

## The complaint

F complains Tide Platform Ltd (Tide) has refused to pay back over £11,000 worth of fraudulent transactions spent from his Tide business account using Apple pay after his mobile phone was stolen.

## What happened

F explained his mobile phone was stolen in the early hours of 21 October 2023 whilst he was out with friends. He said his mobile phone was accessed and over £11,000 transferred into his dormant Tide business account from another of his personal bank accounts. These transferred funds were then spent on a series of purchases in three retailers using the Apple pay feature on his phone on the 21 October over only a few hours.

F said his recollection of the evening of the 20 October is poor and doesn't know how his phone was stolen, he explained he believes he had a drink '*spiked*' and suspects the thief may have obtained his passcode for his phone '*despite having biometrics enabled on my phone*'. F explained if the thief had obtained his passcode, they could have gained access and added their own biometrics to his phone. F said he thinks a situation was '*manufactured*' where he had to put his passcode into his phone when Face ID login had failed. He said this could have been caused by someone making him look away when trying to unlock his phone, then observing his passcode. F also said he kept his passwords saved on his phone, including his Apple ID password. He also explained his biometrics auto populated and authenticated applications on his phone, including his Tide banking app.

F explained the day after his phone was stolen, he didn't know what had happened. He first tried to find his phone thinking he may have left it at the venue. He said when he got home he tried to put his phone on lost mode and used Find my iPhone but the phone showed as not found.

F provided evidence to show he later discovered the thief had changed his apple ID password and turned off Find my iPhone. This also meant he could not access emails so had no idea of the fraud being committed on his various bank accounts.

F obtained a replacement sim card on 22 October. When he placed it inside a spare phone he became aware of the extensive fraud which involved several financial assets and businesses. F said it was only after contacting a third party bank later that day he realised some of the funds had been transferred to his Tide business account and this had been done by the fraudster impersonating him over the phone. F explained he had not used his Tide account before and had set it up to potentially use for a business opportunity which didn't happen over a year earlier.

F explained he didn't realise what had happened until later and raised the issue with Tide on 23 October providing it with a crime reference number.

F explained he is also unhappy Tide did not have any systems in place to detect these transactions as fraudulent. F explained he would like all the money taken out of his Tide account refunded, he would like significant compensation and a letter of apology.

Tide partially upheld F's complaint accepting it took too long to reply to him, but it did not think it needed to pay back the £11,000 spent through his Tide prepaid card.

Tide said it thought there were discrepancies in F's version of events and said it took him two days to contact them and advise his phone had been stolen. Tide accepted it had been told sooner by F's third party bank of the fraud and had already blocked F's Tide account when he contacted them.

Evidence provided by Tide show F's third party bank contacted it at 11.14pm on 22 October telling Tide two transactions into F's Tide account were fraudulent, the third party bank subsequently explained it had been able to stop one of these payments but not the other. The third party bank also later confirmed another fraudulent payment had been made into F's Tide account.

Tide confirmed on 24 October no funds remained in F's Tide account. Tide also explained as F had not used his account, it had no spending pattern data to use to detect fraud and said it was not unusual for large transactions to be made through a business account.

Tide wrote a final response letter (FRL) to F on 2 November. It said it had spoken with F who had confirmed no-one else could access to his mobile phone. Tide said F explained he had *'Face ID with passcode enabled for your device and your Tide app could be accessed with Face ID'*.

The FRL did not say whether Tide are upholding the substantive element of F's complaint, namely the fraudulent transactions totalling over £11,000, but it has since clarified it does not intend to refund this money to F. The letter also explained is partially upheld F's complaint regarding the delays, but did not offer any compensation for this.

Tide claimed F had explicitly said the setting on his phone was for Face ID. This means access to his phone required his face to open it and access his apps. Tide have said as this was the case, it could not see how the transaction were fraudulent. Tide could not say whether F's Face ID had been changed on F's iPhone, as this was not information they had access to.

Tide said they thought F had made these transactions on the balance of probabilities, due to the security on his phone.

Our investigator thought the payments were unauthorised and recommended upholding F's complaint and thought Tide should refund the transactions.

Tide disagreed with our investigator's recommendation. It explained it thought our investigator had relied on evidence provided by a third party bank which it described as not relevant, and that our investigator had not explained why they thought the transactions were unauthorised. Therefore, this complaint has been passed to me to make a final decision.

### **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.

I appreciate how strongly F feels about his complaint. Although I may not mention every point raised, I have considered everything but limited my findings to the areas which impact the outcome of the case. No discourtesy is intended by this, it just reflects the informal nature of our service.

The Payment Service Regulations 2017 (PSR) say customers are generally liable for payment transactions they authorise, and payment service providers will generally be liable for unauthorised transactions. The PSRs also say when a customer denies having authorised a payment, it is for the payment service provider to prove the payment transaction was authenticated and that the customer gave consent for the payment.

F has provided evidence his Apple ID was changed and phone location finder disabled on 21 October soon after he said his phone was stolen. He has also provided a crime number and evidence he has raised similar cases with other financial institutions he is a customer of,

who agreed F had been the victim of fraud. Contrary to Tide's response to our investigators view, I do consider this is relevant and, on balance, corroborates the evidence he has provided of his phone being stolen and compromised.

In its responses, Tide have relied on F explaining he used Face ID to access his iPhone and concluded no-one else would have been able to make the subsequent contactless payments because of this security on F's phone.

F has since clarified that he did keep passwords saved on his phone, including his Apple ID password. F explained he was in a busy pub, may have had his drink spiked and described how he thought a situation may have been manufactured so he revealed his passcode, thus circumventing Face ID. This information would seem consistent with an opportunity for shoulder-surfing F during purchases or otherwise using his phone, and subsequently stealing and gaining access to it.

As stated, F explained a passcode could also be used to access his phone and Face ID could have been changed during this access if he had been shoulder-surfed. Again, I am satisfied there is evidence of an opportunity for a thief to gain access to F's phone. It is clear to me biometrics were not the only method to gain access to F's phone and as his apps were linked to this access. I am satisfied on balance this explains how unauthorised access could have occurred to his various banking apps.

Tide have also explained it thought it unusual the fraudsters knew when to stop using the card and there were no undisputed transactions. However, the evidence suggests the fraudsters had access to F's various bank accounts and were also responsible for transferring the funds into his Tide account so would have known how much they could spend before the card would be declined. Furthermore, I think it likely they would not have wanted to draw attention by having a purchase declined whilst in the various retailers. This is possibly corroborated by the fact the purchases in some of the retailers are spread over several transactions in a short period of time, rather than one large purchase.

Whilst I agree the transactions made on the afternoon of 21 October have been authenticated, I am satisfied from the evidence I have seen that, on balance, F did not consent to these payments. I think the pattern, transfers and amount are consistent with fraud. I also think F has explained how the compromise could have occurred, and I am also mindful F had not used this account before and cannot see a reasonable, logical explanation as to why F would have taken the action here i.e. moving significant funds from his regular bank account and then using Apple pay for numerous high value purchases.

I am persuaded these transactions are consistent with fraud and points to these payments not being consented to. I am not persuaded, on balance, Tide have proved these transactions were authorised.

I now need to consider whether there is any reason not to hold Tide liable for the repayment of these funds, in other words, is there any evidence F did something which enabled these payments.

Tide's terms and conditions (T&Cs) say customers *'must take reasonable steps to keep personalised security credentials for accessing Tide Platform safe and confidential. You must notify Tide without delay on becoming aware of the loss, theft misappropriation or unauthorised access to or use of your personalised security credentials for the Tide Platform ... If someone makes an unauthorised payment because you've failed to do this, we won't normally refund the payment'*.

Tide's T&Cs also say *'A payment from your account was unauthorised, unless:*

- *You've been deliberately or grossly negligent with your security details; or*
- *We can prove you acted fraudulently.*

*One your claim has been investigated and we're satisfied you've not been careless or that you've not acted fraudulently, the payment amount will be refunded and any charges linked to that payment, except for the first £35 which we may charge to you.*

*We won't charge you for any unauthorised payments which take place after you've notified Tide of the unauthorised payment or that your security details relating to your account have been lost or stolen'.*

I have considered the evidence F has provided alongside these relevant Terms and Conditions. Tide said the transactions were not fraudulent because the security restrictions on F's phone were enough to prove the transactions were authorised.

Tide are relying on third party authentication here. Because of this Tide have been unable to say whether the biometrics were changed on F's phone as they do not have access to this information. I therefore think, on balance, I have not seen evidence of consent being proved, as required, by Tide throughout the evidence I have considered.

In terms of reporting the fraud '*without delay*' F has explained he had not used this account and had understandably focused his attention on the fraud on his regular accounts first, before realising that transactions had occurred on his Tide account as well. I consider this to be logical and reasonable in the circumstances and I'm satisfied that once he became aware of the issues, he raised it with Tide. I am therefore persuaded in these circumstances F did report the fraud without delay.

Whilst I appreciate the majority of the distress and inconvenience caused to F is due to the actions of the party that stole F's phone, I have also reconsidered the inconvenience Tide caused F.

I appreciate F has asked for '*significant compensation*' in his complaint to our service. However, I am mindful that the account was a business account, so this limits the award I can make in terms of distress. Nevertheless, I can see F presented evidence to Tide and was repeatedly told he was not eligible for a refund. I have also considered the delays Tide upheld in its final response letter, but decided not to offer compensation for, despite the clear inconvenience this would have obviously caused F.

Having considered the numerous contacts during the period, and the delays Tide have accepted and apologised for, I am awarding £200 compensation for this inconvenience.

To be clear, this award does not include any distress or inconvenience caused by the CIFAS marker Tide applied to F, as I understand F has indicated recently to our service he may wish to make a separate complaint regarding this matter and this did not form part of his original complaint to our service.

Finally, I note Section 13 of Tide's T&Cs allows for £35 per transaction not to be refunded. I would ask Tide to consider not deducting this sum from each of the transactions before refunding F. My reason for requesting this is that the fraud was committed to only a few retailers, but over many transactions. It would seem unfair to rely on these terms and conditions, although agreed to by F, in these circumstances. I also note some of the transactions were for smaller amounts, this fee which would significantly impact the refund for these fraudulent transactions.

### **My final decision**

For the reasons I have given, my final decision is I uphold this complaint. I require Tide Platform Ltd to refund all the disputed transactions to F and pay 8% simple interest on the balance between the date of the withdrawals and the date the refund is made.

I also require Tide Platform Ltd to pay F £200 compensation for the inconvenience it has caused him.

Under the rules of the Financial Ombudsman Service, I'm required to ask F to accept or

reject my decision before 1 August 2024.

Gareth Jones  
**Ombudsman**