DRN-6272550

The complaint

Miss J complains that Prepay Technologies Ltd ("Prepay Technologies") won't refund the money she lost to a scam.

Miss J opened an account with Monese. Monese acts as an agent of Prepay Technologies Ltd. I'll generally refer to Miss J and Prepay Technologies in this decision.

What happened

In summary, Miss J says she received a call from someone claiming to be from her personal bank's ("Bank L") fraud team. She later discovered the caller was a scammer.

Miss J says the scammer convinced her that her Bank L account had been compromised and that she needed to move her money urgently to keep it safe. Believing the caller was genuine, she shared security information and transferred her funds into a newly opened account with Prepay Technologies. She says the subsequent transfers from her Prepay Technologies account, to her own account with a legitimate crypto-platform ("C"), were unauthorised. And that Prepay Technologies should refund the losses resulting from the payments from C to the scammer's wallet. The payments in dispute are listed below.

Date	Method	Payee	Amount
13-Apr-25	Transfer in app	Miss J's account with C	£1,102
14-Apr-25	Transfer in app	Miss J's account with C	£3,446

Miss J says she realised she had been scammed on 14 April 2025, when she noticed the two payments that had been made from her account. Prepay Technologies declined her claim, so she raised a complaint which was referred to our Service.

Our Investigator didn't uphold the complaint. She thought the disputed payments were authorised. She wasn't persuaded by Miss J's later suggestions that her phone had been hacked or that the payments had been made by the scammer using remote access. The Investigator also noted Prepay Technologies had taken steps to identify the possibility of fraud before the payments were made and that those steps were proportionate. She didn't think Prepay Technologies needed to refund Miss J's losses in the circumstances.

Provisional decision

I issued my provisional decision explaining why I didn't intend to uphold this complaint and provided the following reasons**.**

Under the Payment Services Regulations 2017 (PSRs), the starting point is that Miss J is responsible for payments she authorised. With limited exceptions, Prepay Technologies is liable for unauthorised ones. A payment will usually be considered authorised if the customer made it themselves, but it can also be treated as authorised if they allowed someone else to make it on their behalf or they instructed their payment service provider to proceed.

In this case, Prepay Technologies has shown that the transfers were made in-app on Miss J's device and verified using one-time passcodes. There isn't enough evidence to conclude that her phone was "hacked". And Miss J no longer disputes that she made the payments from her device in any event. She has instead explained that the scammer "was able to view [her] screen and guide her through each step in real time" and that she "would not have made the transactions under normal circumstances". While Miss J may have been tricked and guided by a convincing scammer, I'm satisfied the payments were authorised because it's clear she completed the steps required to make them herself. It's important to note that consent under the PSRs is not the same as "informed consent". A payer's consent to the transaction itself doesn't depend on the wider context being fully explained to them.

In terms of prevention, Prepay Technologies is generally expected to process payments and withdrawals that a customer authorises. While there are circumstances in which I would expect it to make additional checks before processing a payment, I can't overlook that Miss J's account of events has not been consistent – to the point I'm not convinced she was the victim of the type of scam she has described. For example, it was only after the Investigator issued their outcome – highlighting the transfers were carried out on a device only Miss J had access to – that she revised her account and said the scammer had asked her to install "security or verification software". It was also after the Investigator pointed out that C had provided evidence showing that account had been opened by Miss J on 5 April 2025, days before she says the scam calls took place, that she then said she had opened that account.

In any event, I note that Prepay Technologies did take some steps to look into the disputed payments before they were made. When asked about the purpose of the transfers, Miss J selected "Paying yourself or someone you know". She was then shown automated warnings relevant to that payment purpose, but these did not stop her from continuing. And given she believed she was speaking to Bank L's fraud team, and her description of the level of control the scammer had over her actions in real time, I'm not persuaded that the scam would have been prevented even if I were to say Prepay Technologies should have taken more steps.

As for recovery, I'm satisfied there was little more Prepay Technologies could have done. The transfers were sent to Miss J's own account with C, and by the time the matter was reported, the funds – apart from £13.84, which was returned to her – had already been moved on and lost to the scam. So while I'm mindful of what Miss J has shared with us about her health and personal circumstances, and I'm sorry for the way she lost her money, I'm not persuaded the payments were unauthorised or that Prepay Technologies is otherwise required to refund them.

Responses to provisional decision

I invited further comments and evidence from both parties. I explained that unless any new information changed my view, my final decision was likely to be in line with my provisional conclusions. Miss J asked me to reconsider. In summary, she said that although she made the transactions, they were not made with genuine consent. She explained she was acting under the direction of a fraudster and believed she was taking steps to protect her funds.

She said the issue was not simply whether the payments were technically authorised, but whether the firm did enough to identify and prevent the fraud. The payments were unusual for her account and made to a crypto-platform. Although automated warnings were shown, she felt these were generic and ineffective given she believed she was speaking to her bank's fraud team and was acting under significant psychological pressure and fear. She said this impaired her ability to question what was happening. While she accepted there were differences in how she initially described events, she said this was common in scam cases and that her later explanations clarified her understanding of what had happened.

.**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've reached the same conclusion as in my provisional decision which is copied above and forms part of this final decision.

I'm satisfied the payments were authorised. Miss J accepts she made the payments and completed the necessary steps herself. Although she may have been tricked into doing so, consent under the PSRs doesn't require "informed consent". It relates to consent to the payment itself, not to whether the wider context was fully understood by the payer.

As for prevention, I explained that while there are situations in which a firm is expected to carry out additional checks before processing a payment, Prepay Technologies did take some preventative steps here. Miss J selected "Paying yourself or someone you know" as the reason for the transfers and was shown automated warnings relevant to that choice. Given the inconsistencies in her account of events, and that I remain unconvinced she was the victim of the type of scam she has described, it's also difficult to determine what form of scam warning would realistically have been effective in preventing her losses.

Even taking Miss J's testimony at face value, and considering the account activity and the payment amounts, I wouldn't have expected Prepay Technologies to go beyond providing automated warnings. And given what Miss J has repeatedly told us about the scammer's level of influence and close real-time control exercised over her actions, I'm not persuaded that proportionate steps on its part would have been likely to prevent her losses.

So, while I'm again sorry Miss J lost her money and understand she wants to do all she can to recover it, I don't consider Prepay Technologies could reasonably have prevented what happened, such that it should be held responsible for her losses in the circumstances.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss J to accept or reject my decision before 6 May 2026.

Thomas Cardia
Ombudsman