

## **The complaint**

Mrs H complains that National Westminster Bank Plc (“NatWest”) won’t refund money she lost when she fell victim to an investment scam.

## **What happened**

The detailed background to this complaint is well-known to both parties and has also been previously set out by the investigator. So, I’ll provide a summary and focus on giving my reasons for my decision.

Mrs H fell victim to an investment scam in 2023. She came across an investment opportunity with a company “B” on social media, which she says was endorsed by a well-known broadcaster. Between 19 May and 9 June, under the instructions of her ‘broker’, Mrs H sent £75,150 from her NatWest account to her newly created account with an electronic money institution – R – before sending the funds on to a cryptocurrency provider. Once converted, the cryptocurrency was transferred to crypto wallets as instructed by the broker. A loan for £40,000 was taken out with NatWest and was used to fund the payments.

Mrs H subsequently learnt that she’d fallen victim to a scam, and she reported it to NatWest and R. This decision only relates to Mrs H’s complaint about NatWest’s refusal to refund her. Her complaint about R has been considered separately.

## **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’m sorry to hear about the impact this incident has had on Mrs H’s health. I don’t doubt that losing a significant sum of money has made things difficult for her, especially where majority of the money was borrowed. I therefore realise that this will come as a considerable disappointment to Mrs H, but I’ve decided I’m not upholding this complaint. I’ll explain why.

Given my research into B, I think Mrs H was likely scammed. The Financial Conduct Authority (FCA) issued a warning about it on the day Mrs H sent the first payment to R which she now disputes.

Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There’s no dispute that Mrs H made the payments or gave consent to the scammer to make the payments by granting remote access, and so they are considered authorised.

But in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent

banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

I've looked at the operation of Mrs H's account. I don't consider the first disputed transaction (£1,000) was particularly unusual or suspicious such that I think NatWest ought to have intervened. A couple of days later, NatWest approved a loan application for £40,000, and Mrs H subsequently transferred this amount to her account with R at a branch. I can see that the branch staff completed a form at the time and Mrs H told NatWest she was transferring money to her own account. The member of staff provided a general scam warning and Mrs H confirmed she was happy to proceed with the payment.

It isn't entirely clear to what extent NatWest probed Mrs H before executing her payment instruction in branch. What we do know is that the scammer had provided a cover story to Mrs H in case her bank questioned the loan itself or the transfer of the loan funds. She had been coached to lie to her bank about the purpose of the loan as well as the reason for sending the money to her other account.

I know Mrs H wasn't honest with the bank when it questioned her about two subsequent payments at start of June. She told the agents that the loan was for home improvements and that she was transferring the funds to her account with R because it offered cashback rewards for making transactions through it. Mrs H also lied to NatWest about how long she'd had her account with R. She said she had opened the account three months prior to the disputed transaction, when in fact it was set up just a few days before the first disputed transaction.

During both intervention calls, which I've listened to, the agents advised Mrs H that there had been an increased prevalence of scams. And they covered the most common types of scenarios. During the second call, the agent described a scam scenario which applied directly to Mrs H. Namely, that a customer is talked in taking out a loan and asked to move the funds into one of their own accounts before sending it on for what appears to be an investment in cryptocurrency, but it all turns out to be a scam. The information the agent provided Mrs H didn't resonate with her and she reassured them that no one had instructed her to move the money. When questioned about multiple devices being linked to her account, Mrs H told the bank the new device belonged to her brother as he had been helping her with something.

I've thought very carefully about Mrs H's interaction with the bank on each occasion it intervened and asked her to phone in. I accept it's possible that NatWest could have asked more probing questions – intervention can always be more detailed – but I'm not convinced that that would have positively impacted Mrs H's decision-making. By her own admission, the scammer had trained Mrs H on how to respond to the bank's enquiries. In my view, she was so under the spell of the scammer that a more thorough intervention – either when the payment was made in branch or when the subsequent payments were made through online or mobile banking – is unlikely to have resulted in the scam being uncovered.

What this means is that I can't fairly hold NatWest liable for the losses Mrs H suffered at the hands of the scammer. It couldn't have done more in preventing the payments from being sent in the first instance. And later, given the funds had already been transferred out of Mrs H's account with R by the point she reported the scam to NatWest, recovery efforts would likely have been unsuccessful.

In relation to the loan which Mrs H says was processed eight times with different amounts, but NatWest didn't query that and approved an application for £40,000, I've not been provided with evidence which shows that eight applications were made. It may be that several loan quotations were obtained using different amounts and repayment terms to

review what was on offer. But that is not the same as submitting a lending application on each occasion. I understand Mrs H has suggested that the scammer manipulated her financial information on the application. But NatWest has told us the loan was approved as the application met its lending criteria. There's no suggestion that there were other factors, such as adverse credit history, which meant NatWest lent to her irresponsibly.

In summary, despite my natural sympathy for the situation in which Mrs H finds herself, I don't find that NatWest has acted unfairly or unreasonably. So, I won't be making an award against it. If she's experiencing financial difficulties, I urge Mrs H to discuss her circumstances with the bank. While the loan remains repayable, NatWest is required to treat customers in financial difficulties with forbearance and due consideration.

### **My final decision**

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 7 May 2024.

Gagandeep Singh  
**Ombudsman**