DRN-4141394

The complaint

Mr S, in his capacity as the director of a limited company "K", complains that PrePay Technologies Limited (PPT) won't refund transactions he didn't authorise.

K has an e-money account with Tide which is provided by PPT, and so PPT is the respondent business here. For the most part, I've referred to it for actions of both businesses. But where necessary, I've referred to Tide specifically.

What happened

In February 2022, Mr S was contacted by someone pretending to be from Tide. They told him K's account had been compromised.

Under the pretext of safeguarding the account, the caller obtained account information from Mr S – including a one-time passcode (OTP). Mr S also followed the caller's instructions and uninstalled the Tide app from his device.

Several days later, when he installed the app again and logged on, Mr S realised money had been fraudulently taken from K's account. The scammer had made more than 50 transactions, totalling approximately £50,000, during that period through Apple Pay. Mr S immediately reported this to Tide through its in-app chat. He also reported the matter to the police.

PPT declined to reimburse K's loss; it said it didn't have compelling evidence to suggest that the disputed transactions were done without Mr S's knowledge or authorisation.

Our investigator didn't agree with PPT that K should be held liable; they weren't persuaded the transactions were authorised by Mr S. They recommended PPT to refund the transactions along with interest and pay £200 compensation. PPT disagreed and the complaint was passed to me to decide.

I requested further information from both parties. Mr S explained why he was unable to provide an itemised call log from his mobile network provider showing the scam call and forwarded an email from the provider to support this. Although PPT replied, it didn't provide all the information I asked for. I issued my provisional decision in April 2023. I said that I intended upholding this complaint and set out the following reasoning:

> *In line with the Payment Services Regulations 2017 (PSRs), K isn't liable for payments it didn't authorise, unless Mr S (acting on K's behalf) failed with intent or gross negligence to comply with the terms of the account or keep the account security details safe.*
>
> *When there's a dispute over whether a payment was authorised, it is for the payment service provider (PPT in this case) to prove that the transaction was authenticated correctly. Under the PSRs, we also need to consider whether the payment service user (here that would be Mr S on behalf of K) gave their consent to it. And consent*

must be in the form and in accordance with the procedure agreed between the two parties.

The terms and conditions explain that Mr S can use his card by entering the PIN or other security code, or by tapping his card against a contactless enabled reader, or via Google Pay when the functionality is made available. Although there's no explicit mention of Apple Pay, practically speaking, my understanding is that Mr S could have used a payment wallet – including Apple Pay – to make payments.

I asked PPT to provide evidence of the Apple Pay token registrations for Mr S's card, as well as details of the token and mobile device that was used to make the disputed transactions. This information hasn't been forthcoming. As such, I would argue that PPT hasn't sufficiently demonstrated that the transactions were authenticated correctly. As it hasn't done that, according to the PSRs, the transactions can be treated as unauthorised.

Even if I were to make a finding that the transactions were authenticated – either on balance of probabilities or on the provision of the outstanding information request – I'm not satisfied that Mr S gave his consent. I say this because I haven't seen any persuasive evidence or arguments that it was Mr S who completed the required steps for the transactions to happen, or that he consented to someone else doing so. I consider it more likely than not – and that is what I must base my decision on in situations where I can't know for sure – that Mr S shared information he was sent by Tide (i.e., the OTP) with the caller. And it was this information that was used to set up an Apple Pay token on another device that enabled the disputed transactions to take place without Mr S's knowledge or consent.

PPT has argued that there's no evidence Mr S was scammed. It says there's no evidence he received a call on the day in question like he claims he did. PPT submits that Mr S initially said he hadn't received any suspicious calls that day and had provided a screenshot of his phone's call log to evidence there were no incoming calls. It argues that Mr S has subsequently changed his testimony but has been unable to provide any supporting evidence.

On the point about the change in testimony, Mr S has previously told the investigator that at the time of reporting the scam he was still trying to piece together what had happened. He'd subsequently remembered receiving a call. That said, when this case came to me for a decision, I did share PPT's concerns regarding the lack of supporting evidence. Mr S had previously requested an itemised call log from his network provider but was told only outbound calls could be provided. Having done some research into this, it doesn't look like the provider in question provides details of incoming calls as a matter of routine. At my request, Mr S made a subject access request to the provider. I've seen the provider's response; it says it can only provide a log of outbound calls and it doesn't hold incoming calls data. As this response has come directly from the network provider, I'm satisfied that Mr S has been honest with us about why he's unable to provide the requested information.

Although there's no explanation for why the screenshot Mr S initially sent to PPT doesn't show any incoming calls, the network provider's response means that we can't say for certain that a call didn't happen. Having weighed up everything, including the lengths that Mr S went to in obtaining information from various merchants involved to try and recover his funds himself (as evidenced in the chat logs with Tide that PPT has provided), on balance, I'm more persuaded that Mr S did receive a call and that he was scammed. And I think it's more likely than not that this

is how the scammer was able to register an Apple Pay token on their device to carry out the transactions in question.

Notwithstanding that I've not yet seen evidence that the transactions were authenticated correctly, I'm not persuaded Mr S consented to them, or gave his consent to someone else. So, I find that they were unauthorised.

As I mentioned earlier, Mr S could still be held liable for transactions he didn't authorise if he failed with intent or gross negligence to comply with the terms of the account or keep the account security details safe.

I don't find that Mr S failed with intent to keep his security credentials safe. I say this because he believed the information he'd been asked to share with the caller was necessary to secure K's account. So, in his mind, he was safeguarding the account's security.

I also don't find that Mr S failed with gross negligence. From what he's described, the caller already had some personal information about Mr S when they called him and created a sense of panic by telling him there had been an attempt to defraud him. The caller gained Mr S's trust and he truly believed he was speaking to someone from his bank who was taking steps to keep his account safe.

As Mr S was then satisfied that he was communicating with Tide, I can see why he complied with the request to provide certain information, including sharing the OTP and uninstalling the app from his phone. I think that, under the circumstances, many people would have followed the instructions and complied with what they were being asked. Especially in the context of (in their mind) protecting their money from fraudsters. Indeed, we've seen many others who've acted in the same way that Mr S did.

I've noted that there's a warning in the text containing the OTP that says not to share it with anyone, and that Tide would never ask for it. But it looks like Mr S was acting quickly, so I can see how he may have missed this and focused more on the instructions he was given from someone who he thought was trying to help. It's easy to be critical of Mr S's actions with the benefit of hindsight. But I've considered he was acting in the heat of the moment, thinking he was speaking with his genuine bank and that something was wrong with K's account. I don't think Mr S's actions in that moment mean that he seriously disregarded an obvious risk.

PPT has questioned why it took Mr S several days to re-install the Tide app. It argues that it's unusual he didn't think it necessary to check his account during that time, given there was a large credit of nearly £12,000 into K's account. Mr S has told us he doesn't use the account that frequently, and this can be seen from the statements. Under the circumstances, I don't find it unreasonable that Mr S didn't install the app for a period of several days. As for the credit, it wasn't a one-off transaction – the statements show credits from that account for similar amounts every other month. Given that it was a fairly regular credit, I don't consider it unusual if Mr S didn't think it was necessary to check his account like PPT argues he should have.

Overall, I'm not persuaded Mr S showed a very significant degree of carelessness such that I think he acted with gross negligence. I recognise that PPT had some concerns after Mr S subsequently reported receiving a call from someone pretending to be from Tide. Regardless, I find that it ought to have refunded K's loss much sooner – and I recognise the inconvenience that's been caused to K by not having

this money back quicker. So, in line with the investigator's recommendation, I also intend awarding £200 to reflect K's non-financial losses.

I invited further comments from both parties.

Mr S said that although his phone provider didn't provide inbound call data as part of the subject access request, he was informed that it could be provided if the request came from the police. He also said that the only credits received in K's account were from a particular company, with whom he had a close working relationship. Therefore, there was no reason for him to be concerned about being paid.

PPT made several comments which it has asked me to consider. I've summarised these below:

- The decision revolves around the fact that Mr S didn't take the necessary steps to initiate the payment and didn't consent to anyone else doing so. PPT argues that disclosing the OTP is the necessary authorisation to add a new device to Apple Pay and without this the card can't be activated on a payment wallet.
- Providing the OTP to a third party is a breach of Tide's terms and conditions and can be considered as disregarding a red flag.
- The comments in the decision (relating to Mr S's actions) are 'very opinionated' and it's easy to make them with the benefit of hindsight. But PPT couldn't have been aware that Mr S was being scammed at the time.
- PPT has been asked to pay £200 compensation for distress and inconvenience, but a business can't suffer distress or inconvenience.
- The log-in IP addresses for February and March 2022, when the disputed transactions took place, show that the same device model was in use for the whole period. And the same device accessed the Tide app from different IP addresses, one of which PPT has assumed was Mr S's home or business WiFi. It has questioned the likelihood that Mr S's phone and the fraudster's phone were of the same make and model. And why would the fraudster have used Mr S's home or business WiFi unless they had legitimate access to it.

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 thank both parties for their response to my provisional decision which I've carefully considered. Having done so, I see no reason to depart from my provisional findings. I don't think it's necessary for me to address every point that PPT has made, but I'll address the key comments.

To consider the payments authorised, the PSRs explain that Mr S must have given his consent to the execution of the payment transactions – and that consent must be in the form, and in accordance with the procedure, agreed between him and Tide. There's no other plausible or persuasive explanation for how someone could have finished setting up Apple Pay without Mr S's involvement. But that's not to say that he understood what his actions meant. Given our experience with dealing with similar scams, I find it more likely that he was tricked into taking the steps.

But even with the conclusion that Mr S must have been involved, I'm not persuaded the disputed transactions were authorised. That's because I'm not convinced the steps to set up Apple Pay are the same as the steps to consent to the execution of a payment, which is

what the PSRs require. After all, it's not possible to make a payment by simply having Apple Pay – the PIN or biometrics must have been used again on the device with the Apple Pay token to approve the payment. I note that PPT still hasn't provided evidence of the Apple Pay token registrations for Mr S's card, as well as details of the token and mobile device that was used to make the disputed transactions.

As for PPT's point that it couldn't have been aware that Mr S was being scammed, what I've needed to decide here is whether the transactions were authorised. Given I've concluded that the transactions weren't authorised, PPT's duty of care in protecting Mr S from financial harm is not a consideration in my decision. Accordingly, I haven't commented or made a finding on whether it ought to have realised that something might have gone wrong.

PPT has questioned the compensation I said I intend to award. I want to make it absolutely clear that in my provisional decision, I haven't made any reference to the compensation being for 'distress and inconvenience' like PPT has suggested. I'm well aware that this complaint relates to a business account and the eligible complainant here is a limited company which is a legal entity separate to the person running it.

It is true that a legal entity can't experience distress, pain or suffering. And so, our service can't make an award for distress in that situation. But an error made by the firm that the complaint relates to could affect the legal entity's operations or reputation. We can and we do consider whether an award for inconvenience or damage to reputation would be appropriate when we're investigating complaints from a customer that is itself a business. More information on the different types of awards our service can make can be found on our website. In relation to this complaint, I explained in my provisional decision why I consider PPT's actions have inconvenienced K, and why £200 compensation is warranted.

Finally, I've considered PPT's arguments in relation to IP addresses, devices, and logins. I'm not sure how the arguments are relevant to the complaint I'm deciding. Essentially, PPT submits that the Tide app logins (and therefore access to the app) during February and March 2022 couldn't have been carried out by anyone other than Mr S or someone with his permission. I don't necessarily disagree with that. But the transactions weren't carried out in the app – an Apple Pay token was used. As I've mentioned, I tried to establish whether the Apple Pay token that was used to make these transactions was registered to Mr S's phone. But despite giving PPT ample opportunity, the information hasn't been forthcoming.

I think it's also important to note that there were no logins during the period that the disputed transactions happened. So, it's not the case that Mr S accessed the app during that time and ought to have noticed the transactions.

Overall, having considered the additional responses, I haven't found any reason to depart from outcome I reached in my provisional decision.

Putting things right

To put things right, PrePay Technologies Limited needs to:

- reimburse K all the transactions disputed by Mr S (less any amount recovered, if applicable);

- pay 8% simple interest per year on that amount, from the date of the transaction to the date of settlement (less any tax lawfully deductible); and

- pay £200 compensation for the inconvenience experienced by K.

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require PrePay Technologies Limited to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S (in his capacity as the director of K) to accept or reject my decision before 29 June 2023.

Gagandeep Singh
Ombudsman