

Draft guidance

Authorised push payment scams reimbursement requirement

Supporting the identification of
APP scams and civil disputes

July 2024

Contents

1	Overview	3
2	Distinguishing between an APP scam and civil dispute	5

1 Overview

This document provides draft guidance to support Payment Service Providers (PSPs) in their assessment of whether an APP (authorised push payment) scam claim raised by a consumer is not reimbursable under the reimbursement requirement because it is a private civil dispute.¹ It applies to claims for payments made via Faster Payments and CHAPS.²

The guidance sets out factors that PSPs should consider when assessing, in the light of the facts available, whether a claim solely relates to a civil dispute and does not fall within the requirement to reimburse. This guidance is indicative only. Civil disputes and scams might look very similar, so each case must be considered in accordance with the facts available. The guidance does not specify evidentiary requirements. PSPs should continue to have regard to the best practice guide to support their assessment of a reimbursable APP scam.

Overview of guidance

- 1.1** In our June 2023 policy statement³, 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 or they are defective in some way
 - There is no indication of an intent to defraud on the part of the alleged scammer
- 1.3** This guidance does not form part of Specific Direction 20 or any future specific direction for APP scam payments using CHAPS⁵, but it is intended to support PSPs' compliance with the legal requirements. When assessing whether a PSP is compliant with Specific Direction 20 or any future direction for CHAPS, the PSR will apply this guidance flexibly, considering each case on its individual merits when taking into account the extent to which a PSP has had regard to this guidance.

1 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.

2 Pending outcome to our consultation [CP24/8: CHAPS APP scam reimbursement requirement](#)

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.

5 Pending outcome to our consultation [CP24/8: CHAPS APP scam reimbursement requirement](#)

Principles of assessment

- 1.4** In our June 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.
- 1.5** 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

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). Where there are clear indicators that a claim is a reimbursable APP scam, the sending PSP should assess the case as such.

Distinguishing between an APP scam and civil dispute

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.'

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
- there was intent to defraud by the alleged scammer

6 [PSR APP scams publications](#)

- 2.4** If the consumer has paid an unintended recipient and there is no evidence to suggest that the payment was accidentally misdirected, and there is evidence of an intent to defraud, it is more than likely to indicate an APP scam has taken place.
- 2.5** If the consumer has paid who they intended (or has paid an account in their name but it is clear that the account was outside of their control) and there is evidence of the below having occurred, this is likely to indicate an APP scam has taken place:
- the payment was not for the purpose they intended and
 - there is evidence of an intent to defraud
- 2.6** 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 therefore need to consider if there was an intent to defraud. For example, just because the consumer wanted to invest in crypto currency and paid a crypto currency wallet does not 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 and if there was any deception or intent to defraud.
- 2.7** To support in determining whether there was an intent to defraud, we set out some factors to consider in the next section. PSPs should consider any process that may be put in place for complex cases as set out in our compliance and monitoring policy statement.⁷

Factors to consider

- 2.8** 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.
- 2.9** These factors are independent of one another and do not represent an exhaustive list. A claim does not have to meet all four factors to be considered a civil dispute or reimbursable APP scam.
- 2.10** 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).

⁷ [PS24/3 Faster Payments APP scams reimbursement requirement: compliance and monitoring](#)

2.11 The high-level factors can be 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 the 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)

Communication and relationship between the consumer and the alleged scammer

2.12 As part of their 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.

2.13 PSPs should also consider if it is clear from the information provided if there has been a breakdown in relationship between the consumer and alleged scammer. This is especially relevant in cases 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 it is more likely that 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

2.14 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, relevant intent to deceive or misrepresentation by the alleged scammer.

2.15 PSPs should check and consider information held on the FCA register⁸, and by Companies House⁹ 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. All information must be considered in the round. Likely sources of information could include but are not limited to information held by the police, trading standards or a foreign regulator/government,) and open-source research. PSPs should consider any indicators that may suggest a claim is a reimbursable APP scam or relates to a civil dispute. For example, if there is a warning on the FCA register which suggests the consumer has been contacted by a cloned investment firm this would indicate that the claim is a reimbursable APP scam.

8 [Register Home Page \(fca.org.uk\)](https://register.fca.org.uk)

9 [Companies House – GOV.UK \(www.gov.uk\)](https://www.gov.uk)

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

- 2.16** As part of the assessment, PSPs should consider the alleged scammer's capability to deliver, including whether this points to an intent to defraud. By this we mean the likelihood of the alleged scammer being able to deliver the goods or services which are the subject of the payment. When making this assessment firms should consider whether the alleged scammers capability to deliver indicates there was an intent to defraud, as opposed to a legitimate commercial transaction that failed to work out as expected.
- 2.17** When completing their assessment PSPs should consider whether there was an attempt by the alleged scammer to deliver or provide the product or service. The communication and engagement between the consumer and the alleged scammer will be helpful to shed light on what happened. As part of this assessment PSPs should also consider whether there are other indicators of fraud, this could include but is not limited to, other reports of scams made against the supplier.
- 2.18** 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/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, then this is more likely to point to a civil dispute.
- 2.19** In all circumstances, PSPs should consider all the available information in the round, including any evidence supplier(s) have provided to the receiving PSP.
- 2.20** 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. When completing an assessment PSPs should take into all the other high-level factors, such as communication between the alleged scammer and the consumer.

The extent to which the alleged scammer deceived the consumer as to the intended purpose of the payment

- 2.21** 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.
- 2.22** Dishonesty on its own is not sufficient to consider a payment an APP scam. PSPs must be able to evidence that the alleged scammer's dishonest actions relate to the intended purpose of the payment. 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.

Receiving PSP evidence and evidence from other parties

- 2.23** 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 regarding the level of legitimacy of their customer.
- 2.24** While not an exhaustive list, we categorise this information into five broad categories:
- Account opening information
 - Account history/usage
 - Any markers on the account
 - Any previous fraud claims
 - Information gathered from their account holder
- 2.25** 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, and the consumer should be reimbursed within 35 days. 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.
- 2.26** 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 statement¹⁰ we will be engaging Pay.UK and industry on the development of a detailed operational process for the allocation and management of complex cases over the summer.

¹⁰ [PS24/3 FPS APP scams reimbursement compliance and monitoring](#)

PUB REF: CP24/10

© The Payment Systems Regulator Limited 2024

12 Endeavour Square

London E20 1JN

Telephone: 0300 456 3677

Website: www.psr.org.uk

All rights reserved