

## **The complaint**

Mr F complains, on behalf of K, that Advanced Payment Solutions Limited, trading as Cashplus Bank, won't reimburse transactions he didn't make or otherwise authorise.

The full details of this complaint are well known to both parties, so I won't repeat them here. Instead, I'll recap the key points and focus on giving reasons for my decision:

- In May 2022, Mr F received a text, in his usual text chain of messages from Cashplus. This referenced a request for change in contact number and that he would be contacted about that. He subsequently received a call, purporting to be from Cashplus's fraud team. He was required to pass security, and the caller knew details about Mr F and K's account, including recent transactions, which he was asked to confirm. He recognised some but didn't recognise others. It was at this point Mr F was asked if certain devices had been added to the account, which he also didn't recognise.
- The caller told him his account was at risk and the online banking would need to be reset, all devices removed and his trusted device added back on. Mr F followed the instructions and entered codes onto a weblink when promoted to do so. But, and unknown to Mr F, the caller had accessed K's account and made transactions totalling £13,100.
- Mr F discovered the loss when the call ended and he called Cashplus immediately. It declined to reimburse the transactions as it said he had shared sensitive information with a third-party and its One Time Passcodes (OTPs) specifically instruct for them not to be shared.
- Our investigator upheld the complaint in full. He wasn't persuaded Mr F made or otherwise consented to the transactions and he didn't find he'd acted with gross negligence or intent. Cashplus asked for the matter to be referred to an ombudsman; it considers as a long-standing customer Mr K ought to have realised he was inputting information into a website that wasn't its, and it says there had been lots of information in the mainstream media about fraud and scams and being extra vigilant especially when receiving unexpected texts or calls from a bank.

## **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 agree with the conclusions reached by the investigator for the following reasons:

- In line with the Payment Services Regulations 2017 (PSRs), Mr F (or K) isn't liable for payments he didn't authorise or consent to, unless he failed with gross negligence or intent to comply with the terms of the account and keep the personalised security details safe.
- It appears Cashplus accepts Mr F has fallen victim to an impersonation scam, and didn't carry out, or otherwise authorise or consent to, the transactions being carried out. Under the PSRs the transactions are therefore considered unauthorised.

- I don't find Mr F failed with intent to keep the security details safe. The actions Mr F took were carried out in the belief he was securing the account.
- I also don't find Mr F failed with gross negligence. Mr F believed he was speaking with someone from his bank. They knew details about him, including information about genuine transactions he had carried out. And the earlier message sent appeared in the same text message chain as other genuine messages from Cashplus. Whilst the text might not have been expected (and not all messages from banks are), the call was, as the text message told him to expect this.
- I accept Mr F passed on information he shouldn't have, including OTPs. But I don't think this means he seriously disregarded an obvious risk, and therefore failed with gross negligence.
- Mr F believed the actions he took were to safeguard the account and remove devices which had purportedly been added by a fraudster. In doing this, he was told his trusted device would also be removed and would need to be readded. He was provided with a weblink and was prompted to enter OTPs in order to do that. I accept K has been a customer for a number of years. I also accept the web address might not have been an exact match for Cashplus's address. But I don't think it was so different that Mr F ought to have been alert to an obvious risk, particularly as he would have been intent on following instructions he believed were being given by his trusted bank. And although the OTPs do say '*DO NOT SHARE with anyone!*' they also say '*This should only be entered on-screen when prompted.*' Mr F didn't share the OTPs per se, rather he entered them onto the website when he was prompted to do so. So he wasn't only following the prompts given by the fraudster but also the instructions in the OTP. This was a sophisticated multi-layered process which started with a text that laid the groundwork for Mr F to believe he was speaking with his bank. Overall, I can see how Mr F was tricked into believing the steps he took were to keep K's account safe, and I think a lot of people would have been tricked into doing to the same, or something similar.
- I don't find Mr F's actions fell so far below what a reasonable person would have done that it amounts to gross negligence. So I conclude neither Mr F, nor K, is liable for the transactions and Cashplus needs to put that right – by refunding the loss from the unauthorised transactions alongside interest to compensate for the time without, and loss of use of, those funds.

### **My final decision**

For the reasons given, my final decision is that I uphold this complaint. I require Advanced Payment Solutions Limited, trading as Cashplus Bank, to:

- Reimburse K £13,100 (less the £35 allowed for in the terms and conditions and PSRs, should Cashplus choose to rely those); and
- Add 8% simple interest per year from the date of that loss to the date of settlement, less any lawfully deductible tax.

Under the rules of the Financial Ombudsman Service, I'm required to ask K to accept or reject my decision before 1 February 2023.

Claire Hopkins  
**Ombudsman**