

APP Scams - PSR Industry Engagement Session 6

18 June 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

Complex business models

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.

Complex business models

In scope transactions, account and PSPs

- Each PSP is accountable for its own compliance with Specific Direction 20 including whether our direction 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*'. PSPs which do not provide relevant accounts are unlikely to be caught by the FPS reimbursement requirement.
- Each APP Scam Claim must be assessed and therefore each payment within a claim must be assessed.
- The following slides lay out one way to help determine whether a claim and its payments are in scope for assessment.

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 definitions and considerations for the application of the reimbursement 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”*

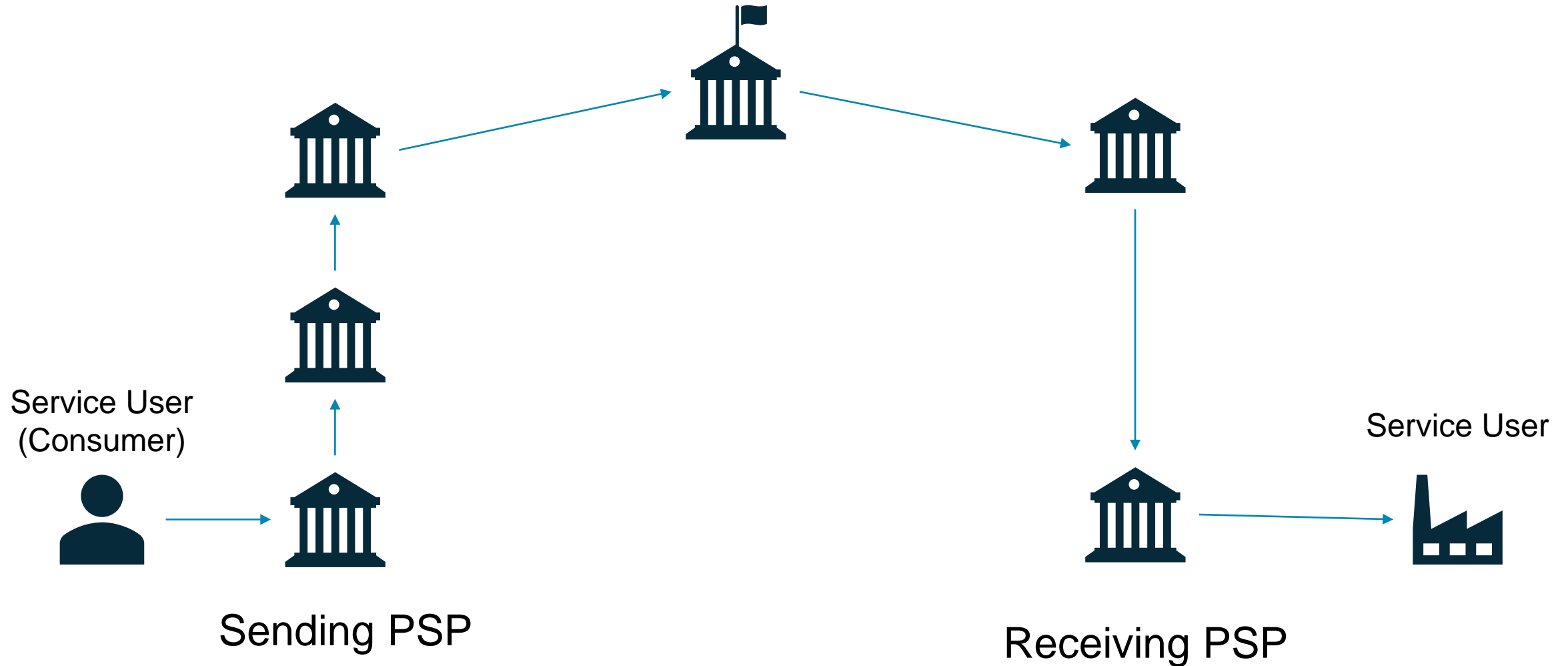
Sending PSP

- *“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)

The Sending and Receiving PSPs can be indirect participants



Assessment of scope, claim and payment

PSR OFFICIAL

PSP

Payment Service Provider

Faster Payments

Relevant account

Claim

Genuine APP Scam

Faster Payments

Sending consumer's relevant
account

Payment

Receiving relevant account

Unintended recipient or purpose

Authorised by victim

Loss of control

Reimbursable?

Is my firm in scope?

Is it a Payment Service Provider?

Does it have access to Faster Payments?

Does it provide relevant accounts?

I've received an APP Scam report.

Do I have the basic information?

Is it a complete claim?

Were the payments sent as Faster Payments?

Did it come from a relevant, consumer account?

I'm looking at each payment in a claim..

Is the receiving account a relevant account?

Was it for an unintended purpose or to an unintended recipient?

Did the victim (my consumer) authorise it?

Was the receiving account not controlled by the victim?

Is this payment a reimbursable APP Scam payment?

Industry question: Are Head Office Collection Accounts (HOCA) in scope?

Is it a relevant account?

- Held in the UK?
- Provided to a Service User?
- Can send or receive Faster Payments?
- (Provided by a Payment Service User?)

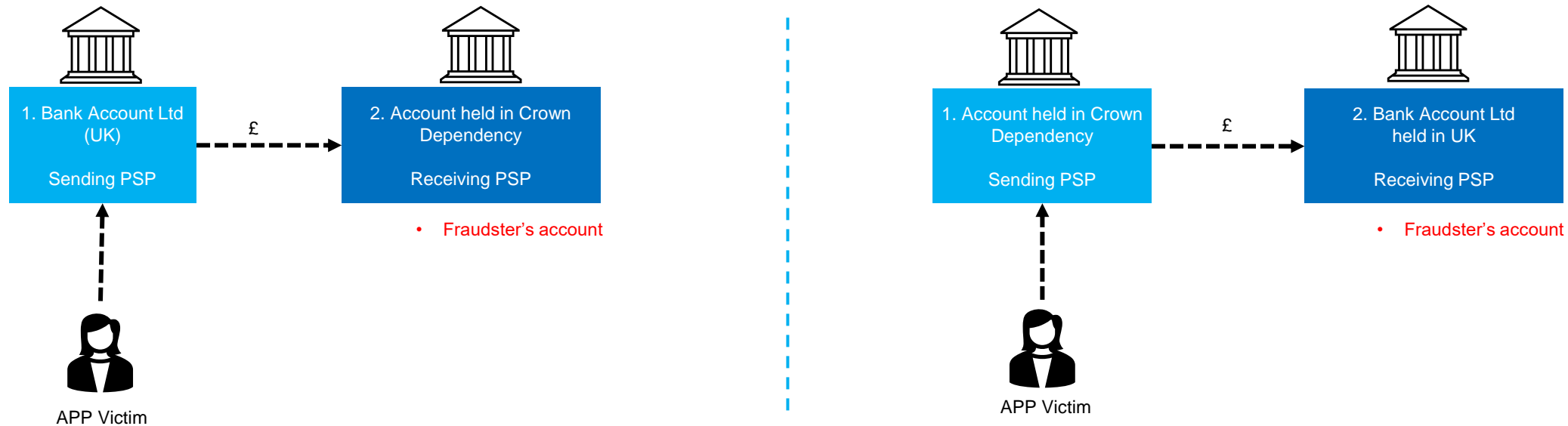
PSP liability scenarios

"UK Finance has kindly provided some broad examples and has analysed these to help increased understanding in their membership and the wider industry. We note that each case turns on its own merits and so any interpretations have to be made in that case-specific context. In this session we will be discussing some of the important questions which PSPs will need to ask themselves as part of their assessment. Comments from the PSR are in blue text boxes."

Source: UK Finance

Receiving PSP Scenario 1 | Crown Dependency scenarios – out of scope for Reimbursement

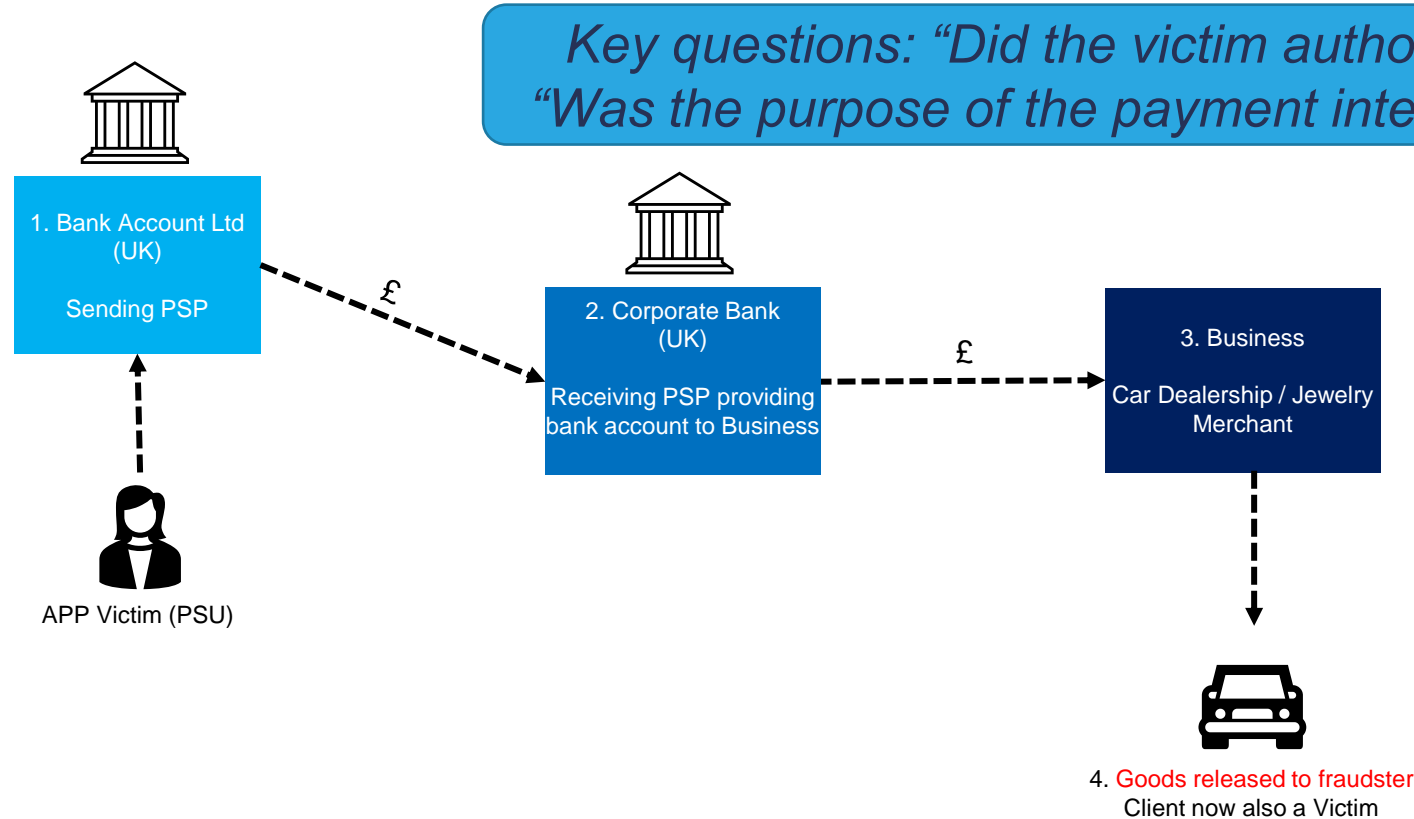
Key question: “Is the PSP providing a relevant account held in the UK?”



Both scenario's are out of scope as one PSP in both scenario's reside outside of the UK, therefore NOT meeting the definition of a relevant account.

Receiving PSP Scenario 2 | Non-Complicit Beneficiary / Unwitting Mule

This is a payment scenario where a victim is coerced by a fraudster into making a APP to a merchant/client with the aim of obtaining goods or services. Both the Victim and the merchant are victims of the APP scam.



Following the PSR’s clarifications outlined on slide 9, **Corporate Bank UK would be in scope** as the receiving PSP. The payment is made to an account **not** in the control of the consumer. The account held with Corporate Bank UK meets the definition of a **relevant account**, in that it is provided to a service user, is held in the UK and is able to send and receive payments.

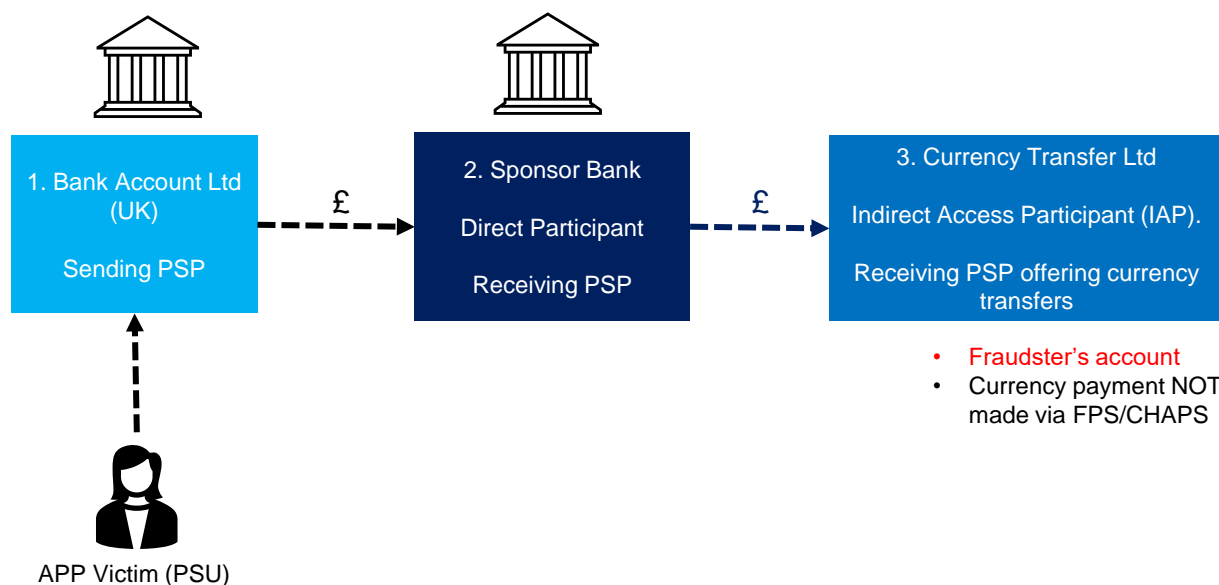
Concerns raised that this could impact the relationship between the PSP and genuine customer. This is a significant shift and poses a risk that a victim be treated incorrectly. E.g. victim reimbursed then posts on social media that the business is run by a criminal when the business themselves are also a victim.

Source: UK Finance

Receiving PSP Scenario 4 | Multi-step international payments

A payment is sent from a UK PSP to another UK PSP who holds a relationship with a currency transfer platform client who then sends a currency payment to a recipient account controlled by a fraudster...

*Key questions: “Does the receiving PSP provide a relevant account?”
“Was the purpose of the payment intended by the payer?”*



Following the PSR’s clarifications outlined on slide 9, **Currency Transfer Ltd would be in scope** as the receiving PSP. They are an FCA regulated firm. Sponsor bank are not in scope as they are providing an account to a participant of the payment system.

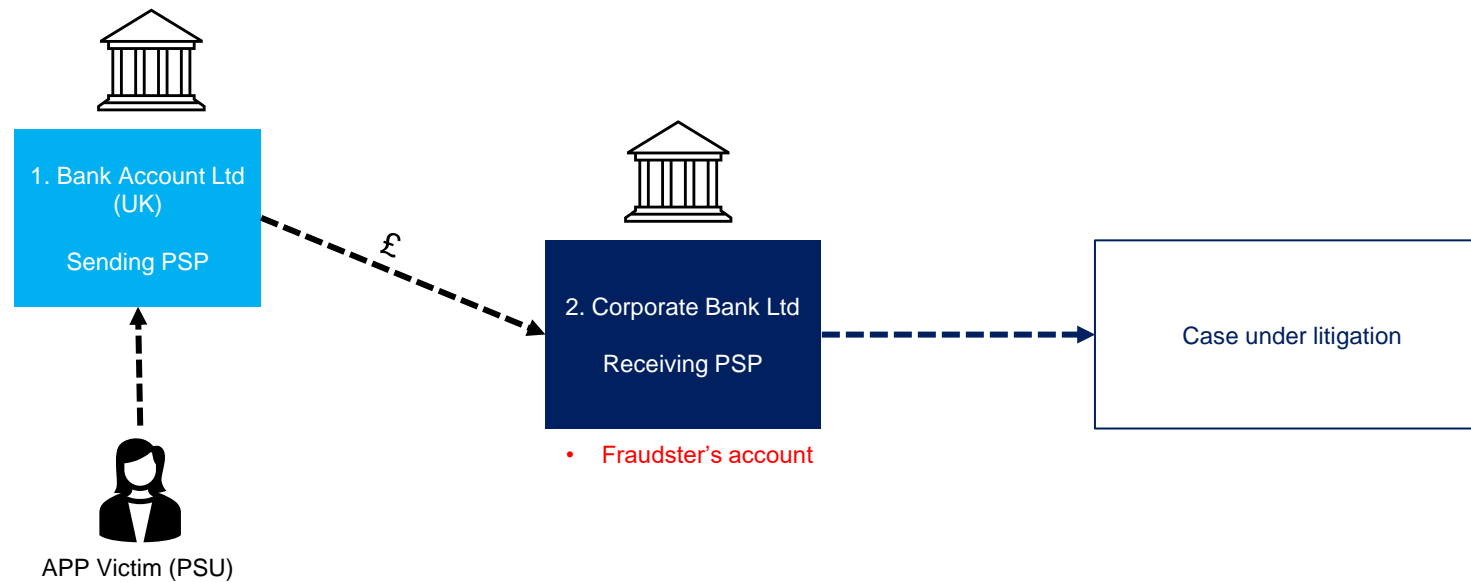
Currency Transfer Ltd is almost definitely a relevant account as it is an account provided to a service user, which can send and receive FPS payments. The payment received into this account is **not** in the control of the consumer.

Source: UK Finance

Receiving PSP Scenario 5 | Complex APP scams subject to investigation / court order / litigation

Law enforcement is investigating a scam, particularly common with Investment Scams.

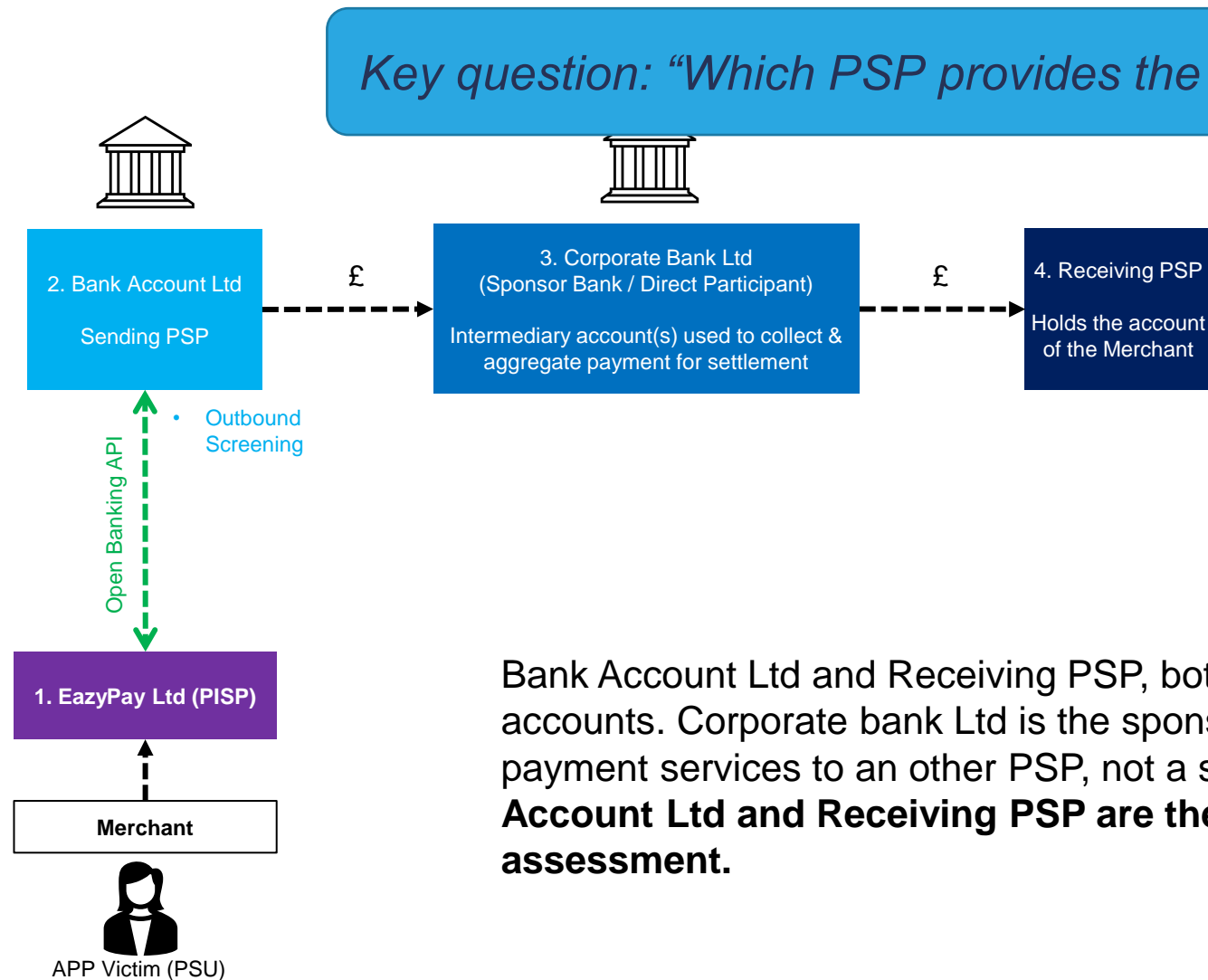
PSR consulted on complex or exceptional cases in CP24/3



This scenario will form a question within the compliance monitoring consultation due to be released in May.

Receiving PSP Scenario 7 | Multi-PSP payment flow

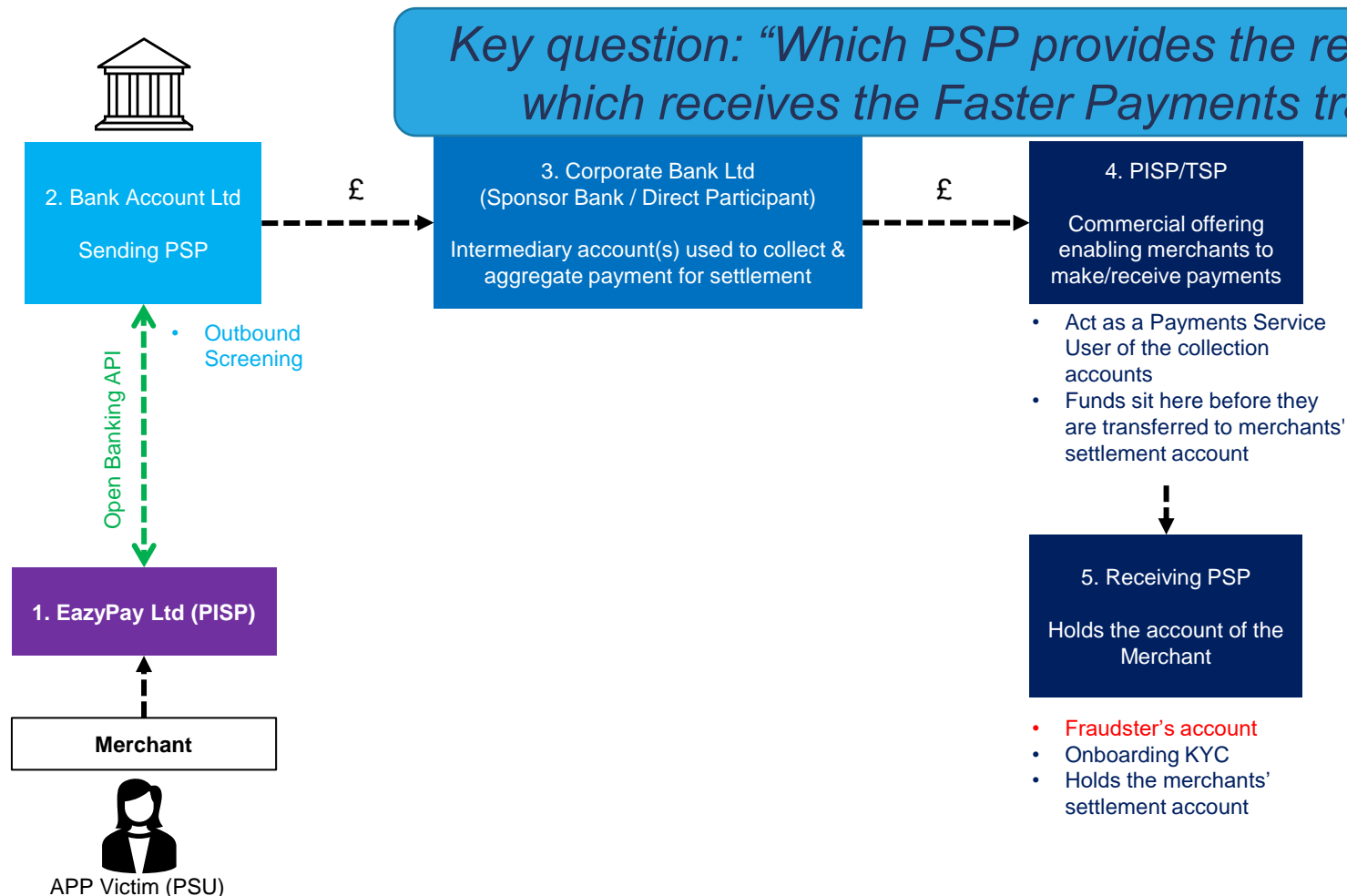
This is a typical Open Banking PISP Model where Account to Account (A2A) payments are aggregated. This is a Corporate Banking service. The PISP is serving a Payment Services Provider.



Bank Account Ltd and Receiving PSP, both hold relevant accounts. Corporate bank Ltd is the sponsor bank providing payment services to an other PSP, not a service user. **Bank Account Ltd and Receiving PSP are therefore in scope for assessment.**

Receiving PSP Scenario 8 | Payments - Acquiring

This is a typical Open Banking PISP Model where Account to Account (A2A) payments are aggregated. This is a Corporate Banking service. The PISP is serving a Payment Services Provider.

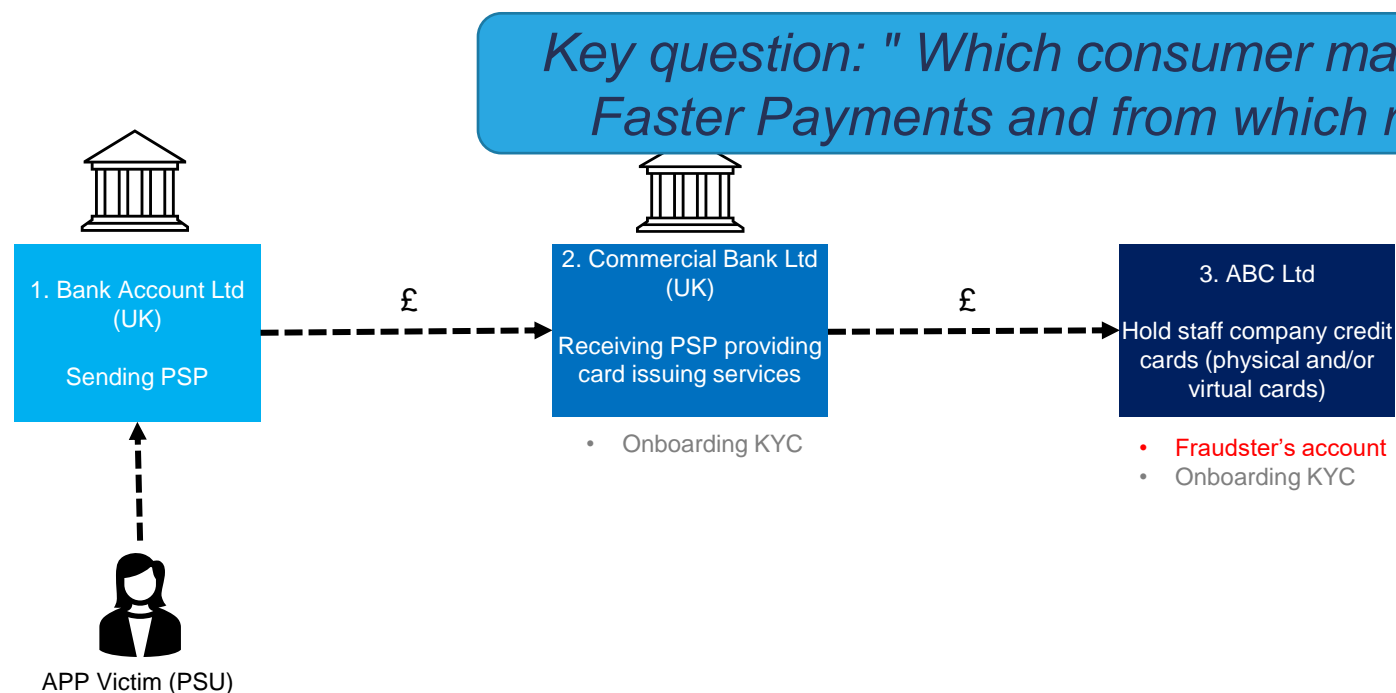


PSPs at 2 and 4 are liable. The PSP at 4 will recover funds from the firm at 5 (a non-regulated entity), through contractual terms. Individual firms will need to determine the contractual arrangements for funds recovery from non-regulated entities.

? What would be the outcome of 5. was also a regulated entity?

Source: UK Finance

Receiving PSP Scenario 9 | Payments – Issuing of Credit Lending Products

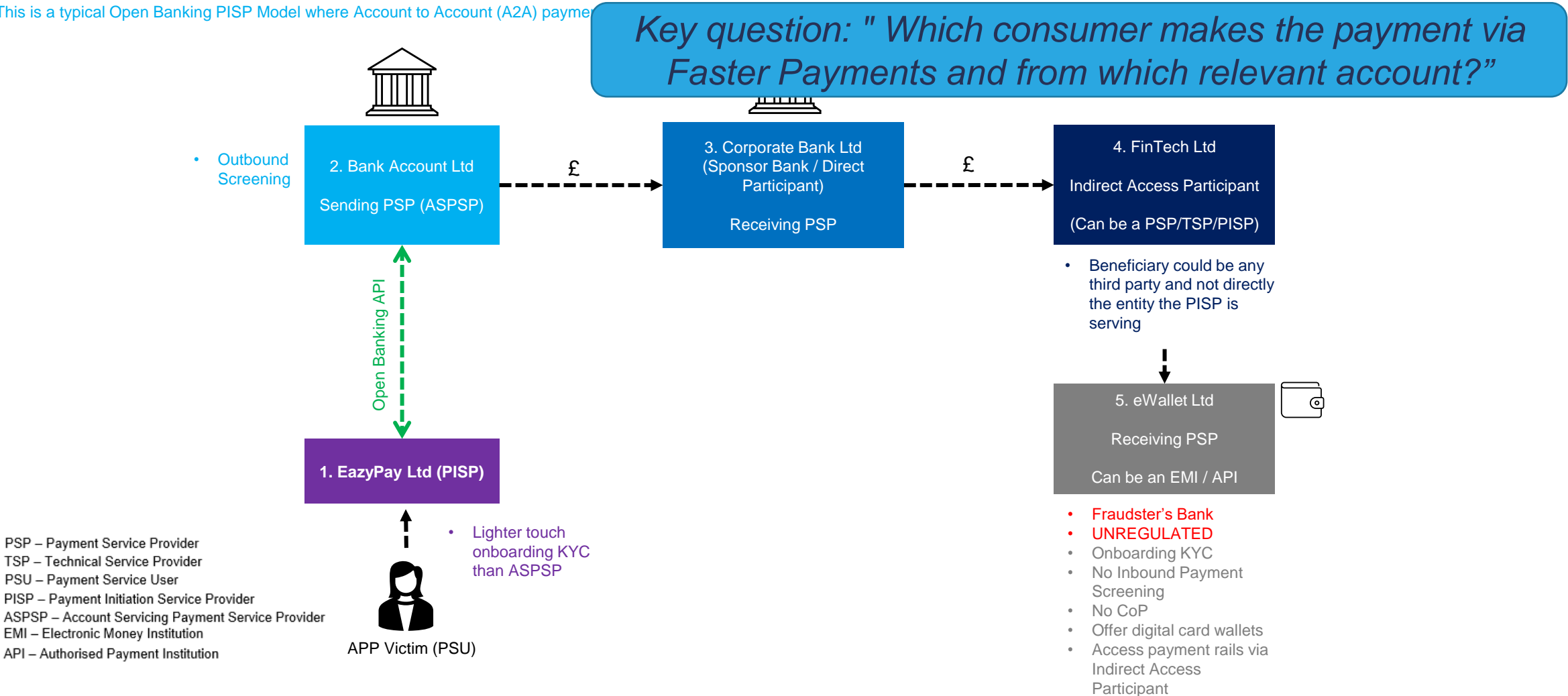


ABC limited is a private company, not a PSP. Commercial Bank Ltd provide ABC Ltd with staff company cards. Commercial Bank Ltd hold the HOCA which transfers the funds to ABC Ltd. A 3rd party consumer (Bank Account Ltd) is coerced by a fraudster into making a payment on to a company credit card held at ABC Ltd.

Where Commercial Bank is not the issuer of the credit card and only provides clearing services, the credit card issuer (not shown on this slide) will be the in scope receiving PSP

Receiving PSP Scenario 10 | Multi-PSP Open Banking payment flow

This is a typical Open Banking PISP Model where Account to Account (A2A) payment



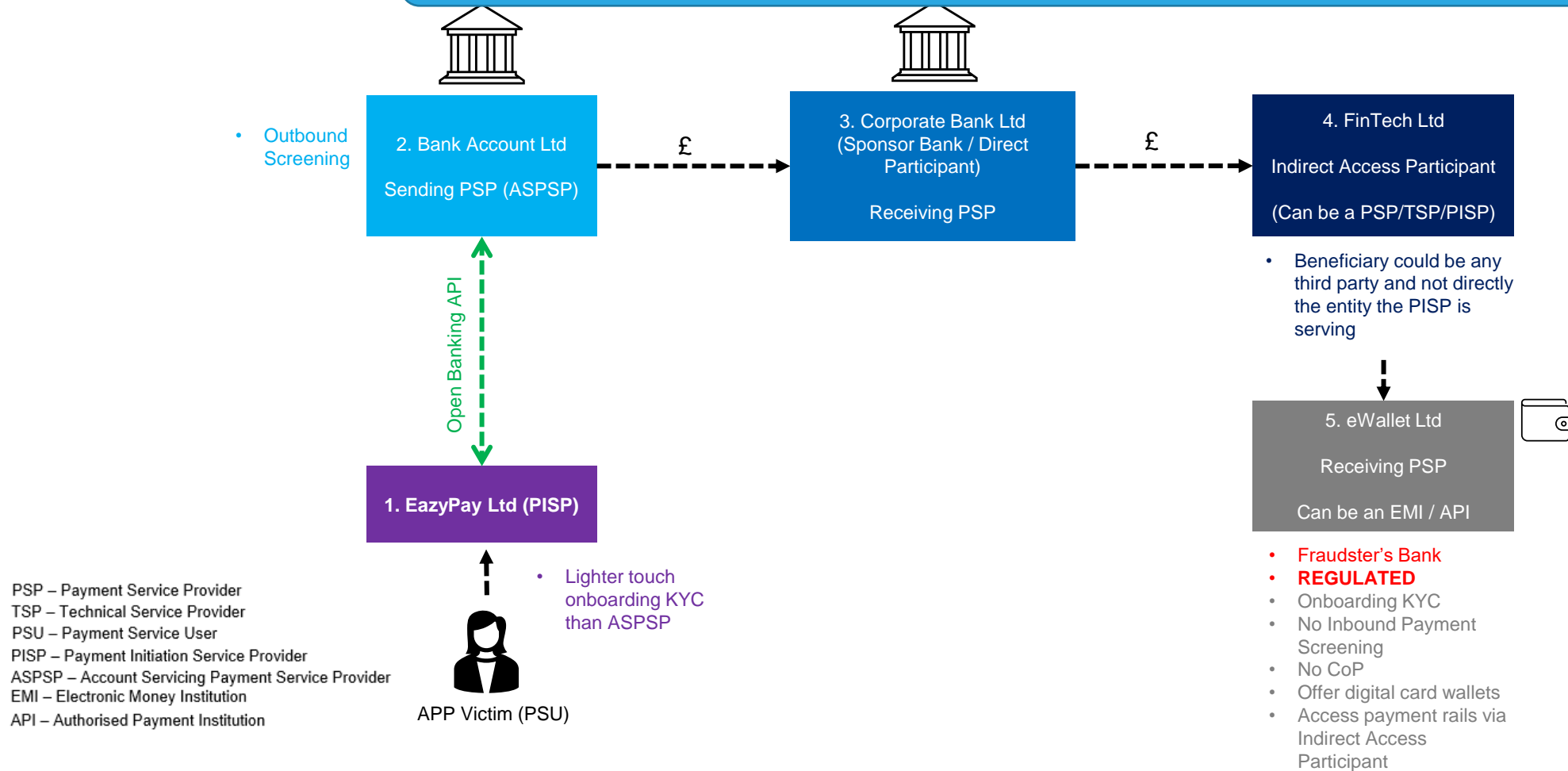
Same as scenario 8, i.e. PSPs at 2 and 4 are liable. The PSP at 4 will recover funds from the firm at 5 (in this case a non-regulated entity), through contractual terms. Individual firms will need to determine the contractual arrangements for funds recovery from non-regulated entities.

Source: UK Finance

Receiving PSP Scenario 11 | Multi-PSP Open Banking payment flow

This is a typical Open Banking PISP Model where Account to Account (A2A) payments are aggregated. This is a Corporate Banking service. The PISP is serving a Payment Services Provider.

Key question: "Which relevant account receives the FPS APP Scam payment?"



PSPs at 2 and 5 are liable (5 is a regulated relevant account).

Source: UK Finance