DRN-4142913

The complaint

Mr L, on behalf of T, complains that ClearBank Limited won't refund transactions he didn't make.

What happened

Mr L fell victim to a scam in April 2022. Following an issue with his internet connection, he received a call from someone posing as a representative from his internet service provider. During this call, he was advised to download software which he was led to believe would help restore his internet connection – but this instead allowed for remote access.

Having downloaded the software, Mr L was asked to put his phone face down by the router and he was periodically required to use his fingerprint on the phone. He believed his fingerprint was requested to allow a refund of £400 for the issues with the internet connection he'd been experiencing and, seemingly, to enable his connection issues to be rectified. But, unbeknownst to Mr L, payments were instead being made to a scammer.

The call is said to have lasted around four hours with multiple payments being made to the scammer during a two-hour period. Some of the payments were made due to money being moved in from another bank account and then transferred out of T's ClearBank account.

Mr L complained to ClearBank about his lost funds. But it didn't uphold his complaint. It noted that Mr L hadn't notified his internet service provider of an issue and said it wasn't convinced being asked to install software would be the 'usual approach' utilised by the internet provider. ClearBank thinks Mr L should have identified an issue when he was asked to put his phone face down and also when asked to put his finger on the scanner. It also considers the £400 compensation Mr L was supposedly offered was too good to be true and thinks this should have raised concerns.

Our investigator upheld this complaint. He concluded that Mr L hadn't completed all the steps to make the disputed payments, or provided consent for them to be made, so were unauthorised. And he didn't think Mr L had failed to comply with the terms of the account with gross negligence or intent.

ClearBank disagreed and largely reiterated the points it had previously made. It maintained that there were 'sufficient red flags' for Mr L to have considered the situation more carefully at the time. And it referenced that it took Mr L an hour to report the fraud from the time of the last payment which it said seemed like a long time.

I contacted ClearBank informally, as the rules we follow allow, in an attempt to resolve the complaint. I let it know that I was minded to agree with the outcome reached by the investigator for the same reasons already provided. But ClearBank maintained its stance. It stated that none of the payments could have been made if Mr L hadn't placed his finger on the scanner. So, it believes T is liable for the payments made, even if Mr L was tricked into making them – and believes the payments to have been authorised. It also believes that Mr L had multiple opportunities to question the nature of the situation and said the outcome would have been different if he had.

So, at the request of ClearBank, I'm now issuing my final decision on the matter.

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 the investigator for these reasons:

- The starting position under the Payment Services Regulations 2017 (PSRs) is that T is liable for authorised payments and ClearBank is liable for unauthorised payments.

- ClearBank says that Mr L's fingerprint authorised the payments, so the payments were *authorised.* But I disagree. To consider these payments authorised, the PSRs explain that Mr L, on behalf of T, must have authenticated the payments *and* given his consent to the execution of the payment transactions – and that consent must have been in the form, and in accordance with the procedure, agreed between him and ClearBank. While there's been no dispute around authentication – it seems to have been accepted by both parties that payments were made largely due to Mr L's fingerprint, as well as one-time passcodes being entered that had been sent to his phone – there is a question around consent.

- To instruct a payment, the payer is required to input the correct unique identifier for that transaction into the platform, such as the sort code and account number or IBAN. But I'm persuaded that Mr L didn't enter any of this information, nor did he 'allow' anyone to do so on his behalf. It would appear that the fraudster entered the required information while they had remote access to Mr L's device. It follows that Mr L didn't consent to the payments in accordance with the agreed form or procedure. He didn't follow all the necessary steps and, as ClearBank acknowledged, he wasn't aware these payments were happening at the time. I consider the payments to be *unauthorised.*

- Given this, ClearBank would be required to issue a refund unless Mr L 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 Mr L's part here, so the question is whether he failed to comply with the terms of his account with gross negligence.

- ClearBank disagreed with our Service's assessment of gross negligence. It reiterated that the £400 supposed compensation, purely because of some internet issues, was too good to be true. It said Mr L bears the responsibility of understanding how payments are made. And that it should be common knowledge that placing one's finger on the scanner isn't a requirement for issuing a payment from a different account. So, it thinks Mr L should have questioned the situation further and that this would have led to a different outcome.

- I acknowledge ClearBank's comments. And I also agree that there were aspects that should have appeared concerning, particularly with the benefit of hindsight. It looks as though a substantial number of payments were made which would have required either a fingerprint or a one-time passcode – and I can see why Mr L might have been expected to question this. But some of this, particularly any payments made requiring one-time passcodes, would have been happening entirely unbeknownst to Mr L, using remote access to his devices. And where Mr L was providing his fingerprint, he was doing so believing – at that moment in time – it was required as a result of his internet connectivity issues – supported by the fact his screen was

repeatedly going blank. But even if I accept that there were things Mr L could have done differently – such as questioning things further – I don't think he acted with very *significant* carelessness to fairly conclude that he failed with *gross* negligence.

- Taking this all into account, I'm not persuaded T is liable for these disputed payments. And I don't consider that taking an hour to report the issue was unreasonable, nor does it make a difference to the overall outcome as it doesn't negate any of the points raised above. So ClearBank needs to put things right – by refunding T's losses alongside interest to compensate for the time it's been out of pocket.

My final decision

For the reasons I've explained, I uphold T's complaint and require ClearBank Limited to, within 28 days of acceptance of the decision, do the following:

- Pay T the total of the unauthorised transactions, less any amount recovered or refunded – I understand this to be £72,925.

- Pay 8% simple interest per year on this amount, from the date of the unauthorised transactions to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 28 July 2023.

Melanie Roberts
Ombudsman