DRN-4391299

The complaint

A company, which I'll refer to as T, complains that PrePay Technologies Limited (PrePay) won't refund unauthorised transactions taken from its account.

Mr S, who is a director of T, brings this complaint on T's behalf.

What happened

In early 2023, Mr S received a call from someone claiming to be from PrePay. They asked him about a request he had recently initiated for a new card. When he confirmed he still needed one, they sent him a follow-up message via WhatsApp.

Mr S was asked to confirm some details, and to share a code he was sent, on the understanding this was necessary to verify him and action the request. However, it seems the caller was actually a scammer who had hacked Mr S's emails. Through this, and the information he shared, the scammer was able to access T's account and send two payments of £2,000 and £600 respectively.

When Mr S raised this issue with PrePay, it offered to refund half of the loss. It acknowledged his frustrations with the process for reporting fraud and said it was working to improve this. Mr S didn't accept this offer and referred the complaint to our service.

Our investigator upheld the complaint as they thought PrePay was liable for the payments in line with the Payment Services Regulations 2017 (PSRs). They were satisfied the payments were unauthorised – and weren't attributable to an intentional, or grossly negligent, failing by Mr S to keep T's security details safe.

PrePay has appealed the investigator's outcome. It says Mr S put T's security details at risk through gross negligent because:

- It doesn't contact customers via WhatsApp, so Mr S should have realised this was suspicious. When he had previously sought support, it had communicated via email;
- The WhatsApp messages don't show as coming from PrePay; they show as coming from a mobile number, and the sender doesn't otherwise identify themselves as PrePay. Yet Mr S trusted them and followed their instructions;
- The device used to make the payments was added via an email sent to T's registered email address, suggesting Mr S either shared this or his emails were compromised. And when he first contacted it about the fraud, he said his emails were secure;
- Mr S shared the last four digits of his card, without which the scammer wouldn't have been able to get control of T's account;
- He also shared a One Time Passcode (OTP) used to add the new payee to the account. The message made it clear this was to add a payee, not for verification; and
- Mr S should have been aware not to share the information he did as this is made clear from PrePay's website, mobile application, customer service and terms and conditions. He was grossly negligent in not reading this material carefully.

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 decided to uphold it. I'll explain why.

It seems PrePay accepts the payments were unauthorised. But it argues it isn't liable under the PSRs as Mr S's gross negligence allowed the fraud to occur.

I've carefully considered the reasons it has given for this. There is a reasonable case for concluding Mr S was perhaps negligent in sharing some of the security details used to make these transactions. But I'm not persuaded PrePay has shown his actions met the high bar of being *grossly* negligent. This is because:

- Mr S has consistently maintained that, at the time of getting the messages, the sender showed as having a PrePay logo. While that's not captured in his screenshots, it's plausible this is because the number was abandoned by the scammer following the scam.
- The messages also followed a call from someone claiming to be PrePay who knew about Mr S's recent card request. In that context, I can see why Mr S believed he was genuinely speaking to PrePay – the messages weren't unexpected, and the scammer was seemingly utilising knowledge about T's account.
- While PrePay doesn't use WhatsApp to contact customers, I don't consider it so implausible it might do. Other companies do use WhatsApp for official communication. The messages were reasonably professional in tone. Following on as they did from the earlier call, I understand why Mr S trusted the sender.
- I think it's likely the scammer did have access to Mr S's emails and used this to get access to T's account. This is because Mr S has consistently maintained he didn't use the QR code sent via email to verify the new device. While he originally said his email was secure, I think this is likely because he simply didn't realise the scammer had accessed his emails at that point.
- Mr S did share the last four digits of his card, which (along with the email link) allowed the scammer access to the account. But I accept he did this in the belief PrePay needed this to verify himself and order a new card. I don't think he foresaw the risk this would put his account at risk; it wasn't obvious to him this could be used to access his account, as he didn't know his emails had been hacked. And he didn't realise he was actually speaking to a scammer rather than PrePay.
- He also shared the OTP code used to verify the new payee. But in the overall context, I'm not persuaded he was very significantly careless in doing so. He did miss that the message said it was for "new payee verification". But he had been primed to expect a code for verification. So I think it's understandable, and not grossly negligent, that he missed the reference to this being for a new payee.
- I also don't think it's grossly negligent that Mr S may not have read, or had forgotten, all the information PrePay has published over various formats which it thinks made it obvious this was a fraud attempt. In the context, bearing in mind the access the scammer seemingly had to Mr S's emails, and the knowledge they had about T's account, I don't think he showed serious disregard to an obvious risk. I think the details he shared were understandably provided on the basis he was speaking to T's genuine account provider, and that the information was necessary to verify himself and request a new card.

I therefore think PrePay is liable for the unauthorised transactions taken. So it should refund T, and pay 8% simple interest per year on the refund amount to compensate T for the loss of use of the funds.

Regarding the issues Mr S has raised about PrePay's service and fraud reporting process – as I've already notified him, I'm not persuaded the impact on T warrants compensation beyond refunding the loss with interest. And I can't award for his personal distress and inconvenience. So I'm not awarding the additional £100 compensation suggested by the investigator.

My final decision

For the reasons given above, I uphold this complaint and direct PrePay Technologies Limited to:

- Refund T for the unauthorised transactions, less any amount recovered or already refunded; and
- Pay 8% simple interest per year on this amount, running from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

PrePay Technologies Limited must pay this compensation within 28 days of the date on which we tell it T accepts my final decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 27 December 2023.

Rachel Loughlin
Ombudsman