DRN-4541670

The complaint

A company which I'll refer to as C complains that ClearBank Limited ('Tide') won't refund a transaction that C didn't make or authorise.

Mr K, who is a director of C, brings this complaint on C's behalf.

What happened

C holds a business account with Tide.

What Mr K says

On 19 August 2022 Mr K received a text message in his usual Tide thread providing him with a one time passcode (OTP) for a payment of £955.25 to a well-known retailer. The message said that if it wasn't Mr K, he should call a phone number provided. Mr K called this number and the person who answered said they were from Tide and took Mr K through security. Mr K said that he hadn't made the payment to the retailer. He was told the transaction would be cancelled but another person had access to his account. The caller talked about malware and sent an email with a "*Malware screening*" code to scan.

Mr K says the caller said a new sort code and account number would be provided and guided him to authorise this to ensure the other person couldn't access his account. He says he thought the account details were genuine as the account appeared to be in his name, and that he thought he was protecting his account rather than making a payment.

After the call Mr K checked C's account and saw that £10,555.29 had been transferred to an account he had no knowledge of. He became concerned and contacted Tide.

What Tide say

Tide didn't agree to reimburse C. It said the transaction was authorised and couldn't have been made without his involvement. Tide explained it hasn't signed up to the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) and that it had done what it could to try to recover C's funds.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld. She said that Mr K, on behalf of C, authorised the transaction when he approved the payment in the app. She went on to consider whether the payment was so unusual and out of character for C's account that Tide ought reasonably to have intervened. Had it done so, the investigator thought the scam would have been uncovered. She didn't think Mr K, on behalf of C, should be held partially responsible for the loss and noted the message Mr K received was in the genuine Tide thread and Mr K was led to believe he was taking steps to protect C's account.

Mr K accepted the investigator's findings but said that the £67.08 balance in C's account was a payment Tide made to him as part of a premium rewards package and the actual balance of the account after the transaction was zero.

Tide didn't agree with the investigator. In summary, Tide said:

- There were high value transactions from C's account in the period leading up to the scam. In particular, there was a £9,750 transaction in April 2022. This demonstrates that from time to time, higher value payments are made from a business account.

- Whilst payments draining an account can be a red flag, Tide can't pause all payments based solely on this factor.
- The investigator's view was inconsistent. She said that the payment approval screen should have prompted Mr K to realise he was making a payment but also said he couldn't have done more to prevent the scam.
- The warning provided to Mr K together with other screens he saw should have caused him significant concern and led to him terminating the call with the scammer.

The complaint was passed to me, and I issued two provisional decisions. In the first, I said Mr K should share responsibility for his loss. After carefully considering Mr K's response, I issued a second provisional decision on 25 March 2024 in which I upheld Mr K's complaint in full.

Tide didn't agree with either of my provisional decisions. I have summarisred the main points it raised below:

- It didn't think it should have intervened for the reasons already provided (which I have set out above).
- The high value transactions to an account in Mr K's name should be taken into account.
- Mr K approved the transaction even though there were several notifications that a new payee was being created and a payment was being made.
- Mr K has proved himself to be an unreliable source of information and Tide has provided evidence that contradicts what he has told this service.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Where there is a dispute about what happened, and the evidence is incomplete or contradictory, I've reached my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence.

The relevant law here is the Payment Services Regulations 2017. Broadly speaking C is responsible for any payments that Mr K has authorised on C's behalf (either by making them himself or allowing someone else to) and isn't responsible for unauthorised payments, except in more limited circumstances.

Mr K believes that because he didn't intend C's funds to go to a scammer the transaction is unauthorised, but this is incorrect. Mr K authorised the payment by giving the one time passcode (OTP), and this is the case irrespective of the fact he didn't intend C's funds to end up in the account of a scammer. When Mr K reported what had happened to Tide on the day of the scam, he said he thought he had been duped into transferring all his money after being told his account was compromised.

Given what Mr K reported to Tide, it reached out to the firm that received C's funds to try to recover them, which is the correct process to follow in the case of an authorised push payment (APP) scam. If Mr K had reported an unauthorised transaction the process would have been different.

The evidence provided by Tide also supports the fact the transaction was authorised. The code sent to Mr K by email allowed the scammer to access his account, but the faster payment could only be completed when he provided the OTP sent to Mr K's registered mobile device. I have seen the message sent by Tide when the OTP was provided. It said:

"*Tide will NEVER call you asking you to move funds. If you did not initiate this request or have received such a call, please contact us via the Tide App. Please enter One Time Passcode [ ] to complete set up of your new Payee with account ending [ ]*".

The OTP was entered, and I'm satisfied Mr K provided it.

Having decided that Mr K, on behalf of C, authorised the transaction I've gone on to consider whether Tide acted reasonably in processing it. There is an obligation on Tide to be on the lookout for, and to protect its customers from, potentially falling victim to fraud or scams. This includes monitoring accounts and identifying suspicious activity that appears out of character. In situations where potential fraud is identified, I would expect Tide to intervene and attempt to prevent losses for the customer.

I've reviewed C's bank statements for the twelve-month period before the scam transaction to establish if it was unusual and out of character. On balance, I agree with the investigator that it was. The previous transaction of £9,750 in April 2022 was to Mr K's own personal account. It was to an established payee that numerous payments had been made to and is a normal transaction from a business account. Excluding regular transfers to Mr K's account, there were no faster payments above a few hundred pounds and a few card payments for around £2,000. So, I'm satisfied that a transfer of £10,544.29 to a new payee which almost drained C's account was so unusual and out of character that Tide ought reasonably to have taken additional steps to protect C's account. I'm not satisfied that the warning provided to Mr K when he set up a new payee went far enough as it didn't cover the essential features of a safe account scam or bring it to life. The warning was also provided at the stage Mr K set up a new payee rather than during the payment journey.

I've thought about whether C should bear any responsibility for its loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint. Having done so, I don't consider Mr K, on behalf of C, should share responsibility for the loss and will explain why.

It's clear that the fact Mr K received a text message in his usual thread from Tide was the main reason Mr K thought what he was being told was legitimate. He says he didn't know it was possible for a scammer to do this and I can understand how persuasive the text message would have been. He also received an email that appeared to him to be legitimate. I'm also mindful that at the time the scam took place Mr K was persuaded he needed to act quickly to safeguard C's funds, which was a deliberate ploy by the scammer. In the circumstances, I can understand why Mr K didn't take as much notice of the new payee warning as he might otherwise have done. And, as I said above, the new payee warning didn't bring to life the scam so that it resonated with Mr K, so I don't consider he acted negligently in moving past it.

Finally, I've considered whether Tide did enough to recover C's funds once Mr K notified it of the scam. I've seen evidence which confirms that the funds were removed from the receiving account shortly after they were credited and before Mr K reported the scam to Tide. So I'm satisfied Tide couldn't have done anything more.

Putting things right

Overall, I'm satisfied that this was a sophisticated scam, and that C should be reimbursed as set out below.

My final decision

I uphold this complaint and require ClearBank Limited to:

- Refund £10,555.29; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of loss to the date of settlement.

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

Jay Hadfield
Ombudsman