

## The complaint

T complains that ClearBank Limited ('Tide') won't refund money it lost in a scam.

## What happened

What T says: T has a business bank account with Tide. In March 2023, a fraudster called a family member and posed as being a representative of another bank ('A') – the family member had an account with that bank (A). The fraudster said there had been a fraud on the account with bank A and wanted to deal with it. The family member gave control of a laptop computer to the fraudster, and then logged onto the account with bank A. The fraudster then made a payment for £5,000 from bank A to T's account with Tide.

The director of T then took over the call and gave control of the laptop to the fraudster (although this may have already taken place) and logged onto the Tide account. The fraudster then said the £5,000 needed to be transferred back to the account with bank A, and he would do that for T. Controlling the laptop, four payments of £5,000 were sent to the fraudster's account with another bank ('B'). The screen of the laptop went blank, so T's director couldn't see the Tide account. T's director was sent four one-time passcodes (OTPs), which he accepted each time.

Bank A refunded the £5,000. T reported the scam to Tide at 3.11pm and Tide contacted bank B at 4.27pm. A refund of £2,878.23 was paid by bank B. So, the total loss was £12,121.77:

Date	Time	Payments	Amount
9 March 2023	2.31pm	Credit from bank A (refunded by bank A)	(£5,000)
9 March 2023	2.41pm	Faster payment to 'bank A refund'	£5,000
9 March 2023	2.43pm	Faster payment to 'bank A refund'	£5,000
9 March 2023	2.43pm	Faster payment to 'bank A refund'	£5,000
9 March 2023	2.43pm	Faster payment to 'bank A refund'	£5,000
23 March 2023		Refund from bank B	(£2,878.23)
<b>Total loss</b>			<b>£12,121.77</b>

T complained. It said the transactions were unusual and were sent to an account titled 'refund account' – which should've alerted Tide to it being a scam. T said Tide shouldn't have allowed the scammer to takeover the laptop or for the screen to go blank – that must be a fault in Tide's systems. T said Tide should refund the money.

What Tide said: Tide didn't uphold the complaint. They said:

- Tide contacted bank B and got a refund of £2,878.23.
- The payments didn't stand out as being unusual, so Tide didn't intervene and stop them.
- T's director willingly gave access to the computer to a third party – and this should have caused him to be suspicious.
- To give access to the computer was also in contravention of Tide's terms and conditions.
- It was suspicious that the contact was from someone purporting to be from another bank's fraud team – this should've been a red flag to T.
- Tide hadn't signed up to the voluntary Contingent Reimbursement Model (CRM) code; so T's complaint couldn't be reviewed under the Code.
- Tide's review of the complaint took longer than they wanted (33 day) and they offered compensation of £150 for that delay.

Our investigation so far: T brought its complaint to us. Our investigator upheld it and said Tide should refund £10,000 (the third and fourth payments), plus interest at 8% per annum. He said that while there were other, high value payments from the Tide business account – four payments of £5,000, within minutes of each other, to a new payee, and which almost drained the account were sufficiently unusual. So, while he accepted that it was OK for the first two payments to go through, the third and fourth should've been stopped by Tide.

He also said that as the Confirmation of Payee (COP) failed this should also have alerted Tide.

Tide didn't agree. They said:

- To give access to the computer to a third party was negligent.
- The argument about COP was flawed – it didn't indicate any issue with the validity of a payment.
- T's director could've seen the transactions on his mobile phone in Tide's app at any time to check what was going on – even if the laptop screen had gone blank.
- It should've been known to T that another bank's employees would never ask to access another bank's account.

Because Tide disagreed, the complaint has come to me to look at.

I then made a provisional decision which said:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I'm sorry to hear that T has lost money in a cruel scam. It's not in question that T's director authorised and consented to the payments in this case. So although T didn't intend for the money to go to a scammer, it is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case. But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Tide should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case because Tide hasn't signed up to it. But, taking into account the law, regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Tide to take additional steps or make additional checks before processing a payment in order to help protect its customer from the possibility of financial harm from fraud.

I need to decide whether Tide acted fairly and reasonably in its dealings with T when it made the payments, or whether it should have done more than it did. I have considered the position carefully.

The first consideration here is: if the payment was of a sufficient size and was out of character with how T normally used its account – then we would expect Tide to have intervened and contacted T about it. I looked at T's account – it's a business account and it's reasonable to say there were a lot of payments of a similar size on a regular basis. For example:

- £4,470 - 8 March 2023
- £2,930 – 28 February 2023
- £4,030 – 25 February 2023
- £3,514 – 21 February 2023
- £5,894 – 5 February 2023

And, as our investigator noted there were also some instances of multiple payments being made on the same day – albeit for a lower individual value.

I accept there is an argument that the payments were typical for a business account, but here – there were four payments, for 'round' amounts – and were made within minutes of each other. And they almost drained the account (the remaining balance was £3.97). So –

I'm persuaded that it is reasonable to say that while Tide may have allowed the first two payments to go through, they should've intervened in the third and fourth payments.

Tide was the expert in such matters and if they'd intervened, held the payments and contacted T, we would have expected them to ask open questions such as:

- Why are you making the payment?
- Who to?
- For what purpose?
- How were you contacted about it?
- How were you given the bank account details where the money was to be paid to?
- Have you given control on your devices to anyone else?

This would then have quickly unravelled the scam and the final two payments stopped.

Our investigator said Tide should've realised there was an issue as the COP didn't match – but I agree with Tide that it's not reasonable to expect Tide to reach that conclusion – as COP isn't supported by all banks in any case. And COP is simply a match between the payee's name and account number.

So – in the first instance, I hold Tide liable for the third and fourth payments (£10,000), less the amount of the refund of £2,878.23 - £7,121,77.

#### *Contributory Negligence:*

But that's not the end of the story here. I also considered whether T could've done more to protect itself and whether it should therefore reasonably share some of its losses. And I think it should. I say that as:

- The family member, or T's director allowed the scammer to have access to the bank accounts at bank A and at Tide - by downloading the scammer's software onto the computer. This would typically have involved clicking on an icon or link to allow this to happen. I know this possibly was done by the family member (and not T's director), but it was part of what happened here – and I must take that into account.
- The family member logged onto the account with bank A – allowing the scammer to make the payment of £5,000.
- Tide's director then logged into the Tide account for the scammer to then make the payments from the Tide account.
- T's director then authorised each of the four payments on his Tide app, or by agreeing to four OTPs on his mobile phone. While I hear his argument that the computer screen went blank, it still appears to me to be negligent to then authorise four separate payments on the app or by OTP.
- Even though the computer screen went blank, the evidence suggests that the mobile phone was still working – as it was used to authorise the payments. And so – Tide's director could've checked the bank account on the phone, but didn't.

So, I'm persuaded that these actions, taken together, mean that Tide's director (and/or family member) contributed to the losses that were suffered, and I think it's reasonable therefore that the losses are shared 50/50 with Tide. This means that I propose that Tide refund 50% - £3,560.89, plus interest at 8% per annum simple. Tide should also pay the offered compensation of £150 – which was for the delay in dealing with the complaint (but

which isn't related to the merits of this case).

#### *Recovery:*

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Tide took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. I can see that here, Tide acted quickly and managed to obtain a refund of £2,878.23 – and this action was effective, and what we would have expected to happen.

#### *Responses to the provisional decision:*

Tide agreed and confirmed the compensation hadn't been paid.

T didn't agree and said the deduction for contributory negligence wasn't reasonable as:

1. The mobile banking screen was manipulated by the scammer and so the withdrawals of £5,000 couldn't be seen. The scammer had been able to do that – so Tide's systems must be at fault.
2. The family member didn't download the scammer's screensharing software to give control but logged onto the account at bank A using a link given to him by the scammer. This was recognised by bank A when it refunded the £5,000.

I now need to consider these points and 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.

On T's point (1): I looked at the evidence provided by Tide again. They said, and showed evidence, that the payments were authorised in the Tide app (not as a OTP).

I don't see how this could've been done if the mobile banking screen had been blocked or frozen/ tampered with by the scammer. So, I'm persuaded that this was the case, and T's director did have access to the app to do that. It's also therefore more likely than not that he would've been able to see the payments of £5,000 being made via the app. Even if he couldn't, it remains the case that T's director authorised the payments in the app, which contributed to the losses. So – I discount this argument.

On point (2), even if I accept that the screen sharing software wasn't downloaded by the family member – it's not in dispute that it was then downloaded by T's director – which I think wasn't a reasonable thing to do, and it's fair for me to say that contributed to the losses.

So, having considered the points made by T's director again, my final decision is unchanged from the provisional decision.

#### **Putting things right**

The remedy is as set out in the provisional decision – to refund £3,560.89, plus interest at 8% per annum simple from the date of the payments to the date of settlement; and pay the previously offered compensation of £150 - for the delay in dealing with T's complaint.

## **My final decision**

I uphold this complaint. ClearBank Limited must:

- Refund £3,560.89, plus interest at 8% per annum simple from the date of the payments to the date of settlement.
- Pay compensation of £150.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 31 January 2024.

Martin Lord  
**Ombudsman**