Payment Systems Regulator

APP Scams - PSR Industry Engagement Session 7

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

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.

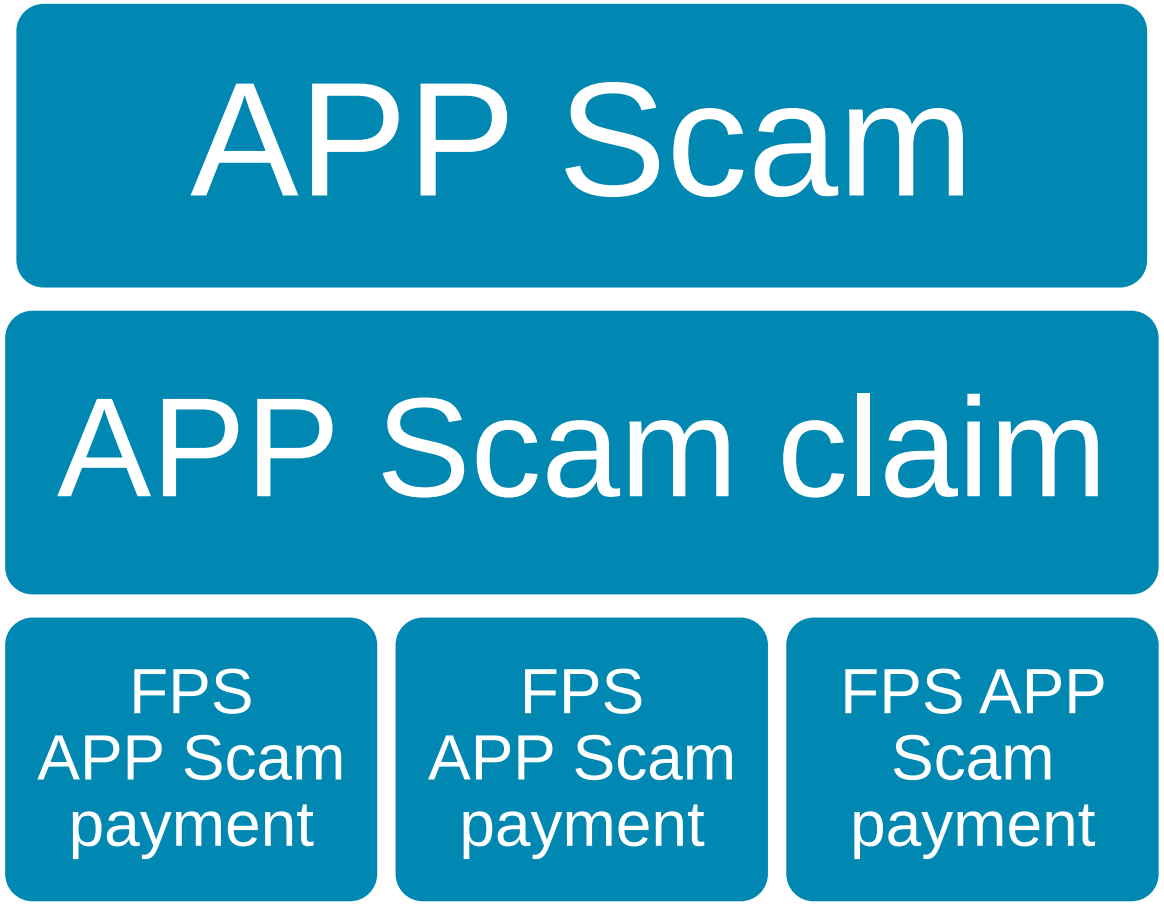
How are "Me2Me" payments treated under APP Scams Reimbursement Requirement

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.*

Assessment of scope, claim and payment

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?

I've received an APP Scam report.

- Do I have the basic information?
- Is it a genuine 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?

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

- consumer account – was the account in the control of the consumer?
- 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)?

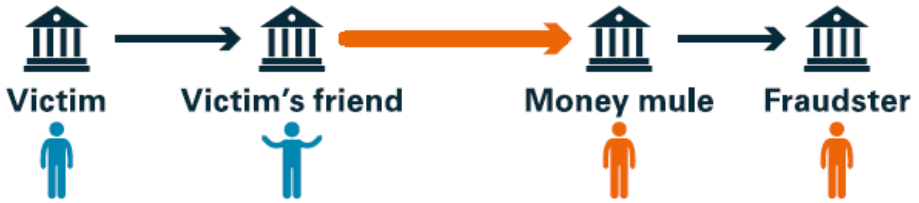
Payments within scope – Policy statement June 2023

Use of mule account

Individual sends a Faster Payment to a money mule which is then sent on to the fraudster

Friends and family

Individual sends a Faster Payment to a trusted friend/family member account which is then sent on to a money mule via a Faster Payment, and finally to the fraudster



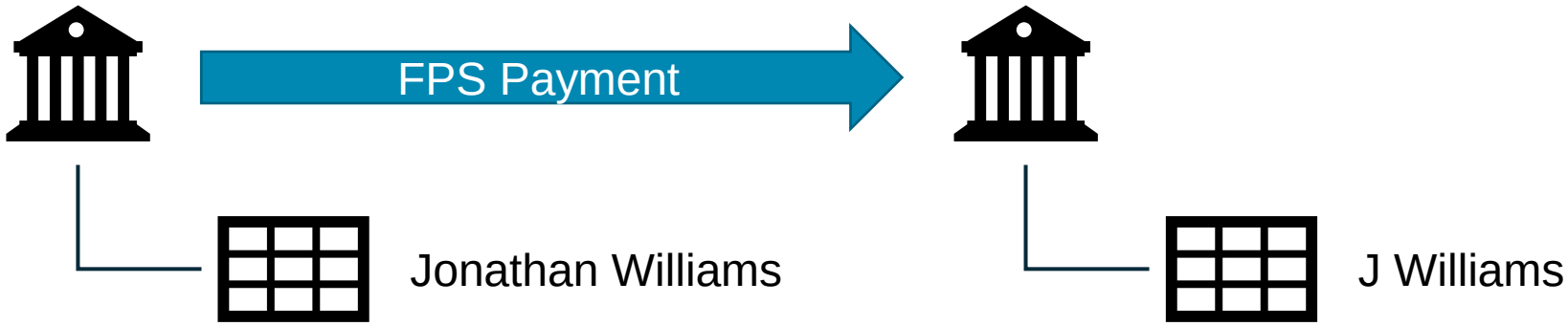
Use of out of scope payment systems

Individual sends a crypto payment to a fraudster

In-scope transaction Not in scope

Examples of Me2Me consideration

Example 1

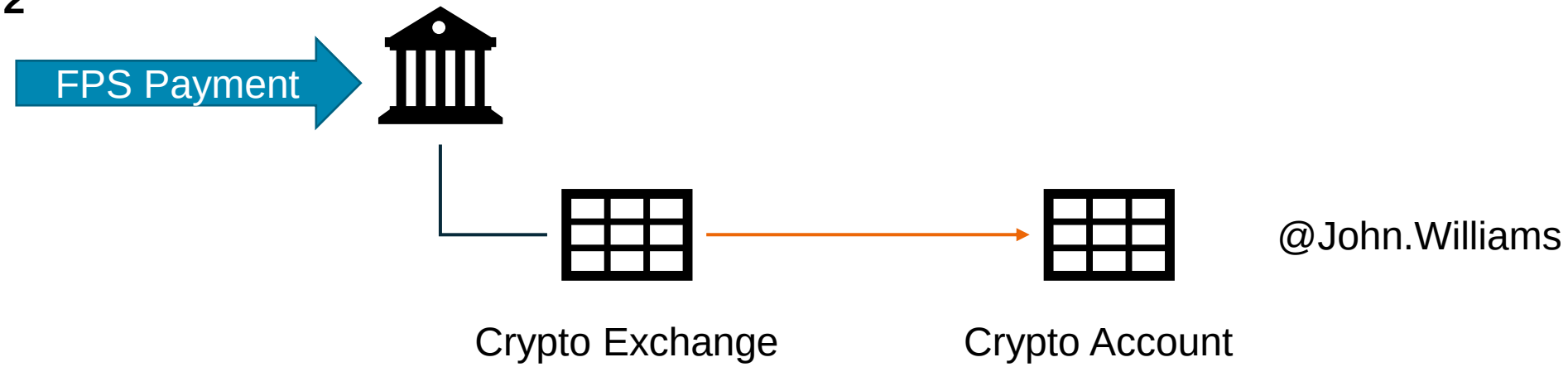


Reimbursable APP Scam payment?
Who initiated payment?
? Consumer
? Fraudster

Reimbursable APP Scam payment?
Is the receiving account in customer's control?
? Consumer's account
? Fraudster accessed - account in customer's control
? Account takeover- account not in customer's control
? Fraudulent account – never account in customer's control

Examples of Me2Me consideration

Example 2



Reimbursable APP Scam payment?

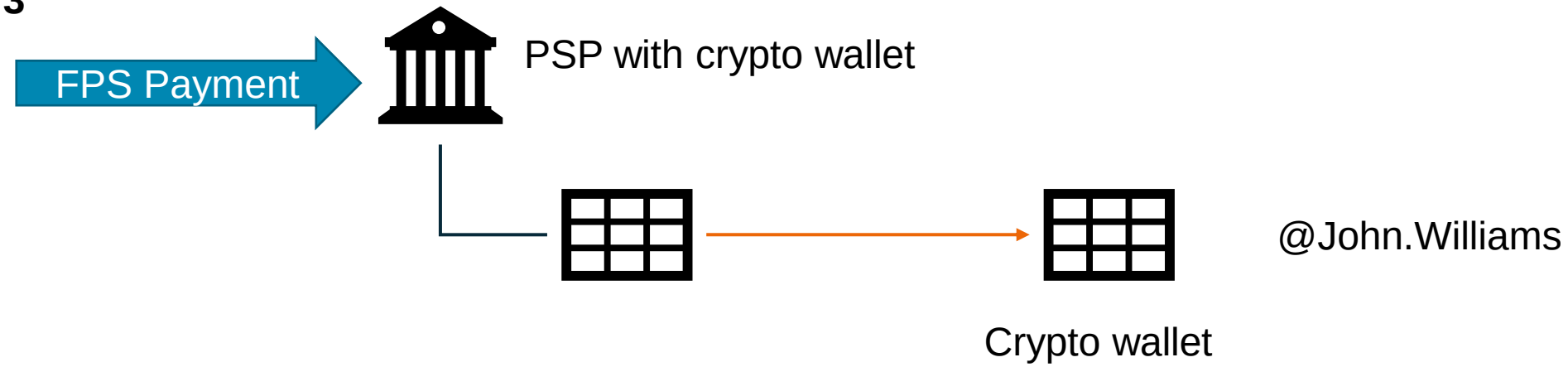
What is the intent of the consumer in making the payment?

? 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



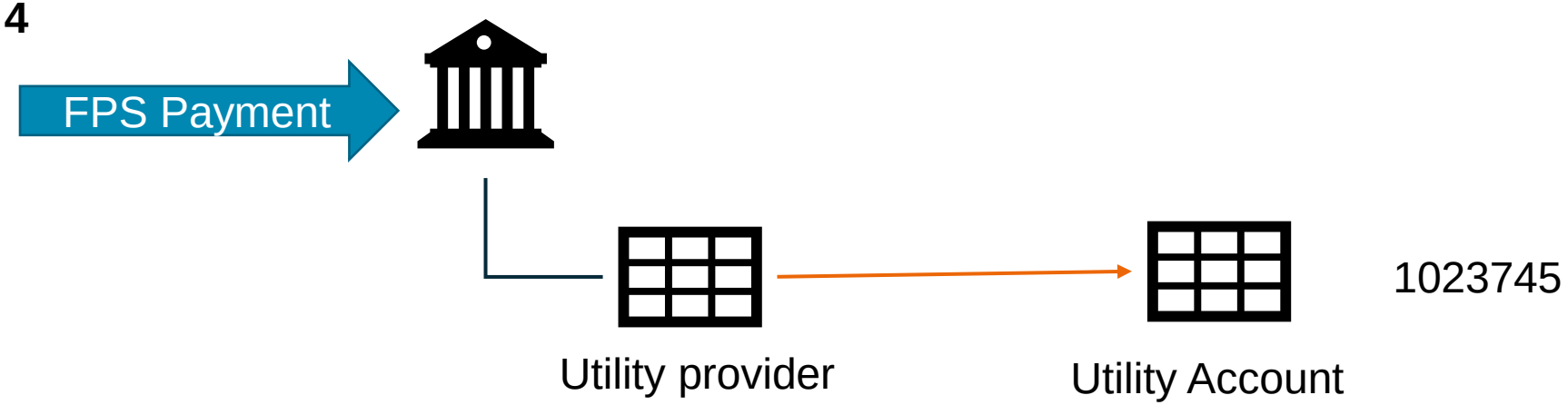
Reimbursable APP Scam payment?

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

- ? 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?

? 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

Me2Me

"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 context. In this session we will be trying to identify some of the important questions which PSPs will need to ask themselves as part of their assessment."

Source: UK Finance

Me2Me Scenarios

- ***Scenario 1*** *- The consumer sent a payment from an account in their name to another account in their name which the consumer had full control of at the point the payment was made. Irrelevant of any subsequent payments made from account two, the payment between account one and two is out of scope of the reimbursement requirement.*

  Key question: "Did the victim have control over the receiving account?"

- ***Scenario 2****: The consumer sent a payment from an account in their name to another account in their name, of which the criminal has dual control at the point the payment was made, with the consumer providing the scammer with access to their personal details. This scenario will be heavily influenced by the circumstances of the scam and assessment of the movement of funds from accounts B to C. In no scenario will the payment from A to B be in scope.*

  Key question: "Did the victim have control over the receiving account?"

Source: UK Finance

Me2Me Scenarios

- ***Scenario 3:*** *The consumer sent a payment from an account in their name to another account in their name – the consumer had assisted the criminal in opening this account, but the consumer has not accessed this account and has no knowledge of how to. The criminal has sole control at the point the payment was made. The payment from account A to B is in scope of the reimbursement requirement.*

  Key question: "Did the victim have control over the receiving account?"

- ***Scenario 4:*** *The customer sent a payment from an account in their name to another account in their name, the customer did not open the account and the criminal still has control of the account at the point the payment was made. The payment from account A to B is in scope of the reimbursement requirement.*

  Key question: "Did the victim have control over the receiving account?"

Source: UK Finance

Me2Me Payments

Case Studies

Key questions:
"Who initiated the payments from Banks B and C?"
"Did the victim have control off the receiving account D?"

Scenario 1 (Multi Bank)

- A customer reported being a victim of an impersonation scam to Bank A
- As part of the scam the customer was asked to send funds to 3 accounts (Banks B, C & D)
- The accounts with Bank B & C were established accounts held by the customer
- The 3rd account (Bank D) was in the customer's name however was opened during the conversation with the bad actor
- According to the customer testimony they did not have control of the 3rd account (Bank D)
- The customer also testified that they did not make the transfers from the established accounts at Bank B & C and that the money was moved onward by the fraudster into an unknown Mule account
- The customer also reported the claim to Bank B, C & D directly
- The outcome of Bank B & C investigation is unknown
- Bank D refuted the customer's claim that they did not have control of the account. This decision was based on the account opening docs, anti-impersonation, contact numbers and correspondence address matching the customer's details
- Furthermore, Bank D was able to confirm that the customer had received and used the bank card associated with the account

When applying the PSR definitions:
Following the PSR's definitions banks B, C and D would need to investigate to determine the accuracy of the consumers claims. Dependent on the outcome of the investigation, banks B and C may be liable for allowing an unauthorised transaction.

In this case, if bank D can confirm that the customer did have access and had used the bank account held with them, bank D would find themselves fully liable for the unauthorised transaction out of the account, where they are unable to evidence gross negligence by the consumer. It is arguably in Bank D's interest not to prove that the customer had access as this would move the payment from A – D into scope of the reimbursement requirement and bank D would only have 50% liability…….

Source: UK Finance

Me2Me Payments

Case Studies with PSR Clarification

Key questions:
"Did the victim have control of the account at Bank B?"
"Who initiated the payment from Bank B?"

Scenario 2 (New Account)

- A customer reported to bank A that they had been a victim of a Crypto investment scam
- The customer testified that as part of the scam they were told by a bad actor that they needed to firstly open a wallet with a Crypto firm
- The bad actor offered to help open this account via remote access software to which the customer agreed
- The bad actor then advised that there was a need to open an account with a second bank (Bank B) as Bank A would not allow a payment to be made to the newly opened Crypto Wallet
- According to customer testimony the Bad Actor assisted in setting up the account which followed all relevant KYC and Anti impersonation checks
- The customer was then advised to send the money from Bank A to Bank B
- According to customer testimony the Bad actor then sent the money from Bank B to the new Crypto wallet before sending it onwards to an unknown destination
- After the fact, the customer was able to access and send screen shots showing the zero balance at both Bank B and the Crypto Wallet

Assessment of this case:

Have the relevant questions been asked? I.e. whilst the criminal assisted in opening both accounts, did both the customer and criminal have access, or did the criminal have full control of both the crypto account and the account with Bank B. Did the customer provide their consent for the payment from Bank B to be sent on their behalf to the crypto account? Does the customer providing consent for the criminal to make the payment on their behalf count as 'explicit consent' and therefore fall under the PSR's definition of an Authorised payment?

Source: UK Finance

Me2Me Payments

Case Studies

Key questions:
"Who initiated the payment from Bank B?"
Who has control of Bank C?"

Scenario 3 (Established Account)

- A customer reported being a victim of a Crypto investment scam to Bank A
- The customer testified that as part of the scam they were told by a bad actor that they needed to firstly open a wallet with a Crypto firm
- The bad actor offered to help open this account via remote access software to which the customer agreed
- The bad actor then advised that there was a need to open an account with a second bank (Bank B), as Bank A would not allow a payment to be made to the newly opened Crypto Wallet
- The customer advises that they already hold an account at Bank B who allow payments to Crypto wallets
- The customer was then advised to send the money from Bank A to Bank B
- The customer was then advised to send the money from Bank B to the Crypto Wallet (the funds hit a HOCA account at Bank C, before being credited to the crypto exchange)
- The customer testimony states that they did not have direct access to the crypto wallet and were only provided a link to a platform to show how their investments were performing

When applying the PSR definitions

The payment from bank A to B is out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer.

The payment from bank B to the crypto wallet is in scope of the reimbursement requirement with the regulated entity (Bank C) providing the payment facilities to the crypto firm liable for the loss. Bank C will need a contractual arrangement to recover the loss from the crypto firm.

Source: UK Finance

Me2Me Payments

Case Studies with PSR Clarification

Key questions:
"Where did the customer lose control of the funds?"
"Who provided the relevant receiving account?"

Scenario 4 (Customer driven me2me)

- A customer reported being a victim of a Purchase scam to Bank B
- The customer advises that they had tried to make the payment directly from Bank A however had been refused, as such they moved the money to Bank B first
- The customer then paid away from Bank B to the fraudsters account via a Faster Payment

When applying the PSR definitions

The payment from bank A to B is out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer. The payment from bank B is an authorised payment, made to an account not controlled by the consumer and is therefore in scope of the reimbursement requirement.

Scenario 5 (Impersonation / Safe Account scam)

Consumer received a call from what she thought was Bank B's fraud team. They asked her about a payment she hadn't made and the consumer was also able to see other payments that she did not recognise on her account. Scammer said all her accounts have been compromised. He stated those transactions were made internally by members of staff in her bank (A). She was then asked to make transfers to Bank C (where she also holds a pre-existing account) to secure the funds, from where the fraudsters moved the money.
Scam conversations were held, however customer was coached to lie.

When applying the PSR definitions

The payment from bank A to C is out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer. Bank A and B were part of the social engineering. The payment from account C is unauthorised. It is therefore the responsibility of the PSP holding account C to conduct the investigation and to potentially reimburse in full due to the unauthorised transactions.

Source: UK Finance

Me2Me Payme

Case Studies with PSR Clarifica

Key questions:
"Is the 'mule account' a relevant account and which PSP provides it?"
"Who authorised the payment from Bank C?"

Scenario 4 (Customer driven me2me)

- A customer reported being a victim of a Purchase scam to Bank B
- The customer advises that they had tried to make the payment directly from Bank A however had been refused, as such they moved the money to Bank B first
- The customer then paid away from Bank B to the fraudsters account via a Faster Payment

When applying the PSR definitions

The payment from bank A to B is out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer. The payment from bank B is an authorised payment, made to an account not controlled by the consumer and is therefore in scope of the reimbursement requirement.

Scenario 5 (Impersonation / Safe Account scam)

Consumer received a call from what she thought was Bank B's fraud team. They asked her about a payment she hadn't made and the consumer was also able to see other payments that she did not recognise on her account. Scammer said all her accounts have been compromised. He stated those transactions were made internally by members of staff in her bank (A). She was then asked to make transfers to Bank C (where she also holds a pre-existing account) to secure the funds, from where the fraudsters moved the money.
Scam conversations were held, however customer was coached to lie.

When applying the PSR definitions

The payment from bank A to C is out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer. Bank A and B were part of the social engineering. The payment from account C is unauthorised. It is therefore the responsibility of the PSP holding account C to conduct the investigation and to potentially reimburse in full due to the unauthorised transactions.

Source: UK Finance

Me2Me Payments

Case Studies with PSR Clarification

Key questions:
"Was the relevant account hat of the customer, a fraudster or the crypto exchange?"
"Did the victim have control of the receiving account?"

Scenario 6 (Advance Fee)

- Customer was approached on WhatsApp by someone claiming to be from Carers UK who were looking to offer him full time or part time positions in online jobs. He initially refused but was later contacted by someone informing him of this position where all he would need to do is complete 40 tasks online to optimise apps.
- He was told he would need to buy crypto currency from places such as okx and use this to invest it in the platform ninja promo where he would then complete tasks and receive the amount back with a bonus amount. He was told they preferred if he made payments from a X account and so the customer opened his own X account and started doing this.
- For the first five days everything was fine and he was receiving pay back from it however after then they started asking for higher amounts as the apps he was optimising were of higher value. At first this seemed fine, however the amount it was asking for was getting higher and higher each time and he tried to contact the customer support and the person who introduced him to it to try to withdraw before completing tasks but they all explained that you cannot withdraw until completing the task and so the customer believes he has been scammed.
- He has sent all the payments to his X account first to which he has explained he has already contacted them and spoke to them about this but his legal team have advised him to raise it with us also.
- **In summary**, the consumer holds an account with A, but was advised to open an account with X. He proceeded to transfer funds from A to X. Both accounts are controlled by the consumer. He then transferred funds from X to buy crypto currency and invested the funds in a specific platform.

When applying the PSR definitions

The payments from bank A to B are out of scope of the reimbursement requirement as both relevant accounts are controlled by the consumer. The payment from bank B to purchase crypto are also out of scope as the consumer has control at all stages. The fraud occurs within the crypto exchange and is then not covered by any current regulations.

Source: UK Finance