DRN-4879217

The complaint

Mr and Mrs M on behalf of a limited company which I will call company A complains that Starling Bank debited approximately £8,600 which Mr and Mrs M said were not made or otherwise authorised by them or company A.

What happened

I issued a provisional decision in March 2024 to explain why I thought company A's complaint should be upheld. And I said I'd consider anything else anyone wanted to give me. This is an extract from my provisional decision:

"*In December 2021 a series of five transactions took place on the account of company A which Mr and Mrs M said neither they nor anyone acting on company A's behalf made or otherwise authorised. They were made early in the morning and in close succession to each other whilst they were both still asleep in bed. The payments were card payments to two companies, and they totalled approximately £8,600. Mr and Mrs M said at the time they were having problems with their mobile phone and their Starling banking application. It does not appear there were any further failed attempts to make payments or take funds from Company A's account.*

Mr and Mrs M explained they noticed the transactions upon waking up in the morning and contacted Starling within an hour of the final transaction to report them as unauthorised. Starling cancelled Company A's card but said that they were unable to stop the payments from going through as they had already been initiated. Mrs M said she was having problems opening the app and read them the error message. Starling looked into what happened and declined to refund the disputed transactions. They said that they thought it was most likely that the payments were authorised because:

- *The transactions took place on the registered mobile phone which had been used for previous transactions and online banking – which by their own admission was with Mr and Mrs M at the time.*
- *The transactions were made using the 3D secure system and verified in the Starling banking app. This would have required biometric or passcode authentication. Starling said their evidence showed that this was done through biometrics – though I am not convinced I have seen supporting evidence of this.*
- *Mr and Mrs M said they had not been asked to verify any payments or been contacted about them.*
- *Between the transactions that were disputed there was an attempted transaction to 'Payment' for the value of approximately £950 which hit the card security rules and so blocked their card. The card was then unlocked – which requires the customer to go into the app and mark the transaction as recognised. They said this was approved and made successfully and was not disputed.*

Mr and Mrs M on behalf of company A did not agree. They thought it was most likely completed by someone else who had managed to get into their device through a sophisticated 'bug'. They said they still had the phone but had not used it since. Mr and Mrs M said they believed that an app Mr M downloaded from a legitimate app store had allowed

someone access to the account. They specified the app store and type of app. They also described the way in which his phone was not running normally at the time. They offered to send the phone to Starling's fraud team, though this offer was not taken up.

Mr and Mrs M contacted the merchants who were the recipients of the funds. They were not able to get a refund from all of them, as goods had already been dispatched in some cases. But they were able to secure a refund of three of the transactions from the merchant – which came to approximately £5,850. Therefore, the remaining loss in dispute is of approximately £2,765.

Dissatisfied with Starling's response, company A brought a complaint to our service. One of our investigators looked into what happened and did not recommend that the complaint be upheld. They thought that on reviewing the evidence it was more likely that company A made or otherwise authorised the transactions. Mr and Mrs M remained unhappy. As no agreement could be reached, the matter has been passed to me to decide.

I reviewed the complaint and wrote to Starling to ask them to reconsider the case as I thought there was evidence to suggest that an unknown third party could have used malware to access company A's mobile phone in order to make the transactions. They continued to decline to refund the disputed transactions. They said they had evidence that screen sharing software had been present on the device at the time, and this did not line up with the kind of malware I had suggested may have played a role in the disputed transactions. Mr M and Mrs M said they did not recall downloading any such software or being asked to do so – they only remembered the app they had already mentioned. As Starling did not agree, I have progressed this matter to a formal written decision.

What I've provisionally 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 am minded to reach a different outcome to our investigator. I'll explain why.

Generally, Starling can hold company A liable for the disputed transactions if the evidence suggests that it is more likely than not that they authorised these payments or gave someone else consent to make them on their behalf. I'm satisfied from Starling's technical evidence that the payments were authenticated on company A's device and using their details. But the regulations relevant to this case say that is not, on its own, enough to enable Starling to hold company A liable. So, I need to think about whether the evidence suggests that it's more likely than not that company A consented to these transactions being made. Having done so, I think on balance it is most likely company A did not authorise these transactions. I'll explain why.

The subject matter of this complaint is sensitive, and so I will not go into every detail of what both parties have told me in depth in this decision. Both parties are aware of the information I have used to consider the complaint. But in short, it is for the bank to demonstrate that company A authorised these transactions and I am not persuaded that they have.

Starling have been able to show that the transactions took place on Mr and Mrs M's device, that screen sharing software was present at the time, and they have asserted that their technical evidence does not show what they think it would if malware was present on the device. They have said that to get into the app and use 3D secure, biometrics will have had to have been used – but have also said it could have been biometrics or a passcode and have not provided me evidence to show clearly that it was the former. I'd invite them to do so if they have this, as this could be compelling evidence in support of their position and may change the outcome of my decision.

In opposition to Starling's arguments, I have carefully considered what Mr and Mrs M have told me about what happened and how they think it happened. I've thought about the type of app they had download. There were reports that around the time of the disputed

transactions, a type of malware had been able to get into phones and access online banking by getting in through a backdoor when users downloaded an app. I thought about the type of phone and operating system they used – these are in line with the devices and operating systems which commonly were subject to this kind of malware. I also considered the issues it caused on their phone, in that it stopped Mr or Mrs M from being able to open the app and caused issues with other apps and the phone freezing. This is in line with reports of

user experience who were subject to a malware attack. The timing (early in the morning) and quick succession of payments are also in line with reported malware attacks. The app not working is also supported in evidence as Mr and Mrs M reported the error message they received when they contacted Starling to dispute the transactions, and it is clear the app was deleted that same morning in the technical device evidence provided by Starling – as was recommended in the phone call. These elements are all in line with this type of malware attack – and the presence of screen sharing software would not in my opinion make their story any less plausible – as the presence of such software does not negate the simultaneous and linked presence of malware. And I do not think it unusual that malware would present in different ways due to the ever-changing nature of it.

I've also considered Mr and Mrs M's behaviour in the time after the disputed transactions. They got in touch with Starling within an hour of the last transaction being made. They have consistently told Starling and our service the same story. They have gone to the police, and they have contacted the retailers whom the funds went to, even managing to cancel orders and secure a refund of payments for goods which had not yet been dispatched. They kept the mobile phone and have tried to get Starling and the police to look at it. They have spent a great deal of time pursuing this and remained consistent in what they have said throughout this time – which I think is compelling.

Starling said that an undisputed transaction took place between the disputed transactions, which required someone logging into the Company A's Starling account in order to unblock it, as the payment had hit one of the card security rules. They have shown data which says this – but the data does not appear to be linked to Company A's account. I say this because the supporting evidence does not include any reference to Company A or the account – and

I cannot see a payment being sent to 'Payment' or for the amount the supporting evidence says the payment was for in Company A's bank statement. I have only been provided with a statement ending on the day after the disputed transactions – so I will be willing to reconsider this point if Starling can show that it did not appear on this statement due to the time some transactions take to leave an account. Clearly if true, this would be compelling evidence which would undermine Company A's case, so I invite both parties to provide further evidence on this point.

I have not seen any evidence that suggests there were failed attempts to remove further funds, and it does seem unusual that an unknown third party with access to the account would not have attempted to maximise profits by emptying an account and any available credit facility. But, I think some of the evidence provided by Starling shows snapshots rather than the whole picture – by showing individual actions on the account rather than the full history of what happened – so I would welcome them to evidence that there were no further attempts with a full data history for the relevant time period.

Starling have suggested that they would have been able to see malware in the digital data and have shown what they think it would have looked like. I am not persuaded that they can say with certainty that they could detect all malware in this way, so this evidence has not altered my opinion.

So I think there is a plausible explanation as to how these transactions could have been completed without any authorisation from company A – and I do not think any of the subsequent evidence Starling have provided me with makes it any less plausible. So I am not satisfied that on balance Starling have been able to show that these were authorised

transactions – and so I am asking them to refund any remaining losses plus 8% simple interest from the date of the transactions.

My provisional decision

If nothing changes, I will uphold this complaint and ask that Starling to refund the remaining losses with interest as outlined above."

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.

After sending both parties my provisional decision, Mr and Mrs M responded with evidence of the specific app they had downloaded in support of their testimony. They also explained that they had kept the phone, but no longer used the device. This supports their testimony as they were able to show me the specific app, and it is in line with an app which at this time was known to provide unauthorised access into devices.

As outlined above, in my provisional decision I said:

> "*The transactions were made using the 3D secure system and verified in the Starling banking app. This would have required biometric or passcode authentication. Starling said their evidence showed that this was done through biometrics – though I am not convinced I have seen supporting evidence of this."*

Starling responded and provided an email in which Mr and Mrs M said that they use their fingerprint to get into their phone and the Starling app. This email stated:

> "*Phone was next to me, on my bedside table. I have a fingerprint unlock screen on it, as I do with my starling app"*

This does not confirm conclusively whether the biometrics were used in the disputed transactions, it just confirms what I already knew which is how Mr and Mrs M would usually get into their device and Starling app. As such, it does nothing to alter my thinking, and I come to the same conclusion I did in my provisional decision.

My final decision

I uphold this complaint and ask Starling Bank Limited to refund the remaining losses, with 8% simple interest from the dates of the losses to the date of the refund.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr and Mrs M, on behalf of Company A, to accept or reject my decision before 26 July 2024.

Katherine Jones
Ombudsman