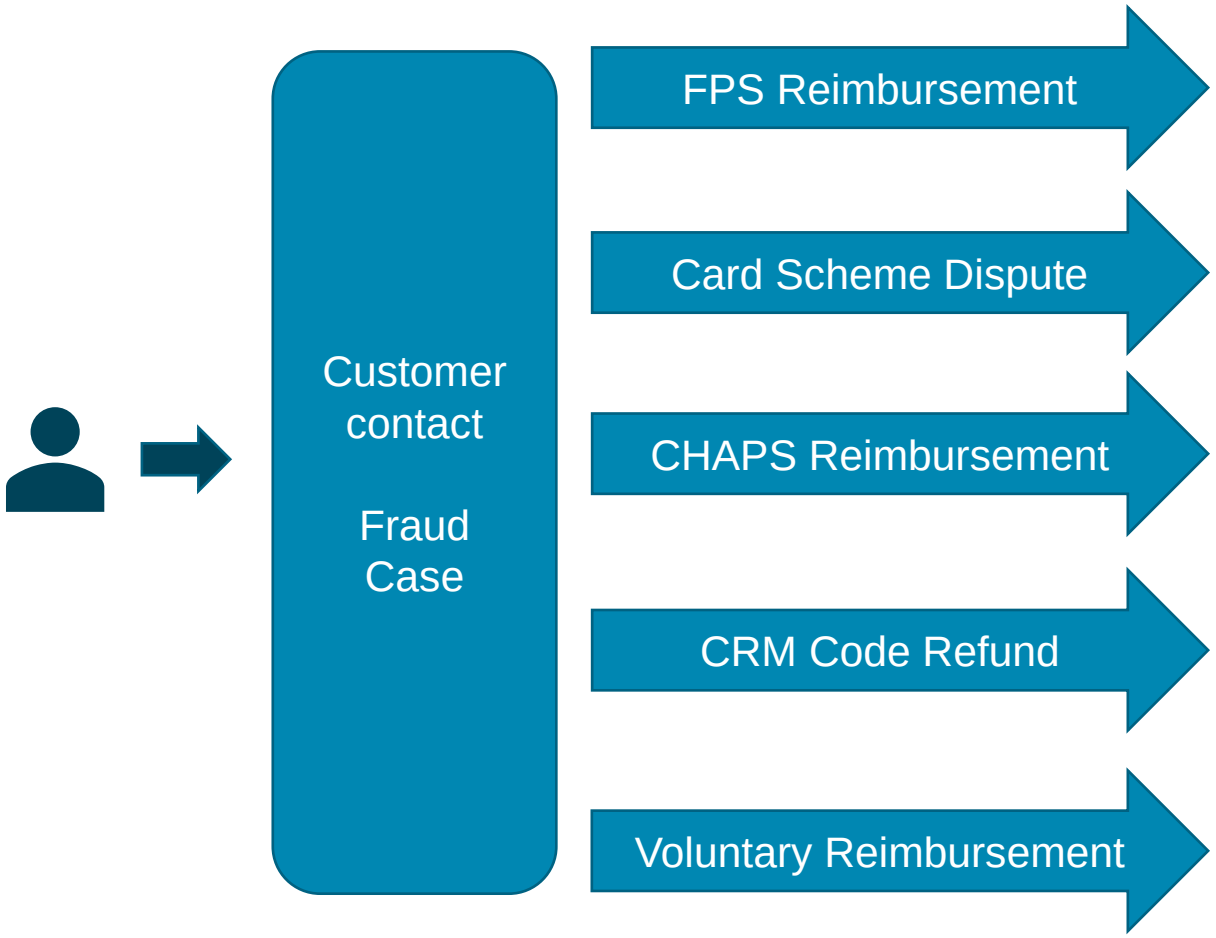
- We will set the boundaries of the data we require firms in scope of the reimbursement requirement must collect and/or report to the PSO for compliance monitoring purposes.
- Following feedback to our initial proposal on the reporting boundary, we have revised the proposal. These slides set out the revised boundary. We consider it strikes an appropriate balance between:
    - achieving good outcomes for service users
    - ensuring Pay.UK and PSR have effective oversight of firms' compliance
    - minimising the operational burden on firms
- We intend to establish this boundary in our spring '24 consultation – but not to consult on the boundary. This is to support firms' operational readiness.

Initial triage – decision tree



N.B. Both entire claims, and transactions within claims, may fall into the grey categories. We would expect the firm to consider any of these transactions or claims for reimbursement under other schemes.

Example treatment of payments or claims under different schemes



PSR Payment Systems Regulator

Next session will take place on 10th April 2024.
Please register online on our website. Details and registration form will be uploaded soon.

How industry should be preparing for 7th October

Actions		
Sending PSPs side	**Receiving PSPs side**	**All**
• Systems in place to respond to claims: PSPs have staff trained, call centres ready to deal with enquiries, processes in place to log cases, they know what information to ask, escalation mechanisms, working/non-working hours processes, information on website • PSPs have processes to handle information and send it to recipients (what information and how to share it) • PSPs have internal review process to investigate / evaluate cases (and vulnerability) and make the decision to reimburse, they know what and how to communicate outcome to their customers and how to reimburse them (within 5 business days – subject to stop the clock)	• PSPs know how to receive information, processes to deal with it and respond to information request from sending PSP in good time • PSPs know how to transfer the 50% back to the sending PSP (implementation)	• Sending and Receiving PSPs have the systems / processes to communicate to each other (implementation) • Contingency plans in case of technical issues from one side or the other (implementation)