DRN-5950833

The complaint

Mr B is unhappy that Wise Payments Limited refused to refund him for transactions he says he didn't authorise.

What happened

Mr B contacted Wise in November 2024 to report six transactions he said he didn't authorise. The transactions totalled around £12,000 and were all made to a trading platform I'll refer to as V.

Mr B said he first became aware something was wrong in November 2024 after seeing an unrecognised transaction to V on his Wise account, but that he didn't raise it with Wise at the time because he wanted to try and resolve it with V directly.

Mr B said V initially seemed cooperative and provided partial refunds with the promise of further refunds being provided. To date, Mr B has received just under £2,500.

Wise investigated the matter but held Mr B liable for the transactions. In summary, Wise's position is that:

- The transactions were all made using Mr B's card details and were 3Ds approved meaning they were approved in the Wise mobile app
- Mr B's account was topped up prior to the transactions being made
- The transactions weren't inconsistent with earlier account usage – Mr B hadn't disputed transactions made to a similar merchant a month prior to the first disputed transaction

In support of Mr B's complaint, Mr B provided our Service with a report explaining how his devices were compromised by fraudsters and emails from overseas police and regulatory officials appearing to confirm that Mr B was the victim of identity fraud and that V were under investigation overseas. Both parties are familiar with the contents of these documents, so I haven't reproduced them in detail here.

One of our Investigators looked into Mr B's complaint and found the transactions were likely authorised on the basis Wise had provided evidence showing each of the transactions triggered app notifications that could only have been accessed through biometrics. The Investigator also noted that all the logins were completed on Mr B's trusted device.
Mr B rejected the Investigator's view, and I've summarised his response below:

- Mr B disagreed that the use of biometrics necessarily meant that the transactions were authorised, as well as the Investigator's statement that Mr B's device couldn't be compromised remotely
- Mr B felt the Investigator misunderstood why he delayed reporting the transactions to Wise and reiterated that he was trying to resolve things with V in good faith
- Mr B was concerned that the partial refunds had been misrepresented as profits when he saw them as evidence V had done something wrong

- Mr B questioned whether Wise's evidence was subject to the same scrutiny as the evidence he provided

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.

Mr B has provided a lot of information in support of his complaint, including details of a potential sophisticated hack resulting in identify theft and large amounts of money being transferred out of his account. It's not my role to forensically investigate the acts or omissions of V, actions of potential fraudsters or to comment on whether a crime has been committed – this is more suited to the courts.

My role is to consider Wise's handling of Mr B's complaint and to decide whether it was fair for them to hold Mr B liable for the transactions. To do this, I've considered whether Wise have fairly applied the relevant regulations, Payment Services Regulations 2017 (PSRs 2017) to Mr B's dispute.

I want to assure Mr B that I've carefully considered all the evidence provided but won't be referencing every point raised explicitly. Instead, I've focused my decision on the issues which I consider a fair outcome depends upon, largely the PSRs 2017. This isn't intended as a discourtesy to Mr B and is instead in keeping with our role as an informal Service.

Under the PSRs 2017, it's for Wise to show that the disputed transactions were properly authenticated. But even properly authenticated transactions can only be deemed authorised if they were made by Mr B himself or with his consent. So, for me to uphold Mr B's complaint, I'd have to be satisfied that either the transactions weren't properly authenticated or that they were made without authorisation from Mr B – it's these issues that I've focused on below.

Authentication

Having reviewed evidence of Wise's internal system, I'm satisfied the transactions were authenticated using Mr B's card details.

So, I've gone on to consider whether Mr B authorised the transactions.

Authorisation

Mr B has consistently said he didn't process the transactions, and I have no reason to doubt what he's said. But, as above, that's not enough for me to say the transactions weren't authorised by him. I must also be persuaded that Mr B didn't give consent for the transactions, perhaps by sharing his card details or approving the transactions on behalf of someone else.

Mr B has suggested fraudsters infiltrated his devices using sophisticated malware and were therefore able to compromise, amongst other things, Mr B's Wise app and emails. Mr B has provided a lengthy report which purports to explain how fraudsters gained access to Mr B's devices and how fraudsters would then be able to make it appear as though the disputed transactions were being carried out by Mr B. If Mr B's device was compromised in this way, it would remove the need for a third party to obtain physical possession of Mr B's belongings as the fraudsters would have had remote access.

I'm not an expert in cybersecurity and nor am I expected to be. As an Ombudsman, my role is to reach a decision based on the evidence provided and to do that I often need to consider the credibility and reliability of the evidence provided to decide what weight, if any, evidence should be given. I appreciate Mr B had concerns that we'd not scrutinised Wise's evidence in the same way, but I can assure Mr B that we test and challenge all evidence provided, equally.

I've not been able to verify the author's credentials or that the institution the author purports to be part of is a reliable authority on cybersecurity. Without this, I can't say the report was written by someone with the appropriate knowledge or experience to be classed as an expert and so can place little weight on either the content or the findings of the report.

I realise this will disappoint Mr B but, without reliable evidence of the use of malware, I can't say it was present on Mr B's device or reasonably conclude that it enabled a third party to infiltrate his phone and approve the transactions remotely in the way Mr B has alleged. So, for a third party to complete the transactions without Mr B's consent, it seems more likely that the third party would need to have taken physical possession of Mr B's card and phone.

There's been no suggestion that Mr B's card was lost or stolen or that he'd shared his details with anyone. So, to compromise Mr B's card details, a third party would likely need to obtain his card – and then return it – without Mr B noticing.

The third party would also need to have obtained Mr B's phone. As the transactions are spread over months, the third party would have needed to repeat this process multiple times. Mr B hasn't said his phone was lost or stolen and I find it unlikely a third party could repeatedly take and replace Mr B's phone without him becoming aware.

Once a third party had obtained physical possession of Mr B's phone, they would then need to have bypassed the security on Mr B's phone and Wise app to approve the transactions. As I understand it, Mr B used biometric security and, given I'm not persuaded by the report, there's no plausible explanation for how this security was bypassed.

On balance, I find it unlikely that a third party was able to take possession of Mr B's card and phone without him noticing. Mr B might not have initiated the transactions but that wouldn't have prevented him from approving the transactions for someone else - and whilst I can't say this is definitely what happened, I think it's more likely that the transactions were carried out with Mr B's consent and were therefore authorised.

Considering the nature of the transactions, I can't say Wise ought to have flagged them as suspicious. I say this because there are transactions to similar merchants, one which may even have a link to V, present on the account so it wasn't inconsistent with Mr B's previous spending history.

I appreciate what Mr B's reason for not disputing the transactions with Wise earlier, but I question why someone who was concerned that they were the victim of identity theft and a sophisticated cyber-attack, didn't take steps to secure their account, such as by asking Wise to block future payments to V or ordering a new card. I don't wish to appear insensitive to Mr B's situation, but I think it's a fair consideration given such action could have prevented further loss to Mr B and would still have left him free to try and resolve the issue with V directly.

With regards to the payments Mr B received from V, I understand Mr B is unhappy that these payments may have been seen as investment profits when they should be seen as an admission of V's wrongdoing. I accept that the payments could have been partial refunds from V because I can see Mr B had raised concerns and V seemed to be engaging with

them. But, as above, I can't consider the acts or omissions of V directly and I'm instead considering what the relevant regulations expect of Wise. So, even if V agreed to refund Mr B, that doesn't mean Wise are obliged to do the same.

Overall, there's insufficient evidence to substantiate Mr B's claim that a third party completed the transactions after infecting his devices with malware and there's therefore no plausible explanation for how a third party could have completed the transactions without Mr B's consent, and authority. I appreciate Mr B feels strongly that he's been the victim of a cyber-attack and has lost a significant amount of money as a result, but the evidence persuades me that Mr B authorised the transactions and it's therefore fair for Wise to hold Mr B liable for them.

My final decision

My final decision is that I don't uphold Mr B's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 4 March 2026.

Freyja Dudley
Ombudsman