DRN-5706721

The complaint

O Ltd, represented by its director Mr D, complained because Tide Platform Limited refused to refund it for a payment Mr D made as a result of a scam. Mr D also complained about Tide's service.

What happened

O Ltd had a Tide business account. These accounts are administered on Tide's behalf by ClearBank Ltd, but as ClearBank deals with transfers and Tide with card payments, Tide Platform Limited is the correct respondent for this complaint.

On 10 May 2024, Mr D received a text which said it was from Tide. It said that a card payment had been declined, and if Mr D didn't recognise the payment, a Tide advisor would be in touch.

Mr D then received a call from someone who said they were a Tide advisor. The caller asked how much money was in the account, and Mr D told them. The caller said that O Ltd's card had been compromised and there was a transaction from someone in another part of the country. Mr D said he hadn't authorised that. The caller told Mr D they'd help prevent that going through, but that there was also another payment trying to be made, to an online money transfer service. The caller told Mr D that if he approved the payment that would reverse it.

Mr D approved the payment request on his Tide app. When he'd input the passcode, he got a message saying ''payment approved'' and at that point he thought it was a scam. He rang Tide about two payments: one for £45 to an e-commerce business and one for £4,491.99 to the online money transfer service, making a total in dispute of £4,536.99. He said that the scammer had asked him for his name and company name, and the balance on his account, but not for his card number or account number.

Tide froze O Ltd's account and issued a replacement card. It told Mr D that it would make an attempt, but it would be difficult because the online money transfer service was a payment third party, responsible for carrying out payments between parties which was equivalent to cash exchange.

At the end of May 2024, Mr D asked for the account to be unfrozen so he could make some business payments, which Tide did. On 4 June, Tide told Mr D that it had rejected O Ltd's dispute for the £4,491.99 payment because it had been 3DS verified and challenged in the app. It said it had raised a chargeback for the £45 payment.

Mr D replied that this wasn't acceptable, as he'd blatantly been scammed. He said he'd checked and the number which had called him was shown online as a fraudulent number, and how could this not be seen as proof of fraudulent activity. Tide said it understood this was frustrating but as the £4,491.99 transaction had been 3DS verified in the app, there were no chargeback rights.

On 7 October, Mr D complained. He said he didn't believe O Ltd's case had been thoroughly investigated, because he was given the decision a very short time afterwards. He said he'd provided substantial evidence including searching for the number which had called him, and he'd discovered that number had targeted other Tide customers too. He wanted a refund, and said for a small business like O Ltd, the amount stolen was a crippling amount. The loss had prevented him from making purchases to keep O Ltd running, such as buying insurance, paying bills, and restocking. He said it had also negatively affected his mental health. He said that new rules from 7 October 2024 meant that banks were expected to reimburse victims of fraud.

Tide sent its final response to the complaint on 16 October. It said it believed Mr D had been a victim of a phishing scam, where a fraudster makes someone believe they're speaking to a financial organisation. Tide said it tried to prevent such scams by having multiple security measures in place, but fraudsters were becoming more and more innovative. Tide reminded Mr D that none of its employees would ever ask for sensitive data, nor ask for a transaction to be approved on the app.

Tide's final response went on to consider the two transactions:

- For the £4,491.99 card payment to the online money transfer service, it accepted that this was the highest on O Ltd's account. But it hadn't raised concerns' as it could have been a business purchase, and it didn't believe it should have stopped the payment for any further checks. It said that what had been presented to Mr D on the app had been a payment approval, not a refund being processed. It also said that Mr D had spent at least 20 minutes on the call with the impersonator, and he'd had time to contact Tide to check whether it was a legitimate call, before he'd made the payment. Tide also pointed out that the impersonator hadn't had a caller ID, and had asked for the account balance which Mr D had provided. It also said it had no chargeback options against the money transfer service. So it didn't uphold O Ltd's complaint about this transaction.

- For the £45 payment to an e-commerce business, Tide said its adviser had closed the chat before checking for the outcome of the chargeback which Tide had sent about this payment. The payment should have been refunded, but that hadn't been done. Tide offered £50 compensation for distress and inconvenience, plus the £45 payment refund, totalling £95.

Mr D wasn't satisfied and contacted this service. He explained that the scam call had been from a number which Caller ID had said was withheld, but he thought this was standard practice because the bank for his personal account did this too. He said he thought Tide's reply had been unacceptable, because it seemed it had made no attempt to recover the money from the money transfer recipient organisation. He said Tide hadn't argued his case strongly enough with the chargeback service.

Mr D also told us that the loss had been disastrous for O Ltd as a small business. He hadn't been able to make running costs purchases for equipment, and had lost out on several contracts as a result. He also hadn't been able to renew O Ltd's business insurance, which again meant that many clients wouldn't give him work. His mental health had also been affected.

Our investigator didn't uphold O Ltd's complaint. He explained that an Electronic Money Institution (EMI) like Tide was expected to process payments which a customer authorises. Mr D had authorised the payment, because he'd believed that doing so would mean he'd recover money back which the scammer told him was being debited. So the starting point was that O Ltd would be liable. But there are some situations where this service considers

that businesses shouldn't have taken payment authorisation instructions at face value, but should have looked at the wider circumstances. So the investigator considered whether Tide should have been concerned about the payments.

The investigator noted that O Ltd had had the Tide business account for some years. The statements showed that there were regular frequent transactions, some of which were similar to the fraudulent ones. For example, nine days before the scam transactions Mr D had made undisputed payments of £1,000 and £3,085. The scam payment which Tide didn't refund had also gone to a legitimate money transfer company. Overall, the pattern and amount of the payments hadn't indicated fraud, so Tide was right not to view them with suspicion.

The investigator looked at whether Tide had acted properly once it knew the payments were fraudulent. He explained that he wouldn't expect Tide to track down the scammers or pursue the money, because often the money was moved on quickly from the account with the money transfer service. He also said that using a chargeback, which is a voluntary agreement between card providers and card issuers, wasn't likely to have been successful so we wouldn't have expected Tide to raise a chargeback.

The investigator also thought that Tide's offer of £50 compensation, for not refunding the successful chargeback for the £45 payment, was fair. He also provided Mr D with links for organisations that might help with the impact of scam on his financial and mental health.

Mr D, for O Ltd, didn't accept the investigator's View. He said:

- While the payment was technically "authorised," he only approved it because he'd been deceived into believing he was speaking with a Tide fraud agent;
- At the time, he'd believed the only way to recover the earlier transaction was to authorise it. He hadn't acted with informed consent, and the payment was only authorised under false pretences. So he didn't think this should be treated as an authorised payment;
- He believed Tide failed in its duty of care to detect a high-risk transaction involving a large sum to a remittance service which was commonly used in fraud cases.
- He said Tide hadn't recognised behaviour consistent with impersonation scams, which are increasingly well-documented. He said Tide hadn't applied any form of Customer Vulnerability or Scam Interruption process to prevent him from completing the transaction;
- He believed it was unreasonable for Tide to rely solely on 3D Secure or historical payment patterns, especially as it had been an unusually large payment to a new merchant;
- The transaction to the money transfer service wasn't consistent with his previous business account usage. He'd only used the O Ltd account to pay legitimate business vendors and contractors in the UK, and to receive payment for commercial work. He hadn't used it for personal money transfer services, and as the money transfer service was associated with high risk fraud, it should have stood out as an anomalous transaction;
- He'd reported the scam immediately, so Tide should have acted more quickly and with greater urgency;
- His mental health has suffered since the incident, and the financial losses had directly harmed his small business. He hadn't been able to meet business expenses, renew insurance, or take on new contracts, which had led to financial and reputational damage. Tide hadn't recognised or acted on this, and its attempt to recover the funds had been limited;
- He said he appreciate that the investigator had followed the Payment Services Regulations and that card payments aren't covered by the October 2024 reimbursement scheme. But he asked us to assess, rules aside, whether Tide's

actions had been fair, reasonable, and aligned with its obligations to protect customers from financial harm;
- He asked us to reconsider whether Tide met its duty of care and acted reasonably; consider the emotional and financial hardship he'd experienced; and review Tide's decision in the context of wider industry standards for fraud protection, including the expectations outlined by the FCA, UK Finance, and the voluntary CRM Code even if not legally binding.

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'm sorry to hear that Mr D was the victim of a scam, and I recognise that it would have been very upsetting.

Relevant codes and rules

The relevant law here is the Payment Services Regulations 2017. These set out what is needed for a payment to be authorised and who has liability for disputed payments in different situations. With some exceptions, the starting point is that the consumer is responsible for authorised payments, and the business is responsible for unauthorised payments.

Mr D has asked this service to review the outcome in the context of the expectations of codes and regulations even if not legally binding, and to assess ''*rules aside''* whether Tide's actions had been fair. But while this service considers cases on the basis of what's fair and reasonable, it wouldn't be right to apply regulations and codes which aren't applicable to the circumstances and timescales of any particular case. I've set out below what does and doesn't apply to O Ltd's complaint, and why the Payment Services Regulations 2017 are the relevant ones here.

The payments made by Mr D took place in May 2024. At that time the relevant scam protection framework was the 2019 Contingent Reimbursement Model (CRM). This was a voluntary code, to which some financial organisations signed up, with the aim of providing customers with increased protection from authorised push payment (APP) scams. Tide wasn't among the organisations which signed up to this. So the CRM Code isn't applicable to O Ltd's complaint.

The Payment Systems Regulator (PSR) set out new rules from 7 October 2024, about reimbursement of victims of authorised push payments, and these applied to all payment service providers, including Tide.
- Mr D's payments were made in May 2024, so wouldn't be covered by these new rules – because they weren't retrospective.
- Even if the new rules had been in place, they wouldn't have applied to O Ltd's complaint. That's because only Faster Payments and CHAPS transfers between banks, and internal transfers within the same bank, are eligible to be considered for reimbursement under the rules. Mr D made the payments using his card.

So the CRM Code and the October 2024 regulations can't determine the outcome for O Ltd's complaint, and the relevant regulations for O Ltd's complaint are the Payment Services Regulations 2017.

The Payment Services Regulations specify that authorisation depends on whether the payment transaction was authenticated correctly, and whether Mr D, or someone acting on

his behalf, consented to it. Consent must be in the form and in accordance with the procedure agreed between the consumer and the payment service provider. In other words, consent is provided when the consumer completes the agreed steps for making a transaction or allows someone else to complete some or all of them.

To establish the agreed form and procedure, I've reviewed the terms and conditions of O Ltd's account with Tide. Section 13.2 of Tide's terms and conditions says:

''You can provide your consent to a Payment Order by using the identified method for giving consent indicated within the Tide Platform interface that you are using, typically a 'Make Payment' button and a verification of the Payment Order, including a fingerprint scan or the submission of a code, as required by the Tide Platform. Payment Orders cannot be instructed by phone, paper-based instruments or other means.''

Authorisation of the payment

Tide sent us screenshots to show the process, and what Mr D would have seen. After entering his security code, the next screen is headed ''Verify payment.'' This gives the amount of the payment, then ''Payment initiated …'' with the date and time. It then says ''you have 5 minutes to approve this payment once it has been initiated.'' There are options at the bottom of that screen to ''Approve payment'' or ''Reject payment.'' If the consumer selects ''Approve payment', the next screen requires the security code to be entered again before the next screen shows ''Payment approved.''

I accept that Mr D was tricked, by what the scammers said he'd be doing, and no doubt he was acting out of panic. It's not clear how the scammers obtained Mr D's card details, but it appears the scammer entered Mr D's card details onto the website to make the payment. Mr D didn't agree to this payment instruction in terms of what he understood to be happening – but he did confirm the payment in his app. I appreciate that the scammer was hurrying Mr D, but I consider that Tide made it clear from the screens presented to Mr D that he was approving a payment rather than cancelling one which had already been made. Mr D had made other card payments on his Tide account, so he'd have been used to the format of authorisation which the system showed. So I think Tide set out sufficiently that what he was being told to do was to authorise a new outgoing payment, not to reverse one which the scammer told him would be blocked or reversed by what Mr D was being asked to do.

I understand that Mr D was tricked into making the payment, but that's not a consideration under the Payment Service Regulations in determining whether the payment was authorised. So, it was reasonable for Tide to treat the payment as having been authorised. This means it isn't obliged to provide a refund.

The two different payments

Mr D disputed two card payments. They're different in several ways, including where they went to, and the position about a refund.

The £45 card payment to an e-commerce business was dealt with by Tide as a chargeback. Tide received the outcome, that the merchant didn't defend the chargeback, on 15 June – but it failed to refund him at that point. Tide's final response letter on 16 October 2024 offered to refund the £45 plus £50 compensation for distress and inconvenience. From the evidence before me, I can't see that this has been paid. I find that Tide was at fault for not refunding O Ltd promptly so I will order Tide to do so below, if it has not already done so.

The more complex payment is the £4,491.99 payment which was the result of the scam and was sent using a money transfer business which specialises in international payments. I'll explain this below.

Could the £4,491.99 payment have been recovered?

I appreciate that Mr D feels that because he reported the scam promptly, it should have been possible for Tide to have attempted to reclaim it. So I asked for more information from the third party organisation, the money transfer business.

When money is sent internationally through a money transfer business which specialises in international payments, the transfer is usually funded by a card payment from the consumer's bank, with the funds pulled through by the money transfer business. The money transfer business then sends it on to the end payee in another financial organisation. Money sent in this way doesn't go to anyone's account with the money transfer business. It just passes through the money transfer organisation on the way to the recipient organisation, usually very quickly. Depending on the type of transfer selected by the money transfer business and the end payee, the authorised card payment and the international transfer often take place almost simultaneously, or within a few hours.

The money transfer service showed us that the funds were transferred out to the recipient at 14:20, just a couple of minutes after the payment was authorised. Even though Mr D contacted Tide quickly to report the scam, there wouldn't have been enough time to stop the money transfer service from processing the transfer. And once sent, international payments are far less likely to be recovered, given the different obligations and rules that exist abroad - though Tide couldn't have instigated that recovery action anyway, as it didn't know the end destination details.

In theory a chargeback is one possible route to reclaim card payments. It does sometimes work, as it did with the disputed £45 payment to a different merchant. But chargebacks would never succeed in the circumstances of the £4,491.99 payment to the money transfer business. That's because it's not the same as buying goods, or sending to someone's account within the money transfer business. All the money transfer business does is provide a service for whoever initiates the payment. In this case that was the scammer who provided O Ltd's card details, and the amount it wanted to claim, to the money transfer business. The money transfer business then fulfilled its responsibilities by issuing the payment request, which Mr D authorised as a result of what the scammer told him, and passing the money to the recipient organisation. The money didn't end up in any account with the money transfer service – it was just processed on its journey by that service. This means that a chargeback wouldn't have worked for the larger payment.

Should Tide have intervened when the payment was attempted?

Payment service providers like Tide have a responsibility under the Payment Services Regulations 2017 to carry out customer payment requests without undue delay, but they have to balance this with appropriate security measures. I've considered whether the £4,491.99 payment should have alerted Tide's security systems and been blocked until Tide could make further checks with Mr D.

I recognise that this was the largest transaction on the account in a while, which combined with the fact that it was going to a company specialising in international payments meant it carried some additional risk. That's because Tide wouldn't have known the end destination for the funds, and international payments are often not recoverable. But the money was going via an FCA-regulated payment service provider, which would have provided some

reassurance to Tide. Card payments also carry some protection, though unfortunately that didn't assist in this case. Both of those factors, from Tide's perspective, would have mitigated the risk involved to an extent. A business making a payment to somewhere abroad isn't inherently suspicious either. So, while I appreciate O Ltd hadn't sent money internationally before, I don't think doing that ought to have automatically led Tide to conclude it was likely fraud, and be concerned enough to refuse the payment instruction.

I've also thought about whether the size of the payment should have concerned Tide. Expected use on a business account would generally involve higher value transactions, and more frequent payments to new payees, than typically seen on personal accounts. One-off larger payments also don't necessarily indicate fraud. Looking at O Ltd's account history, I can see a payment for over £3,000 made ten days prior to the £4491.99 one, as well as regular payments each month (to O Ltd's director) for over £1,000. So the account frequently transacted in the low thousands, and going back further in time there's evidence of some larger one off payment for around the same amount as the disputed one (for example, there had been payments for just over £4,000 in April 2023, for £3,000 in July 2022, and a payment of £4,500 in 2022). There were card payments as well as faster payments, so a card payment wasn't unusual either. Taking all of that into consideration, I don't think the payment in question looked sufficiently out of character compared to prior account activity to have prompted an intervention from Tide. The disputed transaction also didn't drain the account (often an indicator of an 'impersonation scam' like the one involved here), with around £2,000 left in it once sent – meaning an obvious scam pattern didn't form at any point.

So, overall, I don't think there was enough here to indicate to Tide that it needed to step in and block the payment. That's because although it was the first international payment on the account, and the largest transaction for a while, those on their own wouldn't have sufficiently indicated that O Ltd's payment was probably scam-related. So I can't say that Tide should have blocked the payment, or fairly conclude that it should have prevented the loss O Ltd sadly incurred at the hands of fraudsters.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask O Ltd to accept or reject my decision before 17 February 2026.

Belinda Knight
Ombudsman