DRN-5724159

The complaint

At the time of the complaint, Mr B was a sole trader. Mr B is unhappy that Wise Payments Limited have refused to refund a transaction he says he didn't authorise.

What happened

Mr B first contacted Wise in March 2024 to dispute a payment of just over £6,000 to a luxury retailer. Mr B explained he was alerted to the transaction after receiving a text message containing a one-time-passcode (OTP) which prompted him to check his Wise account. Upon checking his account, he saw the transaction had been successful.

Wise looked into Mr B's dispute but didn't offer a refund as they concluded the transaction was authorised. Wise's argument was that the transaction was processed using Mr B's correct card details and had an additional layer of security in the form of 3D Secure (3DS).

Unhappy with Wise's response, Mr B referred his complaint to us.

Mr B said:

- Mr B had provided evidence he was out of the country at the time of the transaction – as well as evidence the transaction originated from a UK IP address
- The transaction was inconsistent with the usual account activity. The account was predominantly used for business related purchases, and the disputed transaction was high value from a luxury retailer.
- Mr B contacted the merchant and Wise promptly in an attempt to resolve the issue and reverse the transactions
- Mr B also asserted that the OTP must have been obtained using a form of malware that enabled a third party to access Mr B's SMS messages and validate the payment without his consent

In terms of suspicious correspondence, Mr B said he regularly received emails with PDFs attached that disappear once opened, and he recalled receiving one around the transaction date.

One of our Investigators considered Mr B's complaint and initially recommended that it was upheld. The Investigator concluded that the transaction didn't match his usual account activity, Mr B's actions were consistent with his testimony that he didn't authorise the transaction and it couldn't be ruled out that Mr B's device was compromised.

Wise didn't agree that Mr B's conduct after the transaction was sufficient to say it was likely unauthorised. Wise explained that the operating software on Mr B's device was secure and malware attacks were incredibly rare. Finally, Wise thought that a single transaction was inconsistent with typical fraudster behaviour.

The Investigator then issued a revised opinion in which they concluded that the transaction was likely authorised because Mr B needed to have participated in the transaction for the OTP to be inputted successfully.

Mr B disagreed with the Investigator's view and provided the following response:

- Mr B reiterated that he was out of the UK at the time of the transaction

- He'd already provided evidence which showed malware was present on his phone following a malware scan
- After conducting research, Mr B found other examples of malware or phishing being used to compromise phones and obtain OTPs without the cardholder's knowledge
- Wise have said it's rare, but not impossible, for his phone to be compromised by malware
- If he'd shared the OTP or authorised the transaction, he'd have been able to share more details with Action Fraud
- Evidence the OTP was entered correctly isn't evidence Mr B entered the OTP
- Mr B reiterated that he reported the transaction promptly

As an agreement couldn't be reached, the complaint was passed to me for a decision.

After reviewing the file, I asked Mr B for more information including evidence of the suspicious emails he said he received. Mr B provided screenshots of multiple emails received at various different times – I've considered what this means for his complaint below.

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.

When deciding this complaint, I have given regard to the Payment Services Regulations 2017 (PSRs 2017).

I've seen evidence from Wise's internal system which satisfies me the transaction was authenticated using Mr B's card details.

However, authentication alone isn't sufficient for Wise to hold Mr B liable for the transactions. Under the PSRs 2017, there must be evidence that Mr B either made the transaction himself or authorised a third party to make it on his behalf.

Under the PSRs 2017, Mr B is liable for any transactions he made himself or consented to. This means that as well as being satisfied Mr B didn't initiate the transaction himself, I must also be persuaded that he didn't give consent for the transaction by sharing the OTP with a third party. Given Mr B has consistently said he didn't participate in the transaction or share the OTP, I've considered the likelihood of a third party being able to obtain the OTP without Mr B's consent.

I can't safely conclude that a third party took and replaced Mr B's phone without his knowledge. I say this because Mr B said his phone was always in his possession and he was out of the country at the time the transaction was carried out in the UK. To carry out and approve the payment a fraudster would have needed to obtain Mr B's phone, bypass its security and his banking app before returning the phone, all without him noticing. I find this very unlikely. Instead, Mr B suggests that some form of malware must have infiltrated his device and enabled a third party to obtain the OTP from his text messages.

Mr B has said he receives regular correspondence through social media and by email which appear to be from scammers. Around the time of the disputed transaction, Mr B said he'd clicked on a suspicious email that then disappeared. Mr B has provided evidence of similar emails to demonstrate the content and frequency of these messages.

Wise have said it's rare for the operating system to be compromised as devices like Mr B's are generally considered secure.

I don't find Wise's statement that successful malware attacks on devices like Mr B's are rare particularly persuasive because they've not provided evidence to support this. But I'm also not persuaded by the malware scan results provided by Mr B either. I say this because the

scan seemed to conclude that ‘threats’ had been identified but none of these threats explicitly linked to malware. And whilst Mr B has provided screenshots of similar emails he says were received from scammers, he’s not been able to provide evidence of the specific email he received and clicked on.

I realise this will disappoint Mr B but without evidence 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 access the OTP in the way Mr B has alleged.

I'm satisfied that Mr B was out of the country when the transaction was carried out from within the UK, as shown by the IP address linked to the transaction. But this doesn’t mean Mr B didn’t consent to the transaction. Being out of the country wouldn't have prevented Mr B from sharing the OTP with someone else – and whilst I can’t say this is definitely what happened, I think it’s the most likely explanation based on the evidence available.

On balance, I think there’s insufficient evidence to substantiate Mr B’s claim that a third party obtained the OTP using malware and there’s therefore no plausible explanation for how a third party could have obtained the OTP from Mr B’s phone without his consent. I understand Mr B’s found this experience stressful and he’s advised the loss of the funds has impacted his business. However, for the reasons I’ve outlined above I think it’s fair for Wise to hold Mr B liable for the transaction. And I won’t be asking them to do anything further here.

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 6 February 2026.

Freyja Dudley
Ombudsman