DRN-5029893

The complaint

Miss E complains that Barclays Bank UK PLC did not refund a series of payments she says she does not recognise.

What happened

Miss E says she downloaded an app to her phone in order to gamble, but later realised it was a scam app that had hacked her phone. As a result, a number of payments debited her Barclays current account which she did not recognise. The total debited from her account at that time was £37,680.01. Miss E raised chargeback claims for two payments online, for £647.99 and £648.85 which were accepted by the merchant and the amounts were refunded to Miss E.

She raised a disputed transactions claim with Barclays, but there were some miscommunications and not all of the payments were included in the original claim. Barclays paid Miss E £50 compensation for the distress and inconvenience this error caused her and a separate £25 for her experience in branch. However, Barclays felt that based on the evidence they had seen, Miss E was liable for the payments as she had authorised them. And they did not raise a chargeback claim for the payments.

Miss E referred the complaint to our service, and clarified that she had authorised some of the payments, however some of the deposits she made onto the betting app did not reach her account and payments out from her Barclays account went to international payees and not to the company she expected.

Our Investigator looked into it and explained it is very unusual for a mobile phone like Miss E's to be hacked in the way she had described and that the payments in question appeared to have been authorised by her using her Barclays app. They also highlighted the unexplained credits into Miss E's complaint at the same time as the payments she had raised that totalled £27,373.49. Overall, they did not think there was evidence a scam had occurred, so they didn't think Barclays had missed an opportunity to reveal the scam.

Miss E disagreed with the outcome. She mentioned that she is a vulnerable individual and that Barclays had not treated her well throughout the complaint. She felt the phone calls and text she had provided showed her details had been compromised. She said that credits into her account could have been refunds she had requested from the gambling app and she did not receive any winnings.

As an informal agreement could not be reached, the complaint has been passed to me for a final decision.

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.

Miss E's testimony is a little unclear as she has accepted that she authorised some

payments on the app she downloaded but has said some deposits she made did not register on the app as expected, and that the payments went to international companies instead of the name of the app on her statement. She has said that she did not recognise some of the payments out of her Barclays account and expected the funds to 'bounce back', but when a significant amount of funds debited on 11 January 2023, she realised something was not right.

Generally, Barclays is able to hold Miss E liable for the disputed transactions if the evidence suggests it's more likely than not that she made or authorised them herself. This position is confirmed in the Payment Service Regulations 2017 (PSRs) and the terms and conditions of her account.

From what I've seen, the payments were made using Miss E's genuine debit card information. While this is important, it isn't enough on its own to say Miss E is liable for the transactions. Barclays also has to show it's more likely than not that Miss E herself made or otherwise authorised the transactions.

Barclays has shown that the IP address used for the transactions matched the IP address Miss E used when logging in to her Barclays mobile banking ("BMB"), so they felt it was more likely she carried them out herself. In addition, 80 out of the 96 transactions were authorised using 'Trust Anchor'. When Trust Anchor is selected, a notification is received on the consumer's BMB app asking them to log in and authenticate the payment and once they log in they will have to either confirm or deny the specific payment. Barclays has confirmed the BMB log ins for Miss E's account match the Trust Anchor verification for the payments. I therefore think it is more likely Miss E's own device and BMB app were used to authorise the payments in question.

Miss E has said that her phone was hacked by the app and has provided some print outs of screen shots taken of the app, as well as websites that appear to direct her to a fake government website. She has said that these evidence her phone was compromised. She has also provided a report from a technician who reviewed her phone.

I've carefully reviewed the evidence provided, but I don't agree that these show Miss E's phone was hacked. Firstly, it is very difficult to hack a mobile phone, and especially difficult to do so remotely with no physical access to the device. The print outs Miss E has provided do not give any context as to how someone could have gained access to her device and I note the website listed on the bottom of one of the pages does not correspond with the app she says she downloaded.

Having reviewed the report provided by the technician, this also does not conclude that her phone was hacked and it says they cannot locate any apps matching the names Miss E provided in the download history of the device. With all of this in mind, I don't think it's more likely that Miss E's phone was hacked n the circumstances. And I therefore think it was Miss E that authorised the transactions in questions.

As I think it's more likely Miss E authorised the transactions, she is presumed liable for them, as set out above. However, there are some circumstances in which I would expect a bank such as Barclays to intervene in a payment prior to it being processed in order to protect a customer from financial harm. But I would only expect them to reimburse a consumer if an authorised push payment ("APP") scam occurred. This is where a consumer is tricked into sending money to a person that they didn't intend to send the money to, or they transferred funds for what they felt was a legitimate purpose but turned out to be fraudulent. I've therefore considered if I think Miss E was the victim of a scam.

I haven't received much evidence showing the app itself, which is understandable as Miss E

says she deleted it. She has said it was called ’32 R’ and has provided a screenshot from her mobile banking app of what appears to be a bank account check with the name ’32 R’ on it. However, she has provided another screenshot which, when considered alongside the report from the technician, appears to relate to a company called ‘Nine Casino’ which Miss E was on the VIP section for. Finally, she has provided a printout which has a website name at the bottom which appears to be the Spanish Casino website. It is therefore difficult for me to know exactly who Miss E made payments to.

Miss E appears to have accepted that she did authorise some of the payments, though as explained above I think it’s more likely she authorised all of them. And I can see that she logged into her BMB app throughout the period in which these payments were being made, so I’m satisfied she was aware of them. Despite this, she did not raise a scam claim until 12 January, almost a month after the payments began. On balance, I think it’s more likely that if Miss E was aware she was being scammed that she would have raised this sooner. However, I do note that she has said the transactions on 11 January were the prompt for her to raise a complaint.

Miss E has said she did not make any winnings on the account and has suggested that the credits into her Barclays account totalling £27,373.49 could have been a refund from the company. However, whether it was winnings or a refund, I think credits of that amount would more likely be connected to a genuine company that had been providing a genuine service. This is a significant amount of money to receive back if this was a scam and it isn’t a typical feature of a scam.

I do accept that the number of international payees could be seen as unusual, however Miss E has said she was using an international app that she accidentally gained access to when she shouldn’t have been able to. So, it therefore makes sense that the payments were to international accounts. Overall, based on the limited information available to me, I think the transactions match the pattern of genuine gambling and not that of a scam. I therefore do not think it is more likely that a scam occurred in the circumstances. And I do not think Barclays needs to reimburse Miss E in the circumstances.

I want to acknowledge the vulnerabilities Miss E has raised and I want to that her for sharing these with me. I don’t want to take anything away from the situation Miss E has found herself in and how difficult the whole complaint process has been for her. I can see that Barclays has not always responded promptly and there were issues with them taking down all the details of the complaint early on in the process. On balance I think the £75 that has already been paid to Miss E is in line with what I would have awarded in the circumstances, so I do not direct Barclays to increase this. And while I recognise and have considered the vulnerabilities Miss E has raised, I don’t reasonably think Barclays could have done more in the circumstances to prevent the loss Miss E incurred in light of these vulnerabilities.

For the reasons outlined above, I don’t think Barclays needs to reimburse Miss E in the circumstances.

My final decision

I do not uphold Miss E’s complaint against Barclays Bank UK PLC.

Under the rules of the Financial Ombudsman Service, I’m required to ask Miss E to accept or reject my decision before 11 December 2024.

Rebecca Norris
Ombudsman