DRN-6269406

## The complaint

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

She held an account with Monese Ltd. Monese Ltd is an agent of Prepay Technologies. For simplicity, I'll generally refer to Miss B and Prepay Technologies throughout this decision.

## What happened

In summary, Miss B explained that she had listed an item for sale on an online marketplace ("D"). She was then contacted by someone she believed was a legitimate buyer. They claimed they couldn't clearly see the images on the platform, so the conversation moved to a messaging app. Miss B later discovered she had connected with a scammer.

Miss B says she was told that, as a first-time seller, she had to complete a "card verification process". She was sent a link for what looked like D's secure payment portal, but in reality it was a cloned site. A pop-up then appeared instructing her to follow the directions given by D's "support chat". Believing this was part of a routine process and that she was complying with verification requirements, Miss B funded her card account and provided her card details.

Immediately afterwards, she realised money had been taken from her card. When Miss B queried this, given she had initially been told her card was being verified and wouldn't be charged, she was instead asked to make another deposit, supposedly guaranteed to be returned along with a small compensation amount. Miss B says she realised this was a scam and that her card details had in fact been used to initiate a payment with a cryptocurrency merchant ("M") which she didn't recognise. She reported what had happened to Prepay Technologies but it declined to provide refund and to pursue a chargeback claim.

A complaint was referred to our Service. Our Investigator considered it but didn't uphold it. In short, he concluded Prepay Technologies could treat the payment as authorised as it had shown that Miss B had approved it in app. He didn't think the payment would have stood out as unusual such that Prepay Technologies should have intervened. He also concluded there was little that Prepay Technologies could have done in terms of recovery. As the complaint couldn't be resolved informally, it's been passed to me to decide.

## Provisional decision

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

*Can Prepay Technologies fairly treat the payment as authorised?*

*The starting point – under the Payment Services Regulations 2017 (PSRs) – is that Miss B is liable for payments she authorised. With some exceptions, Prepay Technologies is liable for unauthorised ones. A payment is normally considered authorised when the customer makes it themselves. But it can also be treated as authorised if a customer allows someone else to make it on their behalf or if they tell their payment service provider they want it to proceed.*

*In this case, Miss B has consistently explained that she funded her Prepay Technologies account and entered her card details because she believed she was completing a legitimate "verification process". Her communications with the fake "support agent" and the scammer posing as a buyer, generally support her testimony that she did not understand these steps to involve money being taken from her account. Based on the evidence, I think it is likely that a scammer, not Miss B, initiated the card payment on M's site using the card information she had provided on what appeared as D's platform – meaning that Miss B didn't complete all the steps required to make the payment. And, on balance, I'm persuaded Miss B did not intend, nor believe she was consenting to, a payment from her account.*

*Prepay Technologies has however provided its technical evidence to show that the payment was approved in-app through strong customer authentication (also known as 3DS). In her more recent submissions Miss B seems to accept she approved the payment. I've also seen, in the messages she exchanged in the "support chat", that she was primed to expect and "confirm" a "push notification" she would receive in her banking app. I appreciate Miss B was deceived about the wider context when she did so and I don't imagine she would have gone along with any of it, if she thought she would lose her money in the way she did.*

*But it still matters that the payment was approved by Miss B in-app. The approval screen asked "Do you want to approve this online payment?". It also displayed key information, including the merchant and the amount, and offered clear options either to approve or decline. As Prepay Technologies clearly asked Miss B whether she wanted the payment to proceed, and that the prompt was unambiguous, I think it was reasonable for Prepay Technologies to rely on the steps Miss B took as a representation of her confirming she consented to the payment, such that it is fair for it to treat the payment as authorised.*

*Could Prepay Technologies have done more to prevent the scam*

*In general, the starting point at law is that Prepay Technologies is expected to process payments and withdrawals that a customer authorises it to make. However, taking account of relevant law, regulatory rules and guidance, industry codes of practice, and what I consider to have been good industry practice at the time, it should also have taken additional steps or made additional checks, before processing a payment in some circumstances.*

*The payment in question was a single card transaction of around £343. While I appreciate that Miss B considers this a significant amount, firms must balance identifying potential scam payments with avoiding unnecessary disruption to legitimate transactions. Considering the account activity and that the payment amount would not have appeared as particularly concerning in value, I'm not persuaded that Prepay Technologies should have identified Miss B as being at heightened risk of fraud or intervened at that stage. The merchant (M) is legitimate, and the transaction was again authenticated using 3DS. Although payments to this type of merchant can carry a higher fraud risk, I don't consider that the circumstances here required Prepay Technologies to carry out additional checks.*

*Recovery*

*Prepay Technologies couldn't have stopped the payment from leaving Miss B's account once she had approved it. Because the transaction was a card payment, the only potential recovery option available to Prepay Technologies was the chargeback scheme. But as the Investigator explained, Prepay Technologies wouldn't be expected to raise a chargeback claim if it believed the claim had no realistic prospect of success.*

*Here a chargeback on fraud grounds was unlikely to succeed because the payment had been approved using 3DS. And since the payment was made to a legitimate merchant, it's also unlikely that a claim would have succeeded as the merchant provided the goods or*

*services, albeit to a scammer. Prepay Technologies has shown that it did submit a claim to the merchant, but the merchant declined it. Given this, and because Prepay Technologies would not be expected to pursue a claim with no realistic chance of success, I don't consider it a failing that it did not pursue a chargeback further in the circumstances.*

**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. Prepay Technologies accepted the provisional decision.

Miss B asked me to reconsider. In summary, she said that the payment was not genuinely authorised, as supported by her evidence. She also said that a proportionate intervention by Prepay Technologies would have prevented her losses in any event, and that she reported the scam promptly once she realised 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 conclusions as in my provisional decision, which is copied above and forms part of this final decision.

I recognise Miss B acted under the influence of a convincing scam. I agree her evidence shows she believed she was taking routine steps to verify her account so she could receive payment. I don't doubt her testimony that she didn't intend to make a payment.

However, it remains significant that the payment was approved by her in-app through strong customer authentication. And because the 3DS screens were clear as to their purpose, it was reasonable for Prepay Technologies to treat the steps Miss B took as a representation of her consent and to treat the payment as authorised, irrespective of the broader context.

I'm still not persuaded there was enough about the transaction, the activity, or the merchant, to conclude that Prepay Technologies was at fault for not intervening. I'm aware that value isn't the only relevant factor, but it's an important one. There was no significant fraud pattern, the payment was to a legitimate merchant, and many payments involving cryptocurrency are entirely genuine. As before, while Miss B acted quickly once she became aware of what had happened, there was no realistic prospect of Prepay Technologies recovering her money.

I'm again sorry that Miss B was scammed and I understand why she wants to do all she can to recover her money. However, for the reasons I've explained, I do not think it would be fair to hold Prepay Technologies liable for her losses in these circumstances.

**My final decision**

For the reasons given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 5 May 2026.

Thomas Cardia
**Ombudsman**