DRN-4506552

The complaint

Mr U complains that PrePay Technologies Limited, trading as PrePay Solutions didn't refund him for disputed payments from his account.

What happened

Around July 2022, Mr U says his device was stolen and used by a third-party to carry out several payments. Mr U complained to PrePay after it refused to refund him for these payments.

In its response, PrePay said that the payments had been made using the mobile payment feature on Mr U's device, which would've required a PIN or biometric verification. Moreover, the business points to the fact that Mr U's online banking app was logged in to using his passcode. PrePay thinks only Mr U could've carried out such activity so it decided that the payments were authorised.

Remaining unhappy, Mr U asked this service to get involved.

As part of its submissions to this service, PrePay says:

- The payments were made using Mr U's device via its mobile payment service – these were authenticated using a PIN or biometric I.D
- Mr U's banking app was logged into and that this would've required knowledge of his passcode. Two transfers of £100 each were made from Mr U's savings account to his main account and Mr U's statements were generated around the time – PrePay points to this as not being typical of actions carried out by a potential fraudster.
- Mr U is liable if he's shared passwords with a third-party. He's also made payments to the relevant merchants before.
- That attempted payments stopped after Mr U blocked his debit card. PrePay finds this to be unusual. The business says it would've expected at least a few failed transactions following the block, as the third-party wouldn't have known about it.

Although Mr U's testimony has been inconsistent is some aspects, he told us that:

- His mobile device was stolen by a third-party while he was distracted by an incident that he wasn't involved in. He says he unlocked his device at the time because the third-party had asked to use it.
- He thinks the third-party saw him enter his mobile device password when he unlocked it.
- He initially told PrePay that he thinks the third-party reset his mobile banking passcode by using the access they had to his email account on his device. Mr U later explained that his banking app passcode and the password to unlock his mobile device consisted of the same sequence of numbers – so he suggests that the third-party was able to work out his banking app passcode, given they had seen him enter it into his device.
- He reported the theft to the police, his mobile service provider and contacted some of the relevant merchants.

Our investigator decided that PrePay should refund the disputed payments to Mr U. The investigator was persuaded by Mr U's testimony and wasn't satisfied that the business had demonstrated how the disputed payments had been authenticated.

PrePay doesn't agree. It says the final disputed payment was carried out after only some of Mr U's savings were transferred into his main account. The business thinks it's unusual that a potential fraudster would leave funds behind. PrePay also finds it unusual that the third-party mostly carried out low value payments and only completed a large payment towards the end. The business also questions why the third-party didn't attempt to use Mr U's card details for online payments – PrePay notes that an attempt was made to do so on a cryptocurrency website, but the business doesn't allow purchases related to cryptocurrency.

Our investigator stood by their view on the complaint. Because PrePay doesn't agree, the complaint has been passed to me to make a final 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.

I'm upholding this complaint – I'll explain why.

PrePay can generally only hold Mr U responsible for the disputed payments if the evidence suggests it was more likely than not that Mr U authorised them. Based on the limited evidence PrePay has provided, I can't fairly conclude that Mr U authorised these payments.

PrePay has put forward numerous arguments to explain why it thinks Mr U authorised the disputed payments. It also questioned parts of Mr U's testimony. But PrePay hasn't submitted actual evidence that would persuade me that Mr U most likely authorised these payments.

PrePay says the payments were authenticated via the mobile payment service on Mr U's device. The business says the payments would've required Mr U's device password or biometric I.D. But we haven't been provided with any audit records to show how each payment was authenticated and which device was used. PrePay also says Mr U's mobile banking app was logged in to around the time and activities including the transfer of funds was carried out. Again, PrePay has failed to provide any records showing how the app was logged in to and from which device.

And although PrePay suggests Mr U may have shared his passcode, I've seen no evidence that he did, either deliberately or negligently. Mr U's explanation of how his device was stolen doesn't sound implausible to me and his actions that followed are in line with what I'd reasonably expect in such circumstances – he reported the theft to the police, his mobile service provider and later seems to have set up access to mobile banking via a different device. And his mobile service provider confirmed his SIM and device were blocked after he reported the theft. I think it's unlikely that Mr U would take such steps if the disputed payments were authorised by him.

Mr U can be held liable for payments he didn't authorise if he's failed with gross negligence to comply with his obligations as a payment service user – and this has allowed the disputed payments to take place. Under the Payment Service Regulations 2009 and 2017, Mr U is required to notify PrePay without undue delay if his debit card information is lost or stolen. He's also required to take reasonable steps to keep his security credentials safe.

I can see that Mr U reported the disputed payments to PrePay that same day, so I'm

satisfied he did so without undue delay. It's unclear exactly how the third-party obtained his password. Mr U has explained that his device password (that the third-party likely saw him enter) and his mobile banking passcode consisted of the same sequence of numbers. So I think this is a plausible explanation as to how the third-party was able to use Mr U's device for the disputed payments and to access his mobile baking account. So I don't think he was grossly negligent.

The onus, in my opinion, is on PrePay to persuade me that Mr U authorised the disputed payments. Given it hasn't been able to, I can only fairly conclude that Mr U didn't authorise the payments he's disputing.

PrePay points to transfers made from Mr U's savings account into his main account around the time. It says funds were left in Mr U's savings account and that it seems unusual that a potential fraudster would leave funds behind. PrePay also says it's unusual that the attempted payments stopped as soon as Mr U blocked his debit card, even though the third-party wouldn't have known that the card had been blocked.

I can't offer a definitive explanation to these points, but I can, based on the information I've seen, explain what I think is the likely explanation to what PrePay says.

Looking at the transaction history PrePay provided, I can see the first batch of funds that were transferred from Mr U's savings account were preceded by two failed debit card payments. These payments likely failed due to a lack of funds in Mr U's account at the time, given the attempt at making the same payment was successful following the initial £100 transfer. It's likely then that the third-party transferred enough for that particular transaction to complete successfully – and then transferred a further £100, possibly to ensure there were available funds for further payments.

Mr U says he managed to regain access to mobile banking shortly after this second transfer and, having noticed there were funds in the account, he transferred what remained into a family member's account. I find this to be plausible – looking at the data PrePay sent, it seems Mr U reauthenticated his access to the mobile banking app, which included submitting a selfie during the morning that immediately followed the disputed payments. It seems to me that, after Mr U managed to gain access to the app, he likely used this opportunity to prevent further funds being used for unauthorised payments.

It's unclear why statements were generated using the mobile banking app during the period the disputed payments took place. Mr U hasn't said that he carried out this activity. So it's likely something that the third-party did. I do accept PrePay's comment on this as it does seem like something unusual for a potential fraudster to carry out. However, although I cannot see a reasonable explanation as to why the third-party would've used Mr U's mobile banking in such a way, I've seen nothing that makes make think it was Mr U that generated the statements – nor have I seen anything that suggests it was most likely him that carried out the disputed payments.

PrePay also questions how the third-party would've known to stop attempting payments as Mr U had blocked his debit card. But I don't find this to be a plausible argument for why the business thinks Mr U authorised the disputed payments. Looking at the transactions, the final disputed payment took place around 9:00am that day and, based on what the business says, it wasn't until over two hours later that Mr U blocked his card. No payments appear to have been attempted during the period in between.

So I don't agree that the payment attempts by the third-party stopped solely because Mr U blocked his card. It seems to me that the payments stopped well before the block was placed. Although it's unclear exactly why the payment attempts ceased, I'm satisfied that this

issue doesn't give me cause to think that Mr U likely authorised the disputed payments.

PrePay also points to the content and value of the payments that took place after Mr U says his device was stolen. The business points to payments on the night of 30 June 2022 that Mr U initially disputed, paid to a friend of his. Initially, Mr U submitted that the third-party transferred funds to this individual in order to use their debit card. I do agree that such activity sounds implausible. But Mr U has since said that his friend returned these payments, so he no longer disputes these.

PrePay flagged that the third-party never attempted to use Mr U's card details for online purchases. It also submits that the disputed payments were generally for low values, until one of the latter payments which was for around £700. So PrePay questions why a potential fraudster wouldn't try to maximise use of Mr U's card details as quickly as possible.

However, the transaction audit PrePay recently provided suggests otherwise. I can see that to start with, multiple attempted payments were made to a cryptocurrency website, each with a value ranging between £150 - £250. These payments likely failed because PrePay doesn't allow the use of its accounts for cryptocurrency related purchases. So I disagree with PrePay's assessment of what happened at the time and remain of the opinion that the disputed payment were most likely unauthorised.

So, for these reasons, I'm of the view that it's unlikely Mr U authorised the disputed payments. Therefore, I think PrePay acted unfairly by deciding these payments were authorised, so it needs to put things right.

Putting things right

PrePay acted unfairly when it decided Mr U was responsible for the payments he disputes. To put things right, PrePay should refund the disputed payments to Mr U and pay him 8% simple interest per year – payable from the date the payments were debited to the date of settlement.

If PrePay considers that it's required by HM Revenue & Customs to deduct tax from that simple interest, it should tell Mr U how much tax it has taken off. PrePay should also give Mr U a tax deduction certificate if he asks for one.

My final decision

For the reasons above, I'm upholding this complaint. PrePay Technologies Limited should settle this complaint in line with what I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr U to accept or reject my decision before 1 March 2024.

Abdul Ali
Ombudsman