DRN-4531079

## The complaint

A company which I will refer to as 'T' complains that Advanced Payments Solutions Limited (trading as Cashplus) allowed payments out of their account which were not authorised by them. They say that the payments were unusual to the normal account activity and the bank failed to prevent them. They are also unhappy with the way Cashplus dealt with the matter after being advised of the fraud.

## What happened

In June 2022, the director of T, who I will refer to as 'S', was contacted by a fraudster pretending to be a staff member of Cashplus. S said that he was busy at that time and asked the caller to call back later.

Later that evening, S received a text message purportedly from Cashplus advising him that his request to change his phone number on T's accounts had been received, and an adviser would contact him shortly. S attempted to message back to say that he hadn't requested this, but the message failed to be delivered.

The fraudster then rang S. S says that the call appeared to come from Cashplus and so he had no reason to doubt the authenticity of the call. The caller explained that there were fraudulent attempts to purchase goods on S's cards, but these had been flagged as suspicious and blocked by Cashplus. The caller said that this happened because someone had changed the mobile number connected to T's bank accounts and then attempted to make these payments. The caller (pretending to be from Cashplus) offered to remove that number and reinstate S's number back on to the account.

The caller said that S would shortly receive an email which he shouldn't act upon as it would be from the fraudster. He was advised to forward that email to an email address the caller gave. S did as he was advised.

Within minutes S was sent a (genuine) text message by Cashplus, which provided a passcode. The message asked S not to share the passcode with anyone and stated that the code should only be entered on-screen when prompted. S says he did not see this text message and as such did not give out any passcode to the caller.

Shortly afterwards S received a genuine email from Cashplus stating that he had just logged in to the Cashplus app using a new device (an iPhone 6s). The email said that he should call Cashplus immediately if he didn't recognise this login. S's phone was not an iPhone 6s but it appears that he took no action following this email.

Company T had two accounts with Cashplus. The above process was repeated in relation to the second account.

S says that he was then told to tap the links provided in two text messages he was sent. He says that the caller claimed that this would de-register the fraudster's mobile and reinstate

his. These texts appear to have come from the fraudster. However, S isn't able to produce a copy of these texts. He says that they were somehow deleted by the fraudster afterwards.

S says the call ended shortly after he tapped the links in the two texts. The next morning S was unable to make a payment through the cards linked to T's accounts. He also couldn't log into the app on his phone. He contacted Cashplus and he was advised that there were insufficient funds available in T's accounts. That was when the fraud came to light.

It appears that unknown to S, the caller had removed his device from the two accounts and registered their phone, through which they had access to T's accounts. They had then made two payments: £7,350 from account 1 and £530 from account 2.

Cashplus was unable to recover any money from the recipient's bank. Following an investigation, it concluded that T was liable for the two payments. It said that this was because S, acting on behalf of T, had failed with gross negligence to protect the security details of T's accounts - in particular, S had provided the fraudster with the passcode.

S denied that he shared any passcode and complained to Cashplus along the lines mentioned earlier. But Cashplus said that it hadn't done anything wrong.

One of our investigators considered the complaint and concluded that it wouldn't be fair to ask Cashplus to reimburse the sum lost by T. They said, in summary:

- It is not in dispute that the two payments were unauthorised and made by a third party. Therefore, according to the Payment Services Regulations 2017, T wouldn't be liable for payments that they didn't authorise, unless they failed with intent or gross negligence to comply with the terms of the account or keep their personalised security details safe. T didn't fail with intent here. Therefore, the question is whether T, or S on behalf of T, acted with gross negligence.

  The very first step in the process of registering a new device was to enter the correct username and password for the account in question. So, it follows that the fraudster had to have known both usernames and passwords for the two accounts. It is not clear how the fraudster managed to obtain this information.

  The second step was an email from Cashplus which S did receive. The email was worded in a way that it was sent to the device which needed to be registered to the account as the new device. The email asked S to ensure that he was on the same mobile with which he logged into the account, and then press a button which said, 'trust this device'.

  S says that the caller alerted him to this email. He says that the caller told him that this email was sent by a fraudster. He was told that within the message there would be a 'trust this device' button but S should not press that button. Instead, he should forward the email on to an email address the caller provided. The caller told him that doing this would stop the fraudster accessing T's accounts.

  This ought to have raised some concerns to S. Firstly, what the caller said contradicted what S was told earlier – which was that a fraudster had already changed the number connected to his bank accounts. Secondly, if this was an email from a fraudulent third party, it raised the question of how a legitimate member of Cashplus could reasonably know its contents and the time it was going to be sent to S so accurately. Further, it is also reasonable to expect that S read the contents of the email before forwarding it, given the circumstances of the call. Finally, there was no reason for S to forward the

email at all. If it was from a fraudster as suggested by the caller, the normal advice would have been to simply delete it. Despite these inconsistencies, S forwarded the email as he was advised.

After S forwarded the email, he received a genuine text from Cashplus providing a passcode. He was asked not to share that code with anyone. There is no dispute about the contents of this text and the evidence shows it was received to S's phone. Cashplus says that entering the code on to the new device is a necessary part of registering it as a trusted device. In addition, the evidence shows that a new device logged into the account only after the code was sent. So, it seems most likely that the caller obtained the code sent to S's phone.

S disputes sharing the code with the caller but based on available evidence, it appears more likely than not that it was the only way the caller had obtained the code. Because S shared the passcode not once but twice (for the two accounts), the fraudster was able to complete the verification process and link their device to the accounts and go on to make the two payments. Taking all of the above into account, it is reasonable to conclude that S failed with gross negligence to keep the security details of each account safe. Therefore, Cashplus wasn't obliged to reimburse the unauthorised payments.

- Having reviewed the statements of each account for the six months prior to the unauthorised payments, it couldn't be said that the disputed payments were particularly unusual to normal account activity. So, it couldn't be said that Cashplus failed by allowing these transactions.

- S has also said that Cashplus didn't help adequately to recover the funds after he reported the fraud. It does appear that Cashplus could have done better in this respect. The evidence shows that it initially contacted a wrong bank thereby wasting time for over a month before it contacted the correct recipient bank. When the correct bank was contacted, Cashplus never received a reply. However, during our investigation, the recipient's bank has confirmed that T's funds were removed out of the recipient's account even before S reported the fraud to Cashplus. So, the bank's error didn't make a difference to the outcome.

S did not agree to the conclusions reached by the investigator. He said that the payments were not in line with the normal account activity and so Cashplus ought to have checked what was going on. He was also unhappy that Cashplus contacted the wrong bank in the first instance. He feels that Cashplus should accept some responsibility for T's loss.

S also said that he was in contact with his phone provider to provide details on the calls he received from the fraudster on the day. However, to date he hasn't provided that information despite reminders. That said, the investigator has accepted that the said calls did take place. So, I don't think I need that information in order to decide the outcome here.

**My provisional decision**

I issued a provisional decision partly upholding the complaint, which forms part of this decision. I said:

*I agree with the investigator that S's actions, taken together, meant that he acted with gross negligence. In addition to what the investigator has said, I also note that after the fraudster registered their device, S received another email from Cashplus which said: "You've just logged in to the Cashplus app using a new device …". The email identified the said device as iPhone 6S. It further said that "If you don't recognise this log-in call our*

*customer team immediately ..". And S received an identical second email in relation to the other account.*

*However, Mr S's phone was not an iPhone 6S and he had not logged into the accounts. I consider that this too ought to have alerted S that what he was seeing didn't match the narration provided by the caller. But there is no evidence that he acted following this warning.*

*Moving on to whether Cashplus in any case could have helped prevent the loss to T, I see that the investigator has concluded that the said transactions weren't unusual to the normal account activity and so it couldn't be said that Cashplus failed by allowing these transactions. S however disagrees. He says that the payments were unusual to normal account activity.*

*I have reviewed the previous account activity on both the accounts as part of my consideration to decide whether these payments were unusual to the extent that Cashplus ought to have intervened to verify that it was really their customer who was making the payments.*

*I have first considered the account from which the larger payment (£7,350) was made. Cashplus has provided us with a statement showing historical transactions on the account. However, from the statement it is difficult to know which of the outgoing payments were faster payments and which were through other modes of payments such as card transactions. It would have been useful to know this information because the disputed transactions were faster payments. So, knowing which past payments were faster payments would have enabled a like for like comparison.*

*Nevertheless, I have compared the disputed payments against all the prior payments made over a period of six months which I consider is a sufficient period of time to understand the normal account activity.*

*I see that this was a busy account with many transactions. However, most of the transactions tended to be of small value, typically below £1,000. The payment of £7,350 was one of the highest during the period. There were few other payments of similar value but from what I could see, they were made to existing payees – for example to HMRC, to a savings account of a director or to another account of T. Whereas this payment of £7,350 was to a new payee.*

*I don't think that in itself automatically ought to have been a concern to Cashplus. However, this large payment happened immediately following a change of device attached to the account. And the payment completely wiped out the balance on the account which was highly unusual to the account. The account had consistently maintained a healthy balance.*

*I think that the combination of the change of device attached to account, quickly followed by an attempt to make a large payment to a new payee and the payment unusually wiping out the account balance was an indication that the customer's account could be at risk of fraud. Therefore, I consider it reasonable to expect Cashplus intervened to verify with S whether he was making the payment on behalf of T. Had the bank done so, I consider the fraud would have come to light as S would have realised that payments were being made out of the account unknown to him. This in turn would have prevented the loss to T. But Cashplus failed to do so. Therefore, I consider it fair that it should bear some responsibility for the loss incurred by T.*

*However, I don't think that the payment of £530 from the second account stood out as unusual compared to the prior activity on that account. It was small in value, in line with the normal account activity and there were several past transactions of much higher value regularly being made out of the account. On balance, I agree with the investigator that it couldn't be said Cashplus failed by allowing this payment.*

*I can see why S is unhappy with the way Cashplus dealt with the matter after it was advised of the fraud, especially as it contacted the wrong bank. However as pointed out by the investigator, even if Cashplus had acted correctly in the first instance, the funds couldn't have been recovered as they were removed from the recipient's account even before the fraud came to light.*

*So, in summary, I have provisionally concluded that S acted with gross negligence. On the other hand, Cashplus too could have done more to prevent the loss to T in relation to the £7,350 payment – but not in relation to the £530 payment. Therefore, I consider it fair that Cashplus reimburses £3,675 to T, being 50% of £7,350. It should also pay simple interest at 8% p.a. on this amount. Interest should be paid from the date of the transaction to the date of settlement.*

**Responses to provisional decision**

Both parties accepted the provisional 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 see no reason to depart from the conclusions I reached in my provisional decision. I remain of the view that the settlement set out in my provisional decision represents a fair and reasonable outcome to this complaint. In summary, I find that S acted with gross negligence and as such Cashplus isn't obliged to reimburse the unauthorised payments. However, Cashplus could have done more to prevent the loss to T in relation to the £7,350 payment – but not in relation to the £530 payment. Therefore, I consider it fair that it reimburses £3,675 to T, being 50% of £7,350, together with interest.

## My final decision

My final decision is that I uphold the complaint in part. In full and final settlement of it, Advanced Payments Solutions Limited (trading as Cashplus) should pay £3,675 to T. It should also pay simple interest on this amount at 8% p.a. Interest should be paid from the date of the transaction to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 25 January 2024.

Raj Varadarajan
**Ombudsman**