PSR Payment Systems Regulator

Guidance

Authorised push payment scams reimbursement requirement

Supporting the identification of APP scams and civil disputes

September 2024

Contents

1 Overview

This document is guidance to support Payment Service Providers (PSPs) in assessing whether an APP (authorised push payment) scam claim raised by a consumer is not reimbursable under the FPS and CHAPS reimbursement rules [1] because it is a private civil dispute. By private civil dispute we mean a dispute between a consumer and payee which is a private matter between them for resolution in the civil courts, rather than involving criminal fraud or dishonesty. This guidance applies to claims for payments made via Faster Payments and CHAPS.[2]

The guidance includes the factors that PSPs should consider when assessing whether a claim solely relates to a civil dispute and does not fall within the requirement to reimburse. It does not put any expectations on consumers.

Civil disputes and scams might look very similar, so each case must be considered in accordance with the facts available.

Overview of this guidance

1.1 In our June 2023 policy statement[3], we confirmed that claims which relate to a civil dispute would not be reimbursable under the reimbursement requirement.

1.2 Civil disputes can vary in nature but most often involve instances where:

- A consumer has paid a legitimate supplier(s)[4] for goods or services and has not received them and/or they are defective in some way, and
- There is no indication of an intent to defraud.

1.3 This guidance does not form part of Specific Direction 20 or Specific Direction 21 but it is intended to support PSPs' compliance with the legal requirements and FPS/CHAPS reimbursement rules. When assessing whether a PSP is compliant with Specific Direction 20 or Specific Direction 21 the PSR will consider each case on its individual merits, and as part of the assessment, will take into account the extent to which a PSP has (or can demonstrate that it has) had regard to this guidance.

1.4 This guidance sets out high-level factors that PSPs should consider when making a determination on whether a claim is a reimbursable APP scam or a civil dispute.

1 FPS reimbursement rules can be found here FPS-Reimbursement-Rules-Schedule-4-V2.0.pdf (wearepay.uk) and the CHAPS reimbursement rules can be found on the Bank's website CHAPS | Bank of England

2 PS24/5 CHAPS APP scams reimbursement requirement | Payment Systems Regulator (psr.org.uk)

3 PS23/3 Fighting authorised push payment fraud: a new reimbursement requirement (June 2023)

4 By supplier we aren't restricting the definition to a commercial supplier, but this could include any provider under any arrangement.

1.5 If a claim is misidentified as a reimbursable APP scam or a civil dispute this can have a significant impact on both the consumer and the alleged scammer(s). Therefore, PSPs should consider all the high-level factors when assessing a consumer's claim, to ensure the best assessment is made as to whether an APP scam has taken place.

Principles of assessment

1.6 In our June 2023 policy statement, we set out that we expect sending PSPs to take a proportionate approach to validating claims based on the relative complexity and value of the fraud. We do not expect them to undertake complex or resource-intensive investigations for simple APP fraud claims. The information for most cases should be gathered through the customer's initial claim.

1.7 We set out the core principles which we expect PSPs to use to guide their assessment of whether there is an APP scam claim. These are:

- All PSPs should consider each claim and payment on its own merits
- All PSPs should consider the circumstances leading up to the disputed payment(s)
- The sending PSP should consider all available relevant information when assessing a claim
- The sending PSP should make best efforts to gather relevant information in a timely manner
- The receiving PSP(s) should provide accurate and complete information where requested or material about the receiving account and the account holder.

1.8 Where a PSP believes the consumer's claim for reimbursement is a civil dispute, the onus is on the PSP to demonstrate why and to clearly communicate this to the consumer or their representative.[5] PSPs should also detail this within their internal records.

5 PSPs should consider their data protection obligations when sharing information with their consumer or their representative.

2 Distinguishing between an APP scam and civil dispute

This chapter sets out guidance to support PSPs in determining whether an APP scam claim is more likely to be a civil dispute rather than a reimbursable claim. The sending PSP may need to gather information from a range of sources, which could include information from the consumer raising the claim and information held by the receiving PSP(s).

2.1 In the legal instruments, which give effect to the reimbursement requirement,[6] we define an APP scam as:

'…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.*

For the avoidance of doubt, if the consumer is party to the fraud or dishonesty, this is not an APP scam for the purpose of the reimbursement requirement, or the reimbursement rules.'[7]

2.2 When assessing whether a claim relates to a civil dispute or reimbursable APP scam, the sending PSP should seek to determine on the facts whether:

- the recipient is not who the consumer intended to pay, or
- the payment is not for the purpose the consumer intended.

2.3 When considering the above, the sending PSP should consider if there is evidence to indicate:

- a dishonest or fraudulent act or course of conduct by the alleged scammer
- the consumer has been deceived or persuaded (as part of a fraudulent or dishonest act) about the recipient's identity or payment's true purpose
- the consumer has been manipulated by the alleged scammer, and/or
- there was intent to defraud by the alleged scammer.

2.4 PSPs should consider what the consumer understood or knew about the purpose of the payment(s) at the time they were made.

6 PSR APP scams publications

7 By this we mean where there is evidence the consumer was party to the fraud for example 1st party fraud

2.5 If the consumer has paid an unintended recipient, such as in an invoice intercept scam, and there is no evidence to suggest that the payment was accidently misdirected, and there is evidence of an intent to defraud, it is more than likely to indicate an APP scam has taken place.

2.6 If the consumer has paid who they intended (or has paid an account in their name but the account was outside of their control) and there is evidence that the following occurred, this is likely to indicate an APP scam has taken place because:

- the payment was not for the purpose they intended, and
- there is evidence of an intent to defraud.

2.7 In situations where the consumer has paid the intended recipient it may be more difficult for PSPs to distinguish between an APP scam and a civil dispute. PSPs should consider the wider facts of the claim and whether there was an intent to defraud.

2.8 In situations where it may appear that the consumer payment(s) met their intended purpose PSPs should still consider the wider facts of the claim and if there was an intent to defraud. For example, a consumer investing in cryptocurrency, and appearing to pay a cryptocurrency account in their own name, does not automatically mean this was a genuine investment. When determining whether the payment is an APP scam, a PSP should consider who had control of the account (as defined in our directions) and if there was any deception or intent to defraud.

Factors to consider

2.9 In some circumstances the PSP will easily be able to identify if a claim relates to a civil dispute but in others it may be more difficult. We have set out key factors that a PSP should consider when trying to determine if a claim relates to a civil dispute or reimbursable APP scam.

2.10 These factors are independent of one another and do not represent an exhaustive list. A claim does not have to meet all five factors to be considered a civil dispute or reimbursable APP scam.

2.11 These high-level factors are designed to apply to all scam typologies and to help PSPs determine if there was an intent to defraud as part of the alleged scam. By 'intent to defraud' we mean where the alleged scammer has acted knowingly and with specific intent to deceive the consumer as to the purpose for which the payment is sought, doing this for the purpose of making a gain for themselves or another. By 'alleged scammer' we mean the person who fraudulently or dishonestly causes the consumer to be manipulated, deceived, or persuaded into making an APP payment to the relevant account(s).

The high-level factors are categorised into five key areas:

1. The communication and relationship between the consumer and the alleged scammer
2. The trading status of the alleged scammer
3. The alleged scammer's capability to deliver any goods and services related to the claim
4. The extent to which the alleged scammer deceived the consumer as to the purpose of the payment
5. Information held by the receiving PSP(s) about the relevant account(s).

2.12 Where the alleged scammer is a private seller[8] or individual then the second high-level factor listed above may not always be applicable.

Communication and relationship between the consumer and the alleged scammer

2.13 As part of its assessment, a PSP should consider any evidence the consumer can provide of the relationship between the consumer and alleged scammer, including any communication between them. This could include the content of communications, as well as the means, frequency and duration of the communication.

2.14 We recognise that some APP scams will involve fraudsters who pose as private individuals where the scam occurs over an online marketplace. PSPs should consider the communication between the consumer and alleged scammer, such as adverts and the market price of the goods/services alongside the other factors to consider if a reimbursable APP scam has taken place.

2.15 In some circumstances a breakdown in relationship may lead to a scam claim being made. For example where the consumer knew the person they were paying and/or had paid the person previously and received goods/services they were satisfied with. In these situations, while this may suggest this would be a civil dispute, PSPs must consider every case on its own merits, and take care to consider all the information provided. PSPs should be mindful of the potential that the alleged scammer may have provided returns or services to further the consumer's confidence and extend the profitability of their crime.

The trading status of the alleged scammer

2.16 A PSP should consider if the trading status of the alleged scammer at the time of the payment(s) supports the view that there has been impersonation, intent to deceive or misrepresentation by the alleged scammer.

2.17 PSPs should consider information held on the Financial Services Register[9], and on Companies House[10] alongside any information provided by a third party. Companies House registration in isolation may not be enough to support a view that the company is trading legitimately. Other likely sources of information could include (but are not limited to) information held by the police, Trading Standards or a foreign regulator/government,

8 By private seller we mean where a person conducts a sale solely for their individual benefit and not for the purpose of conducting business.

9 FCA Register Home Page

10 Companies House

and open-source research (such as reviews on online marketplaces). For example, a warning on the FCA register which suggests the consumer has been contacted by a cloned investment firm would indicate that the claim is a reimbursable APP scam. PSPs should consider all information in the round when assessing a consumer's claim for reimbursement.

2.18 For peer-to-peer transactions, PSPs should consider consumer reviews to help establish the legitimacy of the private seller. However, PSPs must be aware that on-line reviews can be fabricated. Reviews must therefore be considered alongside other available evidence.

2.19 The PSP should consider the trading status of the alleged scammer at the time the payment(s) were made. In some cases where the trading status has changed since the consumer made the payment(s) this should also be considered as an indicator that points to an intent to defraud. For example, in a case where a company was authorised to trade at the time of the payment, but the authorisation was later removed, the PSP may want to consider if this is an indication of the company's overall intent.

The alleged scammer's capability to deliver any goods or services related to the claim

2.20 As part of the assessment, PSPs should consider the alleged scammer's capability to deliver the goods or services which are the subject of the payment. When making this assessment, PSPs should consider whether the alleged scammer's capability to deliver indicates there was an intent to defraud, rather than a legitimate commercial transaction that failed to work out as the consumer expected.

2.21 The communication and engagement between the consumer and the alleged scammer will be helpful to shed light on what happened. This could include (but is not limited to), other reports of scams made against the alleged scammer.

2.22 When making this assessment, a PSP should consider the extent to which the alleged scammer deceived the consumer as to the intended purpose of the payment. For example, where there is evidence that the consumer intended the payment to be used for a specific purpose, but the alleged scammer dishonestly intended to deceive the consumer into making the payment for the different purpose of making a gain for themselves.

2.23 Dishonesty on its own is not sufficient to consider a payment an APP scam. If the alleged scammer's dishonest actions do not impact the intended purpose of the payment, then an APP scam may not have taken place. For example, a newly established business could advertise that it is long established (despite being newly formed), but it is a genuine business and intended to provide the services and/or goods in return for the consumer's payment. In this situation, despite the misrepresentation, the alleged scammer did not deceive the consumer about the intended purpose of the payment and fulfilled that purpose. In the absence of other factors this could indicate a civil dispute.

2.24 In some APP scams, a nominal service may have been started or delivered to induce the consumer into believing the legitimacy of the goods or services being offered by the alleged scammer. PSPs should also consider any information provided about or by the alleged scammer after the payment(s) has been made, such as information about courier issues or supplier insolvency.

2.25 Non-receipt of goods or services does not on its own indicate that an APP scam has taken place. Where goods or services have been received or provided but in the consumer's

view are not as described, or are damaged or defective, or of poor quality, and there is no evidence of an intent to defraud (when considering all the other factors), then this is more likely to point to a civil dispute.

2.26 In some investment scams (such as Ponzi schemes) consumers are paid a 'return' on their investment, when in fact these returns are paid from funds from new 'investors'. If a consumer has received a return from an investment opportunity, a PSP shouldn't conclude that the claim is a civil dispute, instead it should consider this information alongside all the other factors to determine if a reimbursable APP scam has taken place.

2.27 In all circumstances, PSPs should consider all the available information in the round, including any evidence the alleged scammer(s) have provided to the receiving PSP.

Information held by the receiving PSP (s) about the relevant account(s)

2.28 We recognise that the receiving PSP(s) may also hold information about the relevant account and its holder that supports a sending PSP in assessing whether a claim relates to a civil dispute. We expect the receiving PSP(s) to share relevant information with the sending PSP. The receiving PSP may be limited in what actual evidence they can share due to data-sharing restrictions, but they can provide an indication as to the assessment they have conducted and how they arrived at their decision.

2.29 This information can be put into five broad categories, although this is not exhaustive:

- Account opening information
- Account history/usage
- Any markers on the account
- Any previous fraud claims
- Information gathered from their account holder or any other third parties.

Stop the clock

2.30 PSPs may stop the clock under one of the reasons set out in the Faster Payments reimbursement rules and Specific Requirement 1 to ask for information either from the receiving PSP or from third parties such as the police and Trading Standards. There should not be a delay to reimbursement under the policy if it is clear that a reimbursable APP scam has taken place then the consumer should be reimbursed. When considering whether to ask for relevant evidence from a third party, a PSP should consider what additional information might reasonably come from the third party, to inform its decision as to whether a scam has taken place.

Complex cases

2.31 The PSR recognises that certain cases may involve a complex set of factors, which will need to be carefully balanced. As set out in our compliance and monitoring policy statement[11] we will be engaging Pay.UK and industry on developing a detailed operational process for allocating and managing complex cases.

11 PS24/3 FPS APP scams reimbursement compliance and monitoring

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk