DRN-3396222

The complaint

Mr and Mrs M complain that Lloyds Bank PLC are holding them responsible for two bank transfers that they did not make or otherwise authorise from their joint current account.

Mr M has taken the lead on the complaint, so I will refer to his submissions throughout my decision. I intend no discourtesy to Mrs M by doing so.

What happened

On 3 December 2020, Mr M received a text message asking if he'd set up a new payee from the joint account. Mr M explains that he hadn't, and that he tried to call Lloyds about it at the time, but he had to give up as the phone lines were too busy and he couldn't get through.

Later that afternoon, a device was registered to use mobile banking using Mr M's mobile number. Mr M has explained that he didn't have his laptop with him when he received the text message so he tried to download the mobile banking app onto his phone in order to log in and stop the payment mentioned in the text message. Mr M maintains that he was never able to log into the mobile banking app on his phone and that mobile banking has never worked for him.

In the early hours of the morning on 4 December 2020, two payments were made to a new payee. The transfers were made using mobile banking by the device that had been registered the previous afternoon. Mrs M happened to be awake and logged in around the time that the second payment was made. Mr M has provided screenshots to show the transactions were reported using the bank's online chat straight away. Later that morning, Mr M spoke to Lloyds on the phone.

Lloyds started looking into things. The bank's technical records showed that two further attempted payments had been blocked. It initially refunded Mr and Mrs M. But later that day, it reversed that position and said it was holding Mr and Mrs M responsible. It said the payments had been made using Mr M's registered mobile device with fingerprint. When Mr M complained, the bank did not change its position. In its first final response letter on 21 December 2020, it said it could not see how anyone else could have made the payments because there was no compromise of Mr M's phone or his internet banking passwords. It paid £75 compensation to acknowledge the distress and inconvenience that had been caused by crediting and then re-debiting a refund. Mr M continued to dispute the matter. He also pointed out that he'd been left without a bank card for almost all of December. In the bank's second final response, it suggested that Mr M should refer the complaint to this service.

Mr M contacted us. He said it was clear that there had been a fraud caused by the hacking of Lloyds' security systems.

The complaint was looked into by one of our Investigators. During the course of his investigation, our Investigator established that the text message Mr M had received on the afternoon of 3 December 2020 wasn't genuinely from the bank. He was concerned that Mr M could have been the victim of a scam and that the text message had been phishing for him

to reveal personal information. Mr M couldn't remember if he'd clicked on the link contained within the text message or not. He said he'd not received any phone calls from anyone he didn't know personally around that time and reiterated that he'd never been able to log into Lloyds' app. Mr M was very clear that he'd not been tricked into making the payments under false pretences. He said this fraud was only possible because Lloyds' security had been hacked.

After considering everything, our Investigator concluded that Lloyds had provided sufficient evidence to demonstrate that the payments were made with Mr M's consent. He explained the bank's process to add the mobile banking app to a device, which included entering personalised memorable information and an automated phone call being made to the customer's registered mobile number. He said he could not see how a third party could have taken these steps because Mr M had been clear that no one else had accessed his mobile phone, that he didn't click on the link contained in the phishing text and that he'd not shared any personalised security information with anyone else. Our Investigator acknowledged that the situation had been very distressing and inconvenient for Mr M, but explained that he was unable to ask Lloyds to pay compensation for the time he'd spent trying to get a refund when he didn't think the bank had come to the wrong outcome on the fraud claim.

Mr M didn't agree. He was disappointed with the outcome and compared it to the toss of a coin. He pointed out he would not spend so long pursuing this matter if he'd made the transactions himself. He made a subject access request as he thought Lloyds wasn't sharing vital information about the investigation with us. Mr M asked for the complaint to be reviewed again by an Ombudsman, so it was passed to me to decide.

My further investigation

At Mr M's request, we had an initial conversation about the case. Mr M explained there had been a crime here and that the Investigator had sat on the fence and so sided against him. He asked for more time to review the paperwork obtained from the subject access request.

Mr M later explained that he'd not had the chance to look at the paperwork because work and family commitments had taken over. He reiterated he wouldn't still be pursuing this matter if he didn't have a genuine claim, especially as the time and effort this matter has taken now outweighs the value of the loss.

I noted the bank's position that the disputed transfers were made using the device that was set up the day before. I also noted that Mr M maintained that he'd not been able to log into mobile banking at any point. I felt that those positions could not both be right. So I asked the bank if it had any further technical records of mobile banking access for the day before the disputed transactions happened.

Lloyds responded to say it no longer had that specific information, but it was able to confirm that Mr M's genuine phone number was involved in registering the device and provided extracts from its records to support this. It also referred me to a recording of a phone call Mr M had with the bank on 4 December 2020 where the bank says he confirmed he registered the new device.

I listened to the recording and shared the following transcript of the conversation with Mr M:

L: Okay there's a new phone that's been registered on your account yesterday...erm, did you register a new phone with your account?

Mr M: Yes

L: You have?

Mr M: at 615 ending?

L: erm, let me see, it doesn't give, obviously, just says there has been an iPhone that was registered yesterday at about 5:05

Mr M: That was me.

L: That was you then?

Mr M: Yep

L: Okay, no problem.

Mr M responded to say it's not a new phone, it is his only phone and it didn't register as mobile banking had never worked for him. He felt this extract of dialogue was part of the problem as the conversation shows the bank didn't listen to understand.

As both sides have had a fair opportunity to provide further comments and evidence, I have now considered the complaint.

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 recognise that Mr M feels very strongly about what happened. It's understandable that's he's upset. Money has been taken from his account and he feels the only way this was possible is by the bank's systems being compromised. It is not my role to establish the identity of any potential fraudster. My role is to consider whether Lloyds has acted fairly and reasonably by holding Mr and Mrs M liable for the transactions in dispute.

When considering what is fair and reasonable, I am required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time. In cases when there is a dispute about what happened, I base my decision on the balance of probabilities. In other words, what I consider is most likely to have happened in the light of the available evidence.

Of particular importance to my decision about what is fair and reasonable in the circumstances of this complaint are the Payment Services Regulations 2017, (the PSRs), which apply to transactions like the ones in dispute.

The PSRs say that the payment service provider (here, Lloyds) must show the transactions in dispute were authenticated. That's the technical part, and here, I can see from the bank's evidence that the transactions were made from mobile banking using a device set up to link to the account and associated with Mr M's mobile number.

The regulations also say that it's necessary to look at whether the account holder authorised the payments. Whether a payment transaction has been authorised or not is important because account holders will usually be liable for payments they've authorised and, generally speaking, banks will be liable for unauthorised payments.

If Mr M made the disputed transactions himself or authorised for them to be made on his

behalf, it would not be fair to ask Lloyds to refund them. The PSRs explain that a transaction is only authorised if a payer gives consent in accordance with the form and procedure agreed with the payment service provider. But Mr M says he was not involved in the payments in dispute. So the key question for me to consider is whether Lloyds has provided enough evidence to hold Mr and Mrs M responsible.

Turning to consent, Lloyds has provided evidence to show how mobile banking was set up along with log in records from the time the transactions were made. These records show that mobile banking was accessed by the same device that was registered the previous day and that the device is linked to the same telephone number that both Lloyds and this service hold for Mr M. Fingerprint biometrics were used to both log in and to make the payments.

Mr M agrees that he did try to register his device at this time but maintains that the process was not successful. I've thought about whether a third party could have set up a device and linked it to Mr M's bank account without his knowledge or agreement. But this is not supported by the wider evidence. There are no other attempts to register a device at this time. In order to register a mobile device, the user must download and open the online banking app, entering their username and password, along with personalised security information. A four-digit code is then displayed on screen, which the user would have needed to confirm back to the bank in real time during an automated call to the registered mobile number.

From what Mr M has described, there is no clear way how anyone else would have been able to learn his personalised security details, such as his User ID, his password and his memorable information. It's also difficult to see how a third party would have been able to start the process of registering a device without Mr M's awareness given that the process generated a call to Mr M's mobile phone. There is no suggestion of any problem with Mr M's phone network. So I can see no way that a third party would have been able to complete the verification call required to add mobile banking to a device, the process of which includes entering a one-time passcode that can only be obtained by taking a call on the phone number registered. I also don't think it was unreasonable of Lloyds to assume that the process to register the device had completed successfully when Mr M told the bank over the phone that he recognised the registration activity as his own.

Turning now to the specific transactions, the bank has provided technical evidence to show that fingerprint recognition was used. This means the disputed payments must have been carried out by someone with a registered fingerprint on the mobile device used. Given that I cannot see any way for anyone other than Mr M to have registered the device, it follows that I cannot see any way for a unknown third party to make a payment from that device and verify it biometrically.

I accept there are things in the wider circumstances of this case that could stand out as being potential indicators of fraudulent activity, such as Mr M receiving a phishing text message and further attempted payments being blocked. But I am not persuaded that the money left Mr and Mrs M's account because the bank's security systems had been hacked. I have seen no evidence to support this theory.

Nor can I see any way that a third party could have obtained the information needed to make the disputed payments. Looking carefully at the steps required to set up mobile banking and then to make a payment using mobile banking, it would not have been possible to make these payments without validation processes that required interaction with Mr M's genuine mobile phone number to complete. I don't see a likely or plausible way for anyone to have made these payments without Mr M's knowledge or consent in the circumstances that he has described.

This is a difficult message for me to give, and I know it's a difficult message for Mr M to receive. But given the evidence I have, and on the balance of probabilities, I'm unable to fairly reach any other conclusion. I can see no way for anyone else to have accessed Mr M's device or known his personal security information. From the evidence that both sides have provided to me, I don't consider that Lloyds acted unfairly by holding Mr and Mrs M liable for the payments in dispute. This means I am unable to agree that Lloyds should be required to take any further action now.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M and Mrs M to accept or reject my decision before 29 September 2022.

Claire Marsh
Ombudsman