DRN-4592958

The complaint

Mr G is a sole proprietor, trading as O. He complains ClearBank Limited (Tide) is holding him liable for a payment he didn't authorise.

What happened

In early 2023, Mr G received a call from someone claiming to be from Tide. They told him there had been a fraudulent card payment attempt on his card, so they needed to cancel it and order him a new card. Mr G says he could see this fraudulent payment 'live on the app'. Unfortunately, this was a scam.

Thinking his account was at risk, Mr G directed to scan a QR code he was sent. This allowed the scammers to access his account to set up a payment. It appears Mr G was then required to take some action which allowed the payment to be made. But from what he could see, he thought he was authorising a refund for the fraudulent payment.

Mr G then saw that the payment, for almost £5,300, had been debited rather than credited. He complained to Tide as he thought it should refund him. Tide said he was liable as the actions he took had allowed the scammers to access his account. And he had completed steps on his own app to authorise the payment. Tide also said it had acted swiftly to recover the (small) balance left in the account the funds were sent on to - although it did pay £75 compensation for delays responding to Mr G's requests for updates.

Unhappy with this response, Mr G referred the matter to our service. An investigator here ultimately upheld his complaint. She concluded the payment was unauthorised as Mr G hadn't completed all the payment steps or granted someone else consent to do so. The action he had taken was on the understanding it was necessary to get a refund. She didn't think the fraud had occurred due to a failure of intent or gross negligence by Mr G.

Tide has appealed the investigators outcome. It says Mr G's actions - allowing the scammer access via a QR code, and entering an OTP - authorised the payment. It says it would agree to a 50% refund, but not 100%. It says Mr G ought to have picked up on warning signs he wasn't dealing with Tide as the call came from a hidden number; he was instructed to download remote access software to check for viruses; and it wouldn't direct a customer to move to a separate chat software to send a QR code.

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've decided to uphold it. I think Tide should fully refund Mr G for this payment. I'll explain why.

The dispute here is about whether the payment was authorised. That is relevant as, under the Payment Services Regulations 2017 (PSRs), Mr G would generally be liable for a payment he authorises - but Tide would be liable for an unauthorised payment.

As the PSRs set out, if a customer denies authorising a payment, it's down to the business to show the payment was authenticated correctly. Tide has said an OTP would have been sent and entered to add a new payee on to the account. But Mr G doesn't remember receiving one, and Tide hasn't been able to provide a log to show one was sent at the relevant time.

However, it does seem to be accepted that the remaining steps to make the payment – selecting the payee, adding the payment amount and then selecting to approve the payment – was completed. And setting aside the disagreement about the OTP code, showing that the correct procedure was followed to make the payment wouldn't be enough to show Mr G authorised it.

The PSRs further cover that authorisation comes down to whether the customer consented to the payment. And that consent must be given in the form, and in accordance with the procedure, agreed between the customer and business. What this means in practice is that if Mr G, completed the agreed steps to make a then he would have authorised it. He can also give someone else consent to complete the steps on his behalf.

Tide doesn't appear to dispute that remote access was used and that the payment was initiated by the scammer. So, it's clear Mr G didn't complete all the payment steps. While his sharing of the QR code enabled the scammers to get access to do this, he didn't do so to give them permission to go through the form and procedure to make a payment. As he has told us consistently, he thought he had to scan the QR code as part of the process to get a refund, rather than to allow a payment to be taken. Similarly, the messages I've seen suggest Mr G thought the remote access software was needed for a virus check in the wake of the fraud.

It seems Mr G's actions in making the payment were as follows: he scanned the QR code as primed/directed by the scammers. While this gave the scammers access to Mr G's account, it wasn't part of the form and procedure, nor was it done to allow them to act as an agent to make a payment on his behalf.

There is a dispute about whether Mr G entered or shared the OTP code to add the new payee. If he did, I haven't seen enough from Tide to persuade me this message would have made it clear what sharing/entering the code would do. This is bearing in mind, in particular, that the scammers had set up the payee with the name of a merchant followed by "refund". I can see why Mr G wouldn't have realised any action he took in sharing or entering the code was linked to adding a payee to send funds to. I'd also point out that there have been several occasions where Tide has told our service that an OTP code contained a warning not to share it – but the complainant has been able to show that wasn't the case. Which makes it harder to rely on its testimony on this point.

Based on Mr G's testimony, and my understanding of the payment procedure, it also appears he also selected something to allow the payment to go out. But, looking at the information Tide has provided about the payment screen, it appears the payment showed as "[merchant name] refund", with the reference "approve refund". In the context of being put under pressure, thinking his account was at risk, and expecting a refund, I can understand why Mr G completed this step. I don't think he did this in order to consent to a payment being taken, or to authorise the scammers to make a payment on his behalf. So overall, where he didn't complete the full form and procedure for the payment, I consider the payment unauthorised.

In line with the PSRs, that means Tide is required to refund Mr G unless the fraud occurred due to him failing, with intent or gross, to comply with the terms of the account or keep his personalised security details safe. I've seen no indication he intentionally failed in this respect. While his actions did enable the scammers the relevant access to initiate/make the payment, he didn't intentionally do so, as he thought he was genuinely dealing with Tide and that it was helping rectify fraud perpetrated on his account.

Nor do I think Mr G failed with *gross negligence.* While I understand Tide's argument about what it considers missed warning signs, there is a high bar for gross negligence. It would mean finding that Mr G identified, but disregarding, an obvious risk. Or showed a *very significant* degree of carelessness.

In the circumstances, I can see why Mr G believed the caller. While it's not completely clear what he was shown, he's been consistent that the caller showed information which made it appear that payments were being taken or attempted from the account. Tide says no payments were taken beforehand, aside one which Mr G has confirmed was made by him. So the scammers may have shown him falsified/manipulated screens or images. But I can still see what that would be persuaded. Our service has also seen scams where Tide card details were stolen and used to make or attempt payments, then the customer was targeted with a call like this one where the caller claimed to be Tide notifying them of the fraud.

Such a tactic understandably creates a sense of pressure and urgency. It's clear from Mr G's consistent testimony throughout that he believed he was genuinely speaking to Tide, and that it was securing his account and issuing him with a refund. In that context, I can see why the sophisticated tactics used by the scammers convinced him.

For example, it appears to me they used remote access and initiate a chat, then sent a message so it looked to Mr G that Tide was contacting him. Whereas it was actually sending a message from his account to Tide. But I can understand why the way the message was written, and would have appeared on Mr G's screen, would have made him think Tide was speaking to him through the genuine chat function.

Furthermore, the scammers set up the payee and payment reference in a way that made it look as though Mr G was getting a refund. In those circumstances, and in the heat of the moment, I can see why he didn't realise a payment would be taken by selecting to verify the payment.

On balance, I'm persuaded Mr G didn't consent to this payment. Not do I think it was made due to a failing of intent or gross negligence on his part. So I think Tide should refund Mr G for the payment (less any amount it has already credited back) – with interest, to compensate Mr G for the loss of use of the funds.

Tide also offered £75 compensation for Mr G's distress and inconvenience in handling his fraud claim. Bearing in mind I've decided Tide should refund Mr G for his financial loss, with interest, I'm not persuaded the non-financial impact on Mr G warrants a further compensation award. I consider the £75 compensation offered fair.

My final decision

For the reasons given above, my final decision is that I uphold this complaint about Clearbank Limited. To put things right, Clearbank Limited must:

- Reimburse Mr G for the unauthorised payment, less any amount it has already refunded; and

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

- Pay Mr G £75 compensation, if it hasn't already done so.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 21 March 2024.

Rachel Loughlin
Ombudsman