DRN-6131869

The complaint

Miss A complains National Westminster Bank Public Limited Company ("NatWest") refuses to refund her for transactions on her account she says she didn't authorise.

What happened

The facts of this complaint are well known to both parties, so I won't repeat them in detail here.

In short, Miss A says she was contacted by someone on Snapchat offering help applying for university bursaries. As she was a university student, she followed the link supplied and the instructions she was given, while under the impression that these actions were all to facilitate the incoming transfer of bursary funds. Miss A began receiving messages from NatWest about an unpaid overdraft and when she spoke to it about this, she realised she had been scammed. Miss A says she is unhappy she is being held liable for an overdraft she wasn't responsible for and hasn't benefitted from, and she wants NatWest to refund the disputed amounts.

NatWest says it considered this complaint, but it says Miss A has been complicit in the scam by giving the scammers all her personal and account details along with the one-time passcode (OTP) it sent her to set up her mobile banking. So, it says she should be held liable, and it hasn't refunded any of the transactions to her.

Our investigator also considered this complaint but felt it wouldn't be fair to hold NatWest responsible. He said it seems likely the transactions were authorised and it wouldn't be reasonable to have expected NatWest to have flagged these payments as suspicious as there was no indication they were fraudulent. Miss A wasn't happy with this outcome, so 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.

When considering what's fair and reasonable, I'm required to take into account relevant law and regulations; the regulator's rules, guidance and standards; the codes of practice; and, where relevant, what I consider good industry practice at the relevant time.

Where there's a dispute about what happened, and the evidence is incomplete or contradictory, I must make my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence.

A consumer should only be responsible for transactions made from their account that they've authorised themselves. Miss A said she didn't give any permission for the transactions in dispute to be made but NatWest believes she did. My role then is to give a view on whether I think Miss A more likely than not authorised the transactions, based on the evidence I have available.

Firstly, I would like to say that I am sorry to learn of the situation Miss A has found herself in. From what she has told us it seems she has fallen victim to a cruel scam where she followed the scammers instructions with the belief they were helping her apply for a university grant. However, Miss A says she has lost a lot of money as a result, and I can imagine this must be terribly distressing for her.

Unfortunately, there are many sophisticated scams in operation worldwide. My role here is to look at all the evidence and then reach a decision that is fair to both parties. That means I consider NatWest's position as much as I do Miss A's. And what Miss A is asking for here is for NatWest to use its own funds to pay her back money that she says she lost to a third party after falling victim to a scam.

The first thing I need to consider here is whether the transactions in dispute were "authorised", as per the definition laid out in the Payment Services Regulations 2017. NatWest has provided evidence to show that all the transactions were bank transfers made via her online banking account. And it also shows that all the transactions were carried out on the same device. Based on what we know of NatWest accounts, an OTP would've been needed to set up Miss A's online banking. And this OTP would've been sent to the registered number on the account – which is the same number Miss A gave NatWest when she first opened the account and is the same number Miss A gave us to contact her on. So, I am satisfied that this is Miss A's phone number. Miss A says she didn't give the scammers remote access of her device, and she didn't share the OTP. But, as per the evidence, it would not have been possible to make the disputed transactions without the OTP.

Based on everything I've seen I think there are three possible options here. One is that Miss A carried out the transactions herself under the instructions of the scammer. Another option is that she consented to the transactions by making her online banking details available to the scammer after the initial set-up to make the payments. The third option is that the scammer set-up the online banking account and made the transfers after Miss A had given them the OTP needed to set-up the online banking account.

In practical terms, it doesn't make any difference which of these three options happened here. That is because Miss A is liable whether she carried them out herself; or allowed someone else to do so; or was grossly negligent by giving the scammer the OTP which was sent to her phone, even though the message specifically says it should not be shared. The terms and conditions of the account, to which Miss A would've had to consent to when opening the account, provide the customers must keep their information secure including any OTPs, so by not doing so, Miss A was also breaking the terms and conditions of the account. Therefore, I don't think it is fair to ask NatWest to refund these payments as unauthorised.

However, even if a payment is authorised, there are regulatory requirements and good industry practice which suggest firms/banks – such as NatWest – should be on the look-out for unusual and out of character transactions to protect their customers from financial harm. And, if such payment transactions do arise, firms should intervene before processing them. That said, firms need to strike a balance between intervening in a customer's payment to protect them from financial harm, against the risk of unnecessarily inconveniencing or delaying a customer's legitimate transactions.

As this was a new account, there was no evidence of what usual account usage looked like. Miss A is disputing 10 transactions made between 19 and 23 December 2024, but the value of each individual transaction was not alarming. There were all done via Miss A's online banking, and there was nothing to suggest to NatWest that these may be fraudulent. The payees all seem to be individual accounts, and there was nothing which I would've expected NatWest to flag as suspicious at this point – such as payments to a cryptocurrency platform.

So, I can't say that NatWest ought to have blocked the payments or taken any other steps to intervene with the payment processes.

I know this outcome will come as a disappointment to Miss A, but for all the reasons outlined above, I don't think it would be fair to ask NatWest to reimburse Miss A for the money she lost here. I have taken into account what she has said about being tricked and the effects this has had on her. And while I have sympathy for her situation, I can't say that anything else I have been told here makes a difference to the outcome of this complaint.

My final decision

I am not upholding this complaint

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss A to accept or reject my decision before 10 March 2026.

Sienna Mahboobani
Ombudsman