DRN-4504262

The complaint

Ms N, as the director of a limited company "C", complains that ClearBank Limited won't refund transactions she didn't authorise.

C has business banking accounts with Tide. Tide's bank accounts are provided by ClearBank, and so ClearBank is the respondent business here. For the most part, I've referred to it for actions of both businesses. But where necessary, I've referred to Tide specifically.

What happened

The full details of this complaint are well known to both parties, so I won't repeat them again here. Instead, I'll recap the key points and focus on giving my reasons for my decision:

- In July 2022, while unwell with Covid-19, Ms N received a call from an individual who claimed they were calling from a high street bank whom she also banks with. Ms N says the caller, who we now know was a scammer, knew personal information about her and had spoofed the bank's genuine phone number. The scammer said that multiple payments had left the account and they had sent her an email asking her to install a *help tool* to enable them to recover the money. Ms N says the email appeared to have come genuinely from the bank and she followed the instructions. Ms N's laptop screen went dark and while she thought the caller was helping her safeguard the account, they used remote access software to send payments.

- The scammer then told Ms N that all her business accounts, including those with Tide, were compromised. She says she had already been logged on to her Tide account just prior to receiving the call. Having had remote access already, the scammer made two payments – for £6,100 and £3,900 – from C's Tide account while leading Ms N to believe that they were cancelling the fraudulent payments.

- The call ended and Ms N felt something wasn't right. She checked her accounts with the high street bank and Tide and realised she'd been scammed. Ms N reported the matter to both businesses. She says the high street bank refunded the transactions following its investigation. ClearBank considered the payments were authorised by Ms N as they were completed on the Tide app on her phone. But it accepted that once it had been notified of the scam, the payment for £3,900 could have been recoverable from the beneficiary account had it acted sooner in attempting a recall. In response to her complaint, ClearBank reimbursed C's account with that amount along with £100 compensation for the poor service provided at the time the scam was reported.

- Ms N remained unhappy that she didn't receive a full refund and referred her complaint to our service. Our investigator didn't agree with ClearBank that Ms N had authorised the payments. They recommended it to refund the full disputed amount, less any credits or funds recovered, along with interest and pay the £100 compensation already offered. ClearBank said it had already paid £3,900 and £100

into C's account but it disagreed to refund the remaining loss. So, the complaint was passed to me to decide.

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 agree with the conclusions reached by the investigator for the following reasons:

- The starting point for any complaint about unauthorised transactions is the Payment Services Regulations 2017 (PSRs). C isn't liable for payments it didn't authorise, unless Ms N (acting on C's behalf) failed with intent or gross negligence to comply with the terms of the account or keep the account security details safe.

- To consider a payment authorised, the PSRs explain that Ms N must have given her consent to the execution of the payment transaction – and that consent must be in the form, and in accordance with the procedure, agreed between C and Tide.

- To establish the agreed form and procedure for the two payment transactions, which were completed via the Faster Payment service, I've reviewed the terms and conditions of C's accounts. Briefly, they say that consent can be provided by using the identified method for giving consent, typically a "Make Payment" button and verification which could include a fingerprint scan or submission of a code. ClearBank has said both payments were approved via the Tide app on Ms N's phone.

- Ms N submits that she didn't complete the steps involved in creating a payee and instructing the payment. She believes the scammer initiated the payments when they had remote access to her laptop. When asked by the investigator whether she recalls doing anything on her phone under the scammer's instructions and whether she remembers reading anything on the screen, Ms N said she couldn't recall and that it all happened all very quicky. Ms N said she'd been unwell with Covid-19 already and she felt pressured and worried about fraud.

- ClearBank hasn't disputed Ms N's claim that remote access was used and that the transactions were initiated on her laptop by the scammer. Looking at the audit history from the day in question, I can see the account was accessed via a web browser around that time. In the absence of anything to suggest otherwise, I'm not persuaded that Ms N completed all the steps in the form, and in accordance with the procedure, required to consent to making the payment. It seems more likely that the scammer initiated the transactions on Ms N's laptop through remote access and then tricked her into verifying them on the Tide app on her phone.

- At the time, Ms N thought the scammer was helping her cancel the transactions. I don't think she could reasonably be described as having given someone else permission to go through the form and procedure to make the payments on her behalf either. From what she's told us about what she can recall from the time, I'm persuaded that she likely completed verification believing that it was part of cancelling the transactions, not for payments to be sent to third parties. So, under the PSRs, each payment transaction is considered unauthorised.

- Given this, ClearBank would be required to refund the transactions unless Ms N acted fraudulently (which there's been no suggestion of) or failed to comply with the

terms of the account with intent or gross negligence. I'm satisfied there was no intent on Ms N's part here, so the question is whether she failed to comply with the terms of the account with gross negligence – something which, if proven, would mean C wouldn't be entitled to a refund under the PSRs.

- ClearBank says it appreciates the circumstances here, but the clear and concise nature of the warnings plus the fact that Ms N is a long-standing payment service user means she ought to have known that initiating a payment doesn't imply funds are being returned.

- When the scammer called, Ms N said they knew several pieces of personal information about her – and how her accounts had been compromised and someone was making fraudulent payments. Ms N says the email that appeared to come from her bank looked genuine. Given their familiarity with her information and the fact that the call appeared to have come from a genuine number for the bank, I can see why Ms N trusted she was genuinely speaking to her bank and why she became concerned she was a victim of fraud. I think lots of people would have done the same in these deceptive circumstances.

- I can see that the investigator questioned Ms N why she believed the caller, who claimed to work for a different business, would have knowledge that the Tide account was also under threat. Ms N's explained she had been panicking at the time given a large sum of money had left the account with the other business. She says that point didn't register at the time. I accept that Ms N might not have acted perfectly reasonably – it's possible to criticise her actions with the benefit of hindsight. But given that the scam was designed to engineer its victims in acting hastily, and that is what seems to have happened here, I don't consider Ms N acted with *very significant* carelessness to conclude that she failed with gross negligence. I think lots of people would have acted in the same way as Ms N did.

- I've also thought about the warnings that ClearBank has referred to. It has provided a sample of a warning it says would have been displayed at the time the transactions were initiated. It relates to a Confirmation of Payee (CoP) check. ClearBank has also provided an example of the OTP it says it would have sent to Ms N's phone at the time. I've carefully reviewed the technical audit history, and, unlike previous transactions not in dispute, I can't see that an OTP or a CoP check happened at the time of the relevant transactions. The technical data does show that the transactions were approved through the app – which is in line with what ClearBank has said. Our service's understanding of that process is that the customer receives a notification on their device to approve a transaction in the app. They then access the approvals screen on the app to complete the payment journey.

- Ms N doesn't recall approving any transactions, but looking at the evidence, I think it's more likely than not she was tricked into approving the transactions under the guise of cancelling or reversing the payments. I accept that the screen refers to approving payments. But I can appreciate how, in the heat of the moment, talking with someone she trusted, Ms N found it plausible that she'd need to do this for the payment to be returned. I acknowledge ClearBank's point that Ms N had used these steps before, so should have known it was for making payments rather than cancelling or receiving them. But, like most people, Ms N wasn't an expert in fraud – so I can see why it wasn't obvious to her that these steps couldn't also be used for other purposes.

- It follows that, in line with the PSRs, I don't consider C can be fairly held liable for the unauthorised payments and ClearBank needs to put things right. It has already refunded the smaller transaction for another reason. It now needs to refund the larger transaction, along with interest to compensate C for being without the funds all this time. I note that ClearBank has included the £100 compensation in the financial loss that it says remains outstanding. But as it has acknowledged itself, that amount was paid to recognise its service failures, i.e., a non-financial loss. That amount therefore doesn't form part of the financial loss C is claiming and so ClearBank needs to refund the transaction amount of the payment that is yet to be refunded, i.e., £6,100. If it didn't do this at the time of refunding the smaller transaction, ClearBank can of course make a deduction for £45.62 which it says it recovered from the beneficiary accounts and which I can see was paid into C's account on 5 August 2022.

- I've also thought about the compensation paid by ClearBank. The complainant in this case is a limited company. Although I recognise Ms N has suffered some distress in her personal capacity, I can only consider the impact this has had on C here. Based on the information available to me about the impact of the remaining funds not being returned to C earlier and keeping in mind that I'm awarding compensatory interest on that amount, I'm satisfied that £100 which ClearBank has already paid is fair compensation in the circumstances.

Putting things right

To put things right, ClearBank Limited needs to:

- reimburse C the unauthorised transaction of £6,100 *less* the amount recovered from the beneficiary accounts if a deduction hasn't already been made during the previous refund; and
- pay 8% simple interest per year on the amount refunded, from the date of the unauthorised transaction to the date of settlement (less any tax lawfully deductible)

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require ClearBank Limited to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms N – as the director of C – to accept or reject my decision before 8 January 2024.

Gagandeep Singh
Ombudsman