DRN-4088949

The complaint

A limited company, which I'll refer to as B, complains that ClearBank Limited ('Tide') won't reimburse all the money it's lost to a scam.

Mr and Mrs B, who are directors of B, bring the complaint on B's behalf.

What's happened?

B has fallen victim to a safe account scam.

Mrs B has said that, on 14 June 2022, she received a call from someone pretending to work in Tide's fraud squad ('the scammer'). The scammer called from a telephone number which matched the one on the back of B's Tide bank card, they knew her name and they were aware of the current balance on B's account. They said that B had been the victim of fraud. They asked Mrs B to confirm a number of transactions as genuine on B's account, which she did, and eventually they came across a transaction which Mrs B did not recognise. The scammer told Mrs B that B's account was at risk and B's funds needed to be moved to a new account to protect them. She received an email from Tide's genuine email address containing a QR code which she scanned so that B's money could be moved out of the compromised account. Then, the following faster payments were made from B's account to several different accounts held with Tide and other financial institutions:

Date of transaction	Time of transaction	Amount of transaction
14 June 2022	18:59	£30,000
14 June 2022	19:02	£40,000
14 June 2022	19:06	£20,000
14 June 2022	19:07	£50,000
14 June 2022	19:14	£50,000
14 June 2022	19:17	£50,000
14 June 2022	19:27	£30,000
14 June 2022	19:31	£25,726.28

The scammer set the payments up and Mrs B approved them.

The payments drained the available funds in B's account.

Shortly after the payments had been made, Mrs B realised that something was amiss and reported the matter to Tide.

Tide didn't manage to recover any funds from the receiving accounts, but it said that it could've recovered almost £100,000 of B's funds if it had acted quicker. So, it offered to refund the amount it should have recovered, with interest, and pay B £200 compensation to recognise its delays in investigating this matter.

In referring a complaint about Tide to this Service on B's behalf, Mr and Mrs B have explained that the scam has left B facing severe financial difficulties, and only able to trade on a very small scale. B's staff have been let go because of an inability to pay them, and B has been unable to cover essential bills. There is a fear that B will go under because of what has happened.

What did our investigator say?

Our investigator thought that the first £30,000 payment should've triggered Tide's fraud detection systems, due to its value and destination when compared with historic account activity. She said that Tide should've intervened with the payment and, if it had, it's likely the scam would've been unveiled and all of B's losses would've been prevented. So, she recommended that Tide reimburse B's full financial loss, with interest, and pay £2,000 compensation to recognise the financial and reputational damage B has suffered.

Tide did not accept our investigator's recommendations. In summary, it said:

- Businesses are expected to make large and regular transactions, including to new payees. Business customers have a reasonable expectation that they can transact freely and without undue friction. Tide can't be expected to routinely stop payments simply because they are larger than payments previously made, or because they involve a new payee. Commercial customers will commonly make large payments to new payees, and Tide has to take a risk-based approach so as not to cause a significant backlog in payment processing.

- The faster payments made as a result of the scam were not immediately objectively unusual or suspicious, and it doesn't agree that there was a reason to intervene with the payments until at least the second £50,000 transaction. B regularly makes payments of £10-20,000 to new payees and makes multiple payments on the same day. B also made a genuine £50,000 payment eight months before the scam. So, the disputed transactions were not necessarily unusual and there could be a number of reasons for such activity. Tide accepts that B's account was drained and that this was suspicious in hindsight but says that it wasn't drained until the later payments were made.

- B should have had policies and processes in place to protect itself from fraud, and it failed to adequately protect itself. There was information about safe account scams on Tide's website at the relevant time, and B should've been keeping itself abreast of relevant information about fraud and scams.

- B ignored certain clear warning signs which could have prevented the scam and should be held at least partially responsible for its loss. It's implausible that Tide would've required Mrs B to go through such a convoluted process to transfer B's funds out of a compromised account – it could've paid one large amount out of the account rather than making several smaller payments of differing amounts. Mrs B didn't challenge or question the scammer or exercise appropriate caution. She had suspicions but continued regardless.

- In relation to compensation, B is a business and can't suffer distress.

B's complaint was passed to me to decide.

My provisional decision

I issued my provisional decision on 3 March 2023. I'll set out what I said below.

It's not in dispute that B has been defrauded. It's also common ground that the payments made to the scam were 'authorised'. Mrs B has said that the scammer set the payments up and she approved them. So, even though she didn't intend the payments to go to a fraudster, the payments were 'authorised' under the Payment Services Regulations. Tide had an obligation to follow the payment instructions it received, and B is presumed liable for its loss in the first instance. 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 banks 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.

I've looked at B's account statements and I can see that it was normal for several transactions to be made on the same day. Most transactions made were of relatively low-value, but payments of £1-10,000 were not unusual. Five payments for over £10,000 were also made in the months leading up to the scam, including a payment of £21,750. So, I don't think it's reasonable to expect the first £30,000 payment to the scam to have triggered Tide's fraud detection systems because I don't consider that payment to have been particularly unusual or out of character in consideration of the normal account activity. Tide needs to strike a balance in the extent to which it intervenes in payments, against the risk of unduly inconveniencing or delaying legitimate payment requests.

But, when the second payment to the scam for £40,000 was made a few minutes after the first payment, I think it's reasonable to expect Tide to have recognised that B was at risk of harm from fraud and intervened. Although irregular payments out of B's account for over £10,000 were not out of character, multiple high-value payments in quick succession had not occurred before in the months leading up to the scam and were unusual. I consider that, by the time the second high-value payment was instructed, a few minutes after the first high-value payment, the activity on B's account stood out as sufficiently suspicious to expect Tide to have asked B some questions about it.

I wouldn't expect a bank to interrogate its customers about unusual payments. But it doesn't appear that Mrs B was being coached by the scammer, so I think she would've spoken freely to Tide. If Tide had asked her some questions, it's likely she would've explained that she was approving transfers of money out of B's account to a 'safe account' on Tide's fraud squad's instructions after being told B's account had been compromised and, with its industry knowledge of fraud and scams, Tide ought reasonably to have realised that a safe account scam was underway. If Tide had done enough here, I think the second payment to

the scam, and all subsequent payments would've been prevented. So, it's fair and reasonable for Tide to reimburse all the payments made to the scam from the second payment onwards.

I've thought about whether there are any other reasons Tide should refund the first payment to the scam, and I think there are. The payment went to another account held with Tide, and Tide has provided this Service with the relevant account statements. I won't discuss what they show in detail here but, considering the account activity, which I think was suspicious, it's reasonable to expect Tide to have blocked the account before B's money was transferred out of it. If it had done so, B's money could've been recovered.

Considering everything, I think the fair and reasonable outcome is for Tide to reimburse all the money B lost to this scam, along with interest at the account rate from the date of loss to the date of settlement (because, from what I've seen, I think it's likely that B's funds would've remained in its account but for the scam).

In the circumstances, I don't need to go on to consider whether Tide acted with care and urgency in trying to recover B's money. Tide says it could've acted quicker, and I accept that.

I've thought about whether B should bear some responsibility for its loss by way of contributory negligence, but I don't think it should. B fell victim to a sophisticated scam. From what Mrs B's said, the scammer knew personal details about her and they had knowledge of B's account balance and genuine transactions that had occurred on B's account. Tide's number was spoofed, and Mrs B received an email that appeared to come from Tide's genuine email address. Overall, she was convinced that she was talking to Tide and taking action to protect the funds in B's account. I can understand why the fraud went undetected by Mrs B.

I don't agree with Tide that B should've possessed any special knowledge about safe account scams, and I don't think it's reasonable to expect B to have gone looking for information about safe account scams on Tide's website. From what I've seen, B is a relatively small business. I'm not persuaded that B can reasonably be expected to have had an understanding of this type of fraud or how to protect itself against it, and I haven't seen any evidence to suggest that Tide attempted to impart its industry knowledge of safe account scams in an impactful way.

Tide has said that Mrs B ignored clear warning signs and proceeded with the disputed payments despite her suspicions. It's also pointed out that Mrs B realised something was amiss shortly after the payments had been made, and it's suggested that she could've done more whilst on the phone to the scammer to protect B. Mrs B has explained that she was suspicious at one point during her conversation with the scammer, but her mind was put at rest when she saw that the number the scammer had called her from matched the number on the back of B's Tide bank card. I don't think that's unusual in this type of scam, or unreasonable. There were undoubtedly some 'red flags' Mrs B could've picked up on, and more she could've done to protect B from financial harm, particularly with the benefit of hindsight and/or with more time to think. But the scam took place over a short period of time. In the heat of the moment, in a pressured situation, I don't think it's unreasonable that Mrs B didn't realise B was being defrauded.

Finally, I have considered whether it would be fair and reasonable to require Tide to pay B some compensation. I'm very sorry to hear of the negative effects this scam has had on B. It is clear, from what Mr and Mrs B have said, that B is in financial difficulties and struggling to survive as a result of the scam. Ultimately, B's loss was caused by the cruel and callous acts of a fraudster. But, if Tide had prevented the scam from the second payment onwards as I'm satisfied it ought to have and/or of it had reimbursed B in a timely manner, then the negative

effects of the scam would've been lessened.

It is true that a business cannot suffer distress, but a business can suffer inconvenience and reputational damage. And, in the circumstances, I think it's fair for Tide to compensate B for the additional impact it's caused in terms of finances, operations and reputation. I think a total award of £1,000 is fair in the circumstances.

Responses to my provisional decision

Mr and Mrs B accepted my provisional decision on B's behalf. But Tide did not. In summary, Tide said:

- Tide doesn't invigilate, and is not required to invigilate, customer interaction with mobile or web applications in real time as part of its suspicious activity monitoring processes.

- Commercial customers, like B, are much more likely to transact large amounts within a short space of time and to multiple payees – this is not exceptional behaviour. Tide wasn't required to intervene with the second payment. The payments became unusual at a much later stage.

- As is standard in the financial services industry, Tide monitors customer accounts for suspicious activity. What amounts to suspicious activity is a complex risk-assessment conducted by automated machine-learning processes. This risk-assessment considers, amongst other things, transactions on the account, but transaction patterns will often not be fully determinative of whether there is suspicious activity. B regularly made high-value transactions. My provisional decision doesn't explain why a £40,000 payment should've triggered when B regularly transacted multiple amounts on one day and had previously made higher-value payments.

- Tide couldn't reasonably have prevented B's loss on the receiving side.

- Tide has uncovered new data which shows that the payment process during the fraud event was complicated, and different to what Mrs B was used to. She ought to have realised that the payments weren't genuine, causing her to cease communication with the scammer, before the first disputed payment. Numerous, separate steps were required to enable the scam, including:

    - Mrs B logged into her mobile application over 20 times during the fraud event – there's no evidence to suggest she checked for impropriety, which would have been visible to her, on any occasion.

    - Mrs B scanned QR codes received by email, to give the scammer access to B's account, on several occasions. Mrs B will have been familiar with the use of QR codes to log onto Tide's web application. But she will never have experienced QR codes being used in this manner or with such frequency and will never have received QR codes by email from Tide to facilitate web application log-in access. This should've been concerning to her.

    - Mrs B shared one-time passcodes ('OTPs') she received via text message with the scammer to set-up each new payee (the last four digits of the new payee account number would've been displayed in the text messages) and authorise each transaction. Sharing security details in this way is a breach of B's account terms and conditions. It's also an unusual step to take - genuine banks would never ask for OTPs to be shared, and it's not something Tide

would've asked Mrs B to do previously.

    - Mrs B approved all payments in her mobile application – six of which were unsuccessful, including the first four attempted payments. She would've seen the payee name and payment amount when doing so. It should've been a red flag that several transfers to different payees were being made instead of one transfer to one new account in the name of B.

- The interaction between Mrs B and the scammer lasted around an hour and there were lots of separate calls, rather than one continuous conversation. There was a half-hour period between the first QR code being scanned and the first successful payment. The timeframe is suspicious. If B's funds were imminently at risk, why would it take a genuine bank so long to carry out the simple task of moving B's funds? It's also implausible that a genuine bank would move the funds out of its customer's account in several payments of random amounts, rather than one lump-sum.

- Mrs B has said that her mind was put at rest by number spoofing, but engagement with the scammer had been ongoing for at least 30 minutes prior to the first successful payment. In that time, she'd been sent several QR codes and there had been four unsuccessful payment attempts. Any initial comfort Mrs B had gained from seeing a familiar telephone number should've been outweighed in the first 30 minutes of Mrs B's interaction with the scammer, prompting her to discontinue the conversation.

- It's implausible that Tide would've had to ask Mrs B to give it access to B's account. It's also implausible that it would've lost access to B's account and sent new QR codes to regain access on so many occasions.

- The emails Mrs B received from the scammer did not come from an email address which matched, closely resembled or mimicked Tide's.

- Mrs B continued to approve payments out of B's account despite having suspicions about what was happening.

- B is a long-standing customer of Tide's. Mrs B ought to have known how payments are processed and how Tide usually contacts its customers.

Mr and Mrs B's further comments

- The scammer knew Mrs B's name, and they knew about genuine transactions on B's account and B's account balance. Mrs B assumed that only Tide would have access to that information. The scam call came from Tide's genuine telephone number. The emails Mrs B received appeared to come from Tide's fraud department's email address. The OTPs Mrs B received were sent by Tide, and she's received these text messages before when setting-up new payees. Mrs B approved payments to payee names she expected to see and didn't notice any details about the account numbers. Mrs B didn't question the scammer as she thought she was talking to Tide on Tide's telephone number, receiving emails from Tide's fraud department's email address, receiving text messages from Tide and approving payments in her mobile application that Tide had set-up. Mrs B became suspicious towards the end of the fraud event but was reassured by the sophistication of the scam.

- The mobile and internet signal in Mr and Mrs B's property is poor. There were several calls between Mrs B and the scammer because her phone signal kept

dropping. She was told that the poor connection was the reason why she had to keep scanning new QR codes, demonstrating how secure the bank is. The poor connection was frustrating and added to the stress Mrs B was feeling – she was very worried that B's money was unsafe and Tide's efforts to protect it were being hindered.

- Mrs B thought that the first four failed payments were as a result of the poor connection in her property.

- The scammer instructed Mrs B to delete the emails she'd received from them after scanning the QR codes to protect B from further fraud.

- Mrs B realised she'd been scammed when all of B's money had been moved out of its account, but she couldn't see a new account with B's funds in it on her internet banking.

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.

For all the reasons I've already set out in my provisional decision, and considering my findings below, I'm still persuaded that the fair and reasonable outcome is to uphold this complaint and instruct Tide to reimburse B's full financial loss, with interest, and pay £1,000 by way of compensation.

I consider that Tide's response to my provisional decision falls into three broad categories: intervention, receiving account and contributory negligence. I'll address each category in turn.

Intervention

Tide has said that the 2017 British Standards Institution code for protecting customers from financial harm as a result of fraud or financial abuse ('the BSI code') doesn't apply in this case. The BSI code codified what should already have been good industry practice and, as Tide has pointed out, it is standard in the financial services industry to monitor customer accounts for suspicious activity. I consider this to be good industry practice and I'm pleased to see Tide's confirmation that it does monitor accounts in the manner I'd expect to see.

I accept the theory that commercial customers, like B, are much more likely to transact large amounts within a short space of time and to multiple payees. But consideration of what is exceptional behaviour for a particular customer – commercial or otherwise – is subjective. Not every commercial customer operates their account in the same way. Multiple and/or high-value transactions to new payees may well be exceptional behaviour for some businesses (particularly smaller businesses) when it isn't for others.

As I set out in my provisional decision, it was usual for B to make several transactions on the same day – mostly of relatively low-value – and the occasional higher-value payment wasn't unusual. That is why I don't think it's reasonable to expect the first £30,000 payment to the scam to have triggered Tide's fraud detection systems. I don't consider that payment to have been particularly unusual or out of character in consideration of the normal account activity.

But, when the second payment to the scam for £40,000 was made a few minutes after the first payment, I think it's reasonable to expect Tide to have recognised that B was at risk of harm from fraud and intervened. Although irregular higher-value payments out of B's

account were not out of character, multiple high-value payments in quick succession had not occurred before in the months leading up to the scam and were unusual. Also, rapid, high-value transactions are often characteristics of scams, and safe account scams in particular – and I think Tide ought to know this. I consider that, by the time the second high-value payment was instructed, a few minutes after the first high-value payment, the activity on B's account stood out as sufficiently suspicious to expect Tide to have asked B some questions about it. And, if it had, I remain satisfied that the second payment to the scam, and all subsequent payments would've been prevented.

Tide's evidence that there were four unsuccessful payment attempts prior to the first disputed payment adds weight to my finding that Tide ought to have realised something was amiss by the second disputed payment and intervened to prevent the scam. By this time, there had been four unsuccessful payment attempts and two high-value payments out of B's account, all in quick succession.

Receiving account

Tide has said that it couldn't reasonably have prevented the loss of the first disputed payment on the receiving side, but I respectfully disagree. Tide hasn't provided any new evidence or information on this point, and I remain satisfied that it should fully refund the first disputed payment for the reasons I've already explained. I consider that the receiving account activity was suspicious – a high-value payment credited the account within a few days of account opening and was quickly disbursed – and it's reasonable to expect Tide to have blocked the account to carry out further checks before B's money was transferred out of it. If it had done so, B's money could've been recovered.

Contributory negligence

I've carefully reconsidered whether B should bear some responsibility for its loss by way of contributory negligence in light of the new evidence Tide has provided, but I still don't think it should.

B fell victim to a sophisticated scam. From what Mrs B's said, the scammer knew personal details about her and they had knowledge of B's account balance and genuine transactions that had occurred on B's account (the scammer most likely gathered the relevant information through a phishing or smishing attack based on what I know about these types of scams). Mrs B's explained that she thought only Tide would have access to that information. Tide's number was spoofed, and Mrs B received emails that appeared to come from Tide's fraud department (I appreciate that she didn't check this but looking at the email address concerned and considering that Mrs B was already convinced she was speaking to Tide for good reason by the time she began to receive the scammer's emails, I don't think her assumption and lack of verification here was unreasonable). The OTPs Mrs B received were sent by Tide, and she approved payments to payee names she expected to see in her mobile application. She's said that she became suspicious towards the end of the fraud event but was reassured by the sophistication of the scam. Overall, Mrs B was convinced that she was talking to Tide and taking action to protect the funds in B's account, and I can understand why.

As Tide has pointed out, there were 'red flags' that Mrs B could've picked up on, and there was more that she could've done to protect B from financial harm – particularly with the benefit of hindsight and/or with more time to think. But Mrs B understood that the poor mobile and internet connection in her property was the reason for the convoluted payment process and failed payments, so her suspicions weren't roused in this respect. And, although she may be familiar with Tide's usual payment processes and contact methods, she has not been under the impression that she needed to move money out of a compromised account

before and I can't say she ought reasonably to have been aware of what that process looked like. In any event, the scam took place over a relatively short period of time. Mrs B's explained that the constant loss of signal was frustrating and added to the stress she was feeling – she was very worried that B's money was unsafe and Tide's efforts to protect it were being hindered. In the heat of the moment, in a highly pressured situation, I don't think it's unreasonable that Mrs B didn't realise B was being defrauded.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct ClearBank Limited to:

- Reimburse B's full loss, along with interest at the account rate from the date of loss to the date of settlement.

- Pay B £1,000 by way of compensation.

Under the rules of the Financial Ombudsman Service, I'm required to ask B to accept or reject my decision before 25 May 2023.

Kyley Hanson
Ombudsman