DRN-4600663

The complaint

H complains Advanced Payment Solutions Limited trading as Cashplus didn't do enough to protect it when it fell victim to a scam.

What happened

H – a company with two directors including Mr A – has an account with Cashplus and has done so since 2019.

Mr A says he received a text message which appeared to have come from Cashplus saying that it had received his request to change his phone number and would contact him shortly. Shortly afterwards, Mr A says he received a call which appeared to come from Cashplus. He says the person he spoke to told him that he'd need to remove all of the numbers registered on H's account – of which there were two at the time including Mr A's mobile number. Mr A says he was told he'd need to log into H's account but the person he spoke to ended up taking him through the "forgotten password" process because he couldn't remember his password. Mr A says he received a one-time passcode on his mobile phone as well as an email asking him to click on a link and input the code he'd just received. Mr A says the person he spoke to told him that the account had at that stage been secured but that Cashplus would have to remove the numbers registered to the account and that he would receive a code confirming that his mobile number had been added back onto the account. The evidence suggests the call was at 18:37 on 8 December 2022 and lasted 34 minutes. In other words, the call ended at 19:01.

Mr A says he received a text from Cashplus – at 20:12 – confirming that his number had been changed. He says he didn't think much of this as he'd been told his number would be added back to the account.

The following day Mr A says he noticed two transactions totalling £7,690 that he didn't recognise when he logged into online banking. He contacted Cashplus to dispute them.

Cashplus looked into H's claim and said that it wasn't going to refund the two disputed transactions as Mr A had admitted that he'd shared security details with a third party. Mr A complained about Cashplus' decision and about the way his claim was handled, including delays. He also said he'd "never passed any code to anyone" and had "never done that and never said it" when that was something Cashplus relied on.

Cashplus looked into H's complaint, accepted that it could have handled the claim better and offered £25 as a goodwill gesture in compensation. But said that its original decision not to refund was the right one. H complained to our service with the help of a representative.

One of our investigators looked into Mr A's complaint and said that they didn't think Cashplus needed to do more as they couldn't see how H's account had been compromised based on what Mr A had told us. Nor did they think that Cashplus needed to intervene in either payment.

H's representative disagreed with our investigator's recommendation saying Mr A now

remembers that he shared his “memorable word” with the person he spoke to and that he sent an email to what he believed was a Cashplus address, but now realises isn’t. H’s representative said this all happened during the stress of the scam. In addition, they said that all the evidence shows Mr A was called by scammers who had spoofed Cashplus’ details and that both of the transactions were done on a device belonging to the scammers after they’ve tricked Mr A. In other words, H didn’t authorise either of the transactions. In addition, H’s representatives said that Mr A hadn’t acted negligently given the convincing nature of the scam. In the circumstances, they asked for H’s complaint to be referred to an ombudsman for a decision. The complaint was, as a result, passed on to me.

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.

Before I say what I think of this complaint, I believe it would be helpful to set out what happened on 8 and 9 December 2022 as I agree with our investigator that the evidence we’ve seen – and more importantly Cashplus looked at – doesn’t explain how H’s account was compromised unless Mr A carried out the disputed transactions himself or passed on security information. So that’s what I’ll do now.

The evidence I’ve seen suggests that Mr A did indeed receive a text message that appeared to be from Cashplus saying that it had received his request to change his number followed by a call that appeared to be from Cashplus. We know that scammers are able to “spoof” numbers to make messages and calls coming from them appear to be coming from the customer’s bank. So, I’m willing to accept for the moment that this is what happened in this case. The call started at 18:27 and lasted for 34 minutes and took place on 8 December 2022. In other words, the call ended at 19:01. Various things happened during that call based on the evidence I’ve seen.

The first thing that happened was that Cashplus sent Mr A an email with a link so that he could reset his password. That was sent at 18:44 followed by a one-time passcode two minutes later that Mr A had to input after clicking the link. He evidently did that because at 18:47 Cashplus sent him an email saying that his password had been updated and checking it was him. The email said “if this was you, feel free to ignore this email”. Mr A’s evidence is consistent with what I’ve said to date.

The next thing that happened was that Cashplus sent Mr A an email with a button that needed to be tapped in order to trust the device that had been used to log into the account. That email was sent at 18:51. A second one-time passcode was sent to Mr A’s mobile at 18:52 which the device to be trusted had to input. The button and the one-time passcode were evidently used because at 18:54 Mr A was sent another email saying that he’d “just logged in to the Cashplus app using a new device, and we need to make sure this was you”. Once again the email said “if this was you, feel free to ignore his email”. The email also confirmed the type of device that had logged in as an iPhone 7 Plus and that the account username used. Mr A’s mobile isn’t an iPhone7 Plus. In order for the new device to have been added that new device must have been used to log into H’s account, and the button in the email had to have been tapped on that new device and the one-time passcode needed to have been input on that new device.

The final thing that happened that day was that Cashplus sent Mr A an email and a text message to say that his mobile number had recently been changed – and to contact them straightaway if he didn’t make the change. That happened at 20:13. I can see that both of the mobile numbers that had been registered to H’s account before the call were removed shortly afterwards.

Based on what I've just said I'm satisfied that a new mobile phone – an iPhone 7 plus – was added to H's account on 8 December 2022. The only way that this could have been done is if the person who was in possession of the iPhone 7 plus was able to log into H's account and click on the link in the email sent to Mr A at 18:51 and input the one-time passcode that had been sent to Mr A's mobile at 18:52. Mr A told Cashplus that he hadn't shared any codes. Following our investigator's recommendation that this complaint shouldn't be upheld, his representatives have told us that he shared his "memorable word" which I'm assuming means the new password he created at 18:47. But in order to take the steps that the scammers – according to Mr A – took they would have needed much more information.

Given everything I've just said, I don't think it was unfair or unreasonable of Cashplus to say that it wasn't going to refund the two disputed transactions as I'm satisfied that Mr A told them that he'd shared his security details and that he did so. It follows that I agree with our investigator that this complaint ought not to be upheld.

My final decision

My final decision is that I'm not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask H to accept or reject my decision before 30 March 2024.

Nicolas Atkinson
Ombudsman