

The complaint

A limited company, P, complains that ClearBank Limited has declined to refund disputed transactions that debited its account.

Mr A is a director of P and has brought this complaint on its behalf.

P's account is operated through a platform provided by ClearBank under the Tide brand. So, I'll refer to Tide throughout.

What happened

The circumstances of this complaint are well known to both parties, so I will not repeat them all again here in detail. But I will provide an overview of the key events below.

Mr A says 17 card transactions were made from P's account totalling around £4,000, and that he did not make these payments.

The transactions took place between 22 August and the early hours of 23 August 2024 and payments were made to various merchants. On waking up in the morning and discovering what had happened, Mr A states he reported the matter to Tide.

Mr A mentions that prior to the transactions taking place, he had received text messages on 21 August relating to a parcel delivery and that he had clicked on an icon. He states he subsequently experienced strange phone activity – which suggested his phone was being controlled by someone.

Tide investigated but rejected Mr A's claims. It said the payments had been approved via the Tide app and that there were a number of credits to the Tide account which had funded the payments made and these seemed to have happened simultaneously. It said that as the payments were directly approved via Mr A's device, chargeback rights did not apply in this instance and Mr A was referred back to the merchants and the police for further assistance. Mr A says he was unable to make contact with any of the merchants and considered them fake.

Mr A raised a complaint with Tide, he maintained he had not made the payments and that P was at a detriment due to bills remaining unpaid. But Tide's position remained unchanged. As Mr A remained unhappy, he referred P's complaint to this service for consideration. But our investigator didn't think Tide was responsible for P's loss. And she felt that the payments had most likely been authorised by Mr A.

Mr A didn't agree and asked for an ombudsman's decision. So, it'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.

Having done so, I'm not upholding this complaint, for the reasons I set out below. I appreciate this will be disappointing for Mr A, and I'm sorry to hear about P's loss and the financial impact this matter has had on the business, but I can't fairly and reasonably ask Tide to refund P here.

The relevant rules that apply in this instance are the Payment Services Regulations 2017 (PSRs).

Under the PSRs, a payment is authorised if it is correctly authenticated and consented to by the consumer, or on their behalf. The PSRs say that consent must be given in accordance with the form and procedure agreed between the payer (P) and the payment service provider (Tide).

Having considered the evidence as well as the relevant law, it seems to me that the main consideration for me to make here is whether it is more likely than not that Mr A on behalf of P, authorised the transactions now disputed. This is important because a customer will usually be liable for payments they've authorised and, generally speaking, a payment service provider will be liable for any unauthorised payments.

It's clear from the information provided, that transactions totalling almost £4,000 were made from P's account between 8.35 pm on 22 August and 3.14 am on 23 August, and that most of these transactions took place in the early hours of the morning. Tide says that the payments made from P's account were approved on Mr A's device using 3D Secure authorisation (3DS) approval. So, it had no reason to believe the transactions were being made by anyone other than Mr A.

What this means is that the transactions required Mr A to complete a further authorisation step which required him to be logged into the Tide app to approve the payment.

So, I have gone on to consider internal audit records of the transactions presented by Tide, along with information presented relating to Mr A's other business account, which is held with another provider, so as to understand the timeline clearly as to what credits and debits were made on the account. Having done so, I'm satisfied that the disputed transactions were all made using the Tide banking app which was on Mr A's mobile phone device.

The mobile online banking logs for the account, provided by Tide, show that 3DS authorisation was successful after a successful login onto the app via Mr A's mobile device - which Tide says was accessible by passcode or Face ID. Based on the steps required to verify the payments - which required Mr A to select the "approve" option presented - I'm persuaded that Mr A did authorise the payments on behalf of P.

Tide also says that several inbound transfers were credited to the account to fund the transactions in question.

I note that Mr A in his submissions to this service, confirmed that he had himself instructed the transfers of money to his Tide account from an account held with another provider. But on reviewing information presented by Tide I can see that there is some inconsistency with what he told Tide and what he has told us.

Tide has presented a copy of the chat that took place between Mr A and Tide on 23 August when he first reported his concerns, and it seems to suggest that he initially had not instructed the credits to his Tide account.

He specifically mentions the following:

“My phone looks like been scammed they have been transferring money from my other business account and making payments to somewhere...”

But this isn't in keeping with what Mr A told this service. When asked whether he had instructed the transfer of funds from his other business account to Tide on 22 and 23 August 2024, he instead said:

“Yes I made payment”

I can see Mr A then went onto to provide a further explanation stating he had made genuine requests for payments to credit his Tide account, but as the app for his other account failed to respond, he didn't realise that money had in fact been credited to Tide until the next morning. He also says the purpose for transferring the money to Tide was to cover a payment for an order he had placed for the shop, and a rent payment to his landlord, and that he was having difficulty making these payments directly from the other account.

I don't doubt that this is why he transferred the money, but with that being said, what I am finding difficult to understand is why - if it was indeed his intention to cover these two payments - that he went on to make several separate transfers to his Tide account instead of just two. And that these payments then by chance, provided the relevant funding to cover the disputed payments that then left his Tide account.

Mr A says that after clicking on an icon in a message he had previously received, he experienced unusual activity on his phone – as if it was taken over - and mentions that he subsequently took it to a phone shop to be looked at for viruses, and it seems to be restored. But I can see no evidence of a possible compromise has been presented, apart from screenshots of the messages he received, and nor have I seen any persuasive evidence of this being the case.

Given Mr A's concerns about his device - which seemed to be apparent to him as soon as he clicked on the message he had received, and he says he noted access to various apps taking place without his consent - it's also unclear why no precautions or concerns were raised with either Tide or his other account providers sooner.

Mr A maintains he didn't receive any messages from Tide to confirm the payments made and also says he didn't log into the Tide app. But Tide has shown that the account was only ever accessed from Mr A's device, and the Internet Protocol (IP) address remained consistent throughout. In light of this, the only plausible explanation is that either Mr A made and authorised the payments himself from his device, or that he gave his consent and authority for the payments to be made on his behalf.

Mr A, when asked, confirmed that his device was in his possession and that apart from his six-year-old son, no one had access to it and it was password protected. He also says he never shared his Tide banking details with anyone and nor did he have them written down anywhere. And his Tide card also remained in his possession in his wallet.

So, given this, there is no reasonable explanation for how a third party could have gained access to his device. I can understand why Tide believed the transactions were being authorised by Mr A when they were processed and I'm satisfied that all the payments were processed after being 3DS authorised.

I note Mr A told Tide, that his son, who plays games on his phone, may have made in-app purchases using his card details which he states were saved on his phone. But as the

disputed transactions were mostly made in the early hours, Tide were not convinced by this explanation. Having reviewed the times that the transactions took place, I am also not persuaded that this is a plausible explanation for what happened here.

But even if we were to consider this to be the case, it doesn't explain how transfers from Mr A's other account credited P's Tide account prior to the transactions being debited.

I accept it's plausible that Mr A was targeted by fraudsters with the intention of taking advantage of him for their own financial gain. But in light of how the transactions were authorised, which would have first required access to Mr A's device and then secondly access to the Tide app, I find it more likely than not that he authorised all of the disputed payments himself. I appreciate that Mr A says that as his card details were saved on his phone, the fraudsters would have had access to them as he believes his device was compromised, but as previously explained I haven't seen any evidence of this.

It also evident from what Mr A has disclosed, that his account held elsewhere was not affected by what happened. And Mr A confirms he was able to access this via a separate app, also on his phone and I can see it held a considerable sum of money. So, if the phone was compromised as Mr A believes, I would've expected a fraudster to take full advantage of any money held within any account that they could access. But it seems that this was not what happened here.

On the balance of probabilities, I find it more likely that Mr A was aware payments were being made and authorised them himself.

Finally, although I'm satisfied, based on the above that Mr A most likely authorised the disputed transactions, I've also considered whether Tide acted fairly and reasonably in processing the transactions from P's account, or whether it should've done more to assist. And I've reviewed P's bank statements for the months leading up to the disputed transactions.

Having done so, I don't think the payments made were particularly unusual based on previous account activity seen. And while it's clear there were a large number of transactions sent to various merchants during the time in question, I'm not persuaded that the payments were significantly different or unusual in nature for the account, in that they ought to have prompted Tide to intervene. And I also don't think there was anything Tide could've done to recover the money from the merchants. The payments had been approved and made to genuine merchants, which would've most likely provided goods or services in return for the payment. So, I don't think it's likely that Tide could've recovered the money by using the chargeback scheme.

I appreciate this will come as a disappointment to Mr A, and I sympathise with the position he finds himself in. However, it follows that I won't be asking Tide to refund P's loss.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask P to accept or reject my decision before 24 November 2025.

Sukhdeep Judge

Ombudsman