DRN-5968517

The complaint

Mr C has complained that Prepay Technologies Ltd won't refund money he lost to a job scam.

What happened

The details of the complaint are well known to both parties, so I will not repeat them again here. Instead, I will focus on giving the reasons for my decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I agree with the investigator's findings for broadly the same reasons, I will explain why.

In broad terms, the starting position in law is that an EMI is expected to process payments that their customer authorises them to make. It isn't disputed that Mr C authorised the payments from his account. Therefore, under the Payment Services Regulations and the terms of his account, PrePay is expected to process Mr C's requests, and he is presumed liable for the loss in the first instance.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in July 2025 that PrePay should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Having considered Mr C's transactions, I am satisfied that the payment he made on 5 July 2025 for £9,209 ought to have triggered PrePay's fraud detection symptoms. I say this

because it was also larger than any other payment that had debited the account and the fifth payment to have debited the account that day. It was an escalating payment of an increased value being a potential indicator of fraud. Therefore, in my view, there was enough about the characteristics of this transaction and the activity on Mr C's account that ought to have been concerning; such that PrePay should have intervened at that time to indicate he could be at risk of fraud. So, I am satisfied that it is fair and reasonable to conclude that PrePay should have warned its customer before this payment went ahead.

So, with that in mind, I have gone on to consider what I think would have been a proportionate intervention given the risk the payment presented. The FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers. As such, firms have developed warnings to recognise both the importance of identifying the specific scam risks in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, by July 2025 when these payments took place, PrePay should have had systems in place to identify, as far as possible, the actual scam that might be taking place for example by asking a series of automated questions designed to narrow down the type of scam risk associated with the payment he was making – PreyPay have provided a scam warning tailored to the likely scam Mr C was at risk from. I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance.

I can see that PrePay did provide Mr C with a written warning, however, due to Mr C providing the incorrect payment purpose "paying family and friends" when in fact he was paying for a job opportunity, meant that that the warning provided was tailored to the payment purpose provided, which wouldn't have resonated with Mr C. PePay can't be held responsible for this, as it relies on the information provided. In any event, I am not satisfied this amounted to an automated warning. As I have highlighted above, an automated warnings rely on the consumers being asked a series of questions and this wasn't the case in this instance. Despite that, I don't think it would have made a difference if PrePay would have provided an automated warning. I say this because I am aware that a third- party institution did in fact provide an automated warning but due to the heavy coaching by the scammer, Mr C didn't provide accurate answers. As such, I am satisfied, on balance, it's likely Mr C would have taken the same approach here.

I appreciate that Mr C's representative doesn't agree and has stated that human intervention ought to have been considered, I disagree. The representative has said that PrePay ought to have recognised that the account the money was sent to (in the consumers own name, which I will refer to as C) was common in cryptocurrency scams. While that may be the case, C also offers a variety of other services, as the representative has acknowledged. As such there was nothing to indicate to PrePay at the time this was a transaction intended for Cryptocurrency. However, this also supported by the fact that when Mr C was asked for the purpose of payment he stated, "friends and family". Secondly, I am aware that when a third party institution did contact via human intervention and highlighted, he was falling victim of a scam, it didn't prevent Mr C's losses, he simply found an alternative method to make the payment. Mr C has told our service that "*I was under intense pressure and effectively coached by the scammers on how to explain the payments to bypass security".* Therefore, having considered this and the action Mr C took I am satisfied PrePay wouldn't have prevented Mr C's losses.

I've also looked at whether PrePay took the steps it should have once M C contacted them to dispute the payments. It's important to note that Mr C didn't ask PrePay to send the money directly to the scammer but instead to an account in his own name under his control. PrePay did as Mr C requested. So, it was always highly unlikely that PrePay would be able to facilitate the recovery of the payment after they were moved on from Mr C's wallet to the scammers. So, it follows that I won't be asking PrePay to do anything further.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 9 April 2026.

Jade Rowe
Ombudsman