DRN-4135466

The complaint

T, a limited company, has complained ClearBank Limited won't refund money lost from its account as a result of a scam.

Mr B, a director, represents T in its complaint.

What happened

T holds a Tide business account with ClearBank Limited. For ease, I'll refer to T's account with Tide throughout.

In 2022 Mr B received a call from someone (who I'll call E) stating they were from T's bank, Tide. E wanted to check whether some payments on T's account were genuine. T's account, as well as Mr B's personal account, had recently been targeted by fraudsters, so Mr B understood the urgency of the situation.

To check E was genuine, Mr B looked up the telephone number they were calling from. He queried this as it didn't seem right. E hung up and called him again. This call seemed to come from the number on the back of T's debit card.

Whilst Mr B was on hold, he called the number on the back of his card to check whether anybody could call from that number without being employed by Tide. He got the impression this couldn't happen. At the same time he tried to contact Tide through the chat function on the app. He was unable to get any response despite confirming his query was urgent.

Having carried out relevant checks, Mr B followed the instructions he was given. This involved sending all the money in T's business account to a new account that had been set up supposedly in T's name, as well as inputting the relevant code to authorise this payment. Tide had contacted T earlier in the year to confirm changed account details so Mr B wasn't completely surprised by what he was being asked to do.

Mr B immediately noticed T's account was empty. E phoned him back to confirm the account would show in his app imminently. But when Mr B checked again, no new account existed. T's funds had disappeared. He contacted Tide through the app and by email.

Tide believed the payment had been properly authorised on T's behalf. Despite admitting their customer service had not been as they'd have liked, they wouldn't refund T. They would, however, refund the small amount which they understood remained at the beneficiary bank.

Mr B brought T's complaint to the ombudsman service.

Our investigator noted Tide had not taken steps to carry out any additional checks on T's payment. They felt that the transaction was sufficiently unusual to merit either a warning or intervention. Therefore they asked Tide to refund T.

Tide didn't agree with this outcome. They believed T's account was a business account and the suggestion that they should intervene in payments of this nature would be an undue

regulatory burden.

T's complaint has been referred to an ombudsman.

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 reached the same outcome as our investigator. I'll explain why.

There's no dispute that T made and authorised the payment. Mr B believed he knew who the payment was being made to – another account in T's name, and the reasons why. At the stage T authorised the payment by inputting the relevant authorisation code, Mr B believed he was taking urgent action to keep T's money safe.

I don't dispute T was scammed but under the Payment Services Regulations 2017 I'm satisfied the transactions were authorised.

It's also accepted that Tide has an obligation to follow T's instructions. So in the first instance T is presumed liable for its loss. But that's not the end of the story.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider that Tide should:

- have been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.

- 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 (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which financial institutions are generally more familiar with than the average customer.

- in some circumstances, irrespective of the payment channel used, have taken additional steps or made additional checks before processing a payment, or in some cases declined to make a payment altogether, to help protect its customers from the possibility of financial harm.

T fell victim to a sophisticated scam. Unfortunately safe account scams – which is what this was – are not massively unusual. It's unclear exactly how E knew details about T but it's clear they did. This meant the fraudsters could tailor their approach to Mr B and make it completely believable.

Specifically they were able to spoof telephone numbers to appear as if E was calling from the number on the back of T's card.

The fraudster was also able to explain in detail how Mr B should help them make the payment and directed him to the relevant aspects on the app, including providing the QR code which allowed the fraudsters to access T's account and move the money.

Tide has confirmed they do have risk-based mechanisms in place to check unusual transactions, however, what Mr B was doing wasn't sufficiently unusual to trigger any warnings.

However I find this surprising. This fraud resulted in all of the money held in T's account with Tide being moved in one payment. That immediately strikes me as unusual. There's no indication that T was unhappy with Tide's business banking services and I'd have expected this large payment to have alerted the bank.

Mr B had also tried to contact Tide about the payment. Tide has said that as only the 'verify account' was used, they took no action. However I can see even when Mr B used the emergency button on the chat function as he realised what had happened, there was a delay in getting things sorted.

Tide could also see a new account was being set up. Although this was supposedly in T's name, I'm not convinced Tide would have been able to identify this wasn't the case. This is the result of them not being part of the industry confirmation of payee service.

As I say, safe account scams are not unusual. All banks are aware of how these operate. We expect banks to alert customers – including business customers – about so-called impersonation scams.

For these reasons I believe Tide should have issued a warning at the time £29,114.87 was being transferred. Based on the actions Mr B had already taken to check whether this was a scam, I believe any alert from Tide would have ensured he'd take immediate action to stop any payment being made.

I note what Tide has said about them only providing business accounts. However I don't believe this means they are exempt from the requirements to monitor accounts, intervene when payments are being made and alert customers to potential frauds. I note Mr B had made a large payment more than a year previously but it appears to me that the payments Mr B made were generally to an account set up on T's Tide account for transfers. This is not what happened at the time of this fraud when a new account was set up prior to all of the funds from T's account being transferred. This is a clear indicator of potential fraud.

I'm also surprised Tide suggest that Mr B should have been aware that E couldn't have been a Tide employee working from home because of the email details provided and that whatever they were doing would be in contravention of GDPR. As I have said banks are always in a better position to be aware what potential frauds are happening than their customers. And that includes business customers.

I have considered what Tide has said that Mr B would have been aware that Tide would never ask him to scan a QR code. However, I can't see that at the time this was occurring, Tide alerted Mr B of this aspect. I also agree with the points our investigator made that the use of QR codes is pretty ubiquitous so I'm not convinced that Mr B would have known.

I've reviewed what Tide did when they were alerted to the scam. They notified the recipient bank of the transfer the following morning, asking them to see whether money remained. Banks are requested to take immediate action but I also appreciate that the majority of funds were most likely moved on very quickly. Tide has confirmed they asked the recipient bank for remaining funds and issued any required indemnity notice. There's no confirmation that those funds have yet been made available to T, despite nearly a year having passed.

Putting things right

I'm satisfied that if Tide had taken action to warn Mr B or stop the payment, as I believe they should have, T wouldn't have lost considerable funds from their account.

As I believe any intervention Tide should have made would have altered what happened

here, I am going to ask them to refund T's money in full. 8% simple interest a year should be added to the amount.

There's no dispute that the customer service T received wasn't appropriate. Tide has admitted this in their final response to T. I believe a small amount of compensation – £100 – is fair and reasonable in the circumstances.

My final decision

For the reasons given, my final decision is to instruct ClearBank Limited to:

- refund T £29,114.87, minus any money already credited from the remaining funds at the recipient bank;
- add 8% simple interest a year from 1 June 2022 until the date of settlement; and
- pay £100 for the bad customer service.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 20 June 2023.

Sandra Quinn
Ombudsman