DRN-4714326

The complaint

Mr K has complained that Metro Bank PLC won't refund transactions he says he didn't make or otherwise authorise.

What happened

Over the course of several weeks in 2023, Mr K's online banking was used to send around £45,000 from his Metro account to a cryptocurrency account in his name. Just before this, he called Metro to get help logging in. Mr K also contacted Metro to request statements while the payments were still going on.

After the payments finished, Mr K reported them as fraudulent. He insists that he did not authorise the payments and was not scammed into authorising them. He says they were made without his knowledge or permission and he only found out about them after the fact.

Metro held Mr K liable for the payments in dispute, on the basis that they were made from his device and IP address, using his correct security details and one-time passcodes sent to his mobile number, to an account in his name set up using his photo ID, after he called Metro to get help logging in.

Our investigator looked into things independently and didn't uphold the complaint. Mr K appealed, particularly as he felt that Metro should have contacted him to check he was really authorising the payments. The complaint's been passed to me to decide.

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.

Broadly speaking, Metro can hold Mr K liable for the payments in dispute if the evidence suggests that he authorised them.

I'm satisfied from Metro's technical evidence that the payments in dispute used Mr K's genuine online banking facility, accessed from the registered device using the correct security details, with no remote access software detected. So I can see that these transactions were properly authenticated. The question, then, is whether the evidence suggests that it's most likely Mr K consented to the transactions or not.

Shortly before the disputed payments started, Mr K called Metro to get help accessing his online banking. Having listened to those calls, as well as Mr K's later calls to complain and his calls to our service, I am satisfied that this was Mr K.

With help from the staff on those calls, Mr K accessed his online banking on his device. That same device was then used to make the disputed payments. The payments were also made from the same IP address which Mr K used for his genuine activity both before and after the disputed payments. This IP address matches the internet connection for Mr K's home address. This strongly suggests that Mr K – or someone he gave his permission to – made the disputed payments.

According to Metro's technical evidence, no remote access software or virtual networks were used to access Mr K's online banking, and I've not found any evidence of hacking or of the security being bypassed. Mr K also confirmed that a trusted technical colleague had recently checked his device and found nothing suspicious, and his device was well protected. As far as I can see, the person using Mr K's account accessed it in the normal way using his security details. And based on what he's told us, it's not clear how anyone other than Mr K would've known his security details.

In order to log in and set up the payments, one-time passcodes were sent to Mr K's mobile number – the same number he gave our service. They were not sent anywhere else. Those passcodes were then entered to facilitate the disputed payments. Mr K was in possession of his phone. There doesn't seem to be a likely or plausible way that someone could've known those one-time passcodes without Mr K's consent. But again, it does suggest that he either made the payments or gave someone else permission to make them.

The disputed payments went to a crypto account in Mr K's name. The crypto platform confirmed that the account was set up using Mr K's photo ID, which matched with live facial recognition done via the phone's camera. While Mr K says he previously gave someone a copy of his photo ID, it's unclear how anyone could plausibly pass the facial recognition process without his consent.

It looks like Mr K checked his online banking a number of times during the weeks the disputed payments were being made. But he didn't tell Metro that anything was wrong until after they'd finished. It's not likely he'd wait until the payments were done before reporting them, if they were made without his consent. Similarly, while the disputed payments were still going on, Mr K asked Metro for statements for this month and for this particular account, saying he'd had some transactions and he wanted to see what his statements said about them. And before this incident, the last payment he made on this account was the previous year. So it looks like Mr K was aware of the disputed transactions at the time. But again, he chose not to report them to Metro until after the fact.

Lastly, I've not seen any evidence which makes it seem implausible or unlikely that Mr K could've authorised these payments or given someone else permission to make them.

In summary, I'm satisfied that the payments were properly authenticated, and that Mr K called Metro to get help logging in shortly before they started. The disputed payments were made on Mr K's protected device, on his home internet connection, with his correct security details, using passcodes sent to the mobile number he still uses, made to another account which it looks like only Mr K could've set up, with no signs of remote access or hacking. And Mr K appears to have been aware of the payments at the time, but he chose not to report them until afterwards. I've not found a likely or plausible way that the disputed payments could've been made without Mr K's consent. Instead, the evidence strongly supports that the payments were authorised.

Mr K suggested that Metro should've called him to check whether he was really authorising the disputed payments. But given that the payments were made to an account in his own name, from his device, at his home IP address, using his correct security details along with passcodes sent to his mobile, with no signs of remote access or hacking, following his call to Metro to get help logging in, I think Metro had enough to be reasonably satisfied that the payments were authorised. I don't see that they needed to carry out further checks about whether the payments were authorised or not.

So while I know this will come as a disappointment to Mr K, and while it is not my intention to disappoint him, I cannot fairly or reasonably tell Metro to refund these payments on the basis of them being unauthorised. The evidence too strongly supports that they were in fact authorised.

As has been mentioned before: if Mr K authorised these payments as part of a scam, there may possibly still be routes for getting his money back. But he would need to first divulge that the payments were authorised, and give full details on how any scam took place. If Mr K would like us to consider a complaint about being scammed into authorising the payments – as opposed to the payments being unauthorised – then he can ask our investigator for help setting up a separate case.

My final decision

For the reasons I've explained, I don't uphold this complaint about unauthorised payments.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 13 May 2024.

Adam Charles
Ombudsman