DRN-4801551

The complaint

Mr J (on behalf of Company H) has complained that ClearBank Limited won't refund him for transactions he didn't authorise.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On 17 August 2022, Mr J opened an account with ClearBank in the name of Company H and paid in £129,727.86 to fund the purchase of a plot of land by Company H.

On 1 November 2022, between 13:09 and 13:18, there were four transactions from the account. Three of the transactions were for £20,000 and were paid to other ClearBank accounts. The fourth transaction of £40,000 was paid to an account with a different bank. All four payees were business accounts with different variations of the same payment reference.

Mr J complained to ClearBank when he discovered the transactions. He said his wife was out shopping from mid-morning to mid-afternoon on 1 November 2022. He left the house on his bicycle around 11.30 and arrived back before her at about 13.45. He didn't take his mobile phone with him, the house was securely locked, and the alarm was set. He told ClearBank he didn't consent to the transactions, he wasn't anywhere near his phone when they were made, and his personalised security credentials were locked in the house. He said the transactions should have been stopped because they were unusual for the account.

ClearBank said it contacted the beneficiary banks to see if any funds could be recovered, but the funds were disbursed before Mr J notified it about the payments. It accepted there was a missed opportunity to save £1,528, but this was never refunded.

It said there was no opportunity to intervene due to the speed in which the funds left the account and bigger transactions may occur from business accounts. So even if sums seem out of character, it wouldn't be feasible to stop and check every single payment.

It didn't accept the funds left the account without proper authorisation, so it didn't agree the transactions were unauthorised. It explained that each individual transfer needed to be authorised through the device and according to the evidence, there were no phone number changes and no account-recovery attempts by a third-party, so, nobody had attempted to access the account through a different device. This meant there was no doubt that the four transactions were made through Mr J's device.

It said Mr J's account credentials must've been used and its logs indicated that the one-time passcodes ("OTP)" used to authorise each of the payees were sent to Mr J's phone number, which is the number associated with the device registered to the account. The payees were then added, and the transactions were subsequently approved through the app from Mr J's device.

It said that as Mr J had said he wasn't at home, the transactions must have been made by someone who knew his information or who was able to access the information and then gain access to the account. It said that in line with the terms and conditions of the account, it was Mr J's responsibility to keep his account credentials secure and since his device was used without his knowledge, the only way this could've happened was if the perpetrator knew his security credentials, which is information which he must keep secure and not share with anybody. Otherwise, the device wasn't secured either via a passcode or biometrically, which would mean that access would be easier for a fraudster. It also said that £29,727.86 remained in the account and it's not indicative of fraud for funds to be left in an account following an alleged account takeover.

Mr J complained to this service with the assistance of a representative. He maintained that ClearBank should have blocked the payments and that The Payment Services Regulations 2017 (PSRs) state that unless a bank immediately advises an account holder that they are at fault or are to blame, they should within 48 hours repay the lost money to the account. He argued that ClearBank sent five notifications to his phone for authorisation and the fifth message probably related to the scammer's final attempt to empty the account.

He maintained he wasn't responsible for making the payments and that no-one else had the ability or opportunity to access his account. He doesn't think his house was broken into, rather, the money was taken by someone who knew about the loan, which account the money was in and where he lived. He explained his devices are all secure and his phone was biometrically locked and had a complex passcode.

ClearBank said the payments weren't sufficiently high-risk to have triggered a manual review. It clarified they were made online via a web browser, and it didn't have any data regarding login attempts on the account.

Our investigator recommended that the complaint should be upheld because ClearBank hadn't produced any evidenced that the transactions were authorised by Mr J. She explained a transaction is considered authorised if it is both authenticated and consented to, and the evidence didn't indicate that Mr J had consented to the payments. She noted he'd reported the disputed transactions as soon as possible and ClearBank had shown the funds were moved on to other accounts, which was indicative of fraud.

She noted that ClearBank said Mr J's device was used to authenticate the logins to the web-browser and the app login data indicated his genuine device was used to login to the app around the time the payments were made. But she concluded it hadn't evidenced how the payments were authenticated so it hadn't met the conditions of Regulation 75, therefore it should be held liable for the unauthorised transactions.

ClearBank asked for the complaint to be reviewed by an Ombudsman. It explained the app was signed into with the security code that was designated by Mr J during the account creation at 13:02, the QR code for Web access was scanned at 13:04 and the payments were issued from there. Once this was done, the payments would have to be approved via the app, which took place at 13:09; 13:11; 13:15, and 13:18. It said the only two possibilities were that Mr J signed into the app and arranged the payments himself or that a third party had access to the security code that would allow them to sign into the app. It explained the code is meant to only be known by the member and shouldn't be kept with the device that the app is installed on or accessible to other individuals.

ClearBank further explained that to add a payee, an SMS is sent to the phone number registered with the account and the OTP needs to be shared or entered in the app to create the new payee. From there, a payment can be started from the web, but it can only be authorised through the app. It argued that the evidence it provided shows the payments

were approved through the app which couldn't have been done without approval through the device, which requires access to the account using the account credentials which should only be known to Mr J.

My provisional findings

I've summarised the main points from my two provisional decisions below:

Authorisation

I explained ClearBank is expected to process payments and withdrawals that a customer authorises it to make and under the PSRs, a payment service provider generally must provide a refund if a payment hasn't been authorised. Authorisation has two limbs – authentication and consent.

So, ClearBank needed to show the transactions were authenticated and that Mr J most likely consented to them.

Authentication

Authentication can be shown by the correct details and credentials being used to log into online banking.

ClearBank had explained each individual transfer needed to be authorised through the app using the registered device. It stated there were no phone number changes or account recovery attempts and nobody attempted to access the account through a different device, so there was no doubt the payments were made using Mr J's registered device. I was satisfied that it had produced evidence that the device ID the payments were approved from was the only device ever used to access the app.

ClearBank had also said the payments were authenticated using OTPs which were sent to the registered phone number via SMS. But I concluded it hadn't produced any evidence to show that the OTPs were entered when the payees were set up.

ClearBank had also stated that the payees were set up through Mr J's online banking facility and the payments could only be authorised through the app, which requires access to the account using the registered device. It stated that the app was signed into at 13:02 with the security code that was designated by Mr J during the account creation. I accepted it had produced evidence relating to the device ID the payments were approved from. But it hadn't shown Mr J's security code was used to sign into the app when the payees were set up or that the OTPs were entered when the payees were set up, so I wasn't satisfied it has shown the transactions were authenticated.

I explained the starting point under the PSRs is that ClearBank is liable for unauthorised payments, so I said that unless it was able to produce evidence that Mr J's security code was used to log into the app when the payees were set up and that the OTPs were entered when the payees were set up, I was minded uphold the complaint.

In response, ClearBank produced evidence showing the account was accessed at 13.02 using Mr J's security code and that the app was then opened on a desktop or laptop at 13:04. I was satisfied this showed that whoever made the disputed payments did so using Mr J's mobile phone and that the app was signed into using his security code. It also followed that whoever used the phone would have gained access to it using Mr J's PIN number.

ClearBank didn't produce evidence that that the OTPs were entered when the payees were set up, but as it had shown the phone would have been used to access the app on the desktop or laptop, I explained I didn't need that evidence to make a finding and concluded it had shown the transactions were authenticated.

Consent

I explained that as a rule it's reasonable for ClearBank to hold Mr J liable for transactions where the evidence suggests he authorised them and, in the circumstances, I was satisfied that it did.

Even if Mr J didn't authorise the transactions himself, by allowing someone access to his phone and security credentials, he'd allowed someone to make them. The transactions Mr J disputes were all made using his genuine device, so if they weren't carried out by him, someone else would have had to have access to and know how to unlock the device, and also know the security code to access the account via the app.

So, if Mr J didn't make the payments himself, the only reasonable conclusion was that he allowed someone access to this information, in which case, he breached the terms and conditions of his account and ClearBank is entitled to hold him liable for the loss. And even if I didn't accept that Mr J consented to the transactions, in sharing his personal banking information he was in breach of the terms and conditions of the account.

Compensation

I explained there were no failings in the way ClearBank investigated the claim and the subsequent complaint, so I wasn't minded to ask it to pay Mr J any compensation or to make an additional payment for the other losses to has attributed to the disputed payments.

Recovery

ClearBank had shown the funds had been removed from the recipient accounts by the time Mr J reported the disputed payments to it and so I was satisfied there was no reasonable prospect of a successful recovery. However, it previously agreed to refund £1,528 and I thought that was fair and that it should now be paid.

Developments

ClearBank has stated it has no further comments.

Mr J has responded to say he doesn't accept my provisional findings. He has stated there is no possibility that his phone or computer were used to authorise the disputed transactions and that he didn't authorise them. He has reiterated that he was out when the transactions were made, and he never uses his mobile phone to make transfers.

He is confident that his property wasn't broken into and maintains no one else knew the code to access his mobile phone. He has explained that he checked his ClearBank account when he returned from his bike ride.

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 have considered the further comments that Mr J has made but I'm afraid the findings in my final decision will be the same as the findings in my provisional decision.

Mr J has explained there is no possibility that his house was broken into, and I'm satisfied this is the least likely of the possible scenarios because an intruder wouldn't have known his security credentials to gain access to his mobile phone.

He doesn't accept his phone or computer were used to authorise the disputed transactions, but ClearBank has shown there were no phone number changes or account-recovery attempts and so I'm satisfied that they were.

Mr J maintains he was out on his bike when the disputed transactions were made and that no one else knew the code to access his mobile phone. While I accept he has said this from the outset, I'm afraid the available evidence shows that whoever made the disputed payments did so using Mr J's mobile phone and that the app was signed into using his security code. And in the absence of any evidence to the contrary, I'm satisfied this means the payments were authenticated by someone who knew his security credentials.

I understand Mr J is adamant he didn't make the payments himself, but the only other reasonable conclusion is that he allowed someone access to this information, in which case, he breached the terms and conditions of his account and ClearBank is entitled to hold him liable for the loss.

In the circumstances, while I sympathise with the situation Mr J now finds himself in, I can't fairly ask ClearBank to refund the money.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask H to accept or reject my decision before 13 June 2024.

Carolyn Bonnell
Ombudsman