

## The complaint

Mrs B complains that National Westminster Bank Public Limited Company (NatWest) won't refund the money she lost to an investment scam. Mrs B has a representative but I'll refer to her as it's her complaint.

## What happened

In August 2024, Mrs B saw a fake online advertisement, from a well-known financial expert and broadcaster, about a crypto investment opportunity in which she could earn 100% profit. Mrs B believed it to be real and after clicking on the link she was contacted by a scammer.

Mrs B was persuaded to invest £295 in (fake) Company W and, under the guise of assistance, download a remote desktop application that enabled the scammer to access and control her devices from anywhere.

The scammer downloaded several apps onto her device and opened an account with Company C (a crypto company) and Firm R (a legitimate Electronic Money Institution), so they could credit Company W's crypto wallet.

Mrs B appears to have been instructed to transfer funds direct to Company C but found this difficult as NatWest have a limit on crypto payments. So, Mrs B made three payments to the crypto company for £1,000 or less and transferred three payments to Bank H so she could subsequently transfer the funds from her account with them. The following table shows the six payments she made:

Payment Number	Date	Payment method	Payee	Amount
1	17/12/24	Phone via agent	Mrs B's account with Bank H	£3,000
2	18/12/24	Faster Payment	Mrs B's account with Bank H	£750
3	20/12/24	Faster Payment	Mrs B's account with Company C	£690
4	8/1/25	Faster Payment	Mrs B's account with Bank H	£2,000
5	9/1/25	Phone via agent	Mrs B's account with Company C	£1,000
6	14/1/25	Faster Payment	Mrs B's account with Company C	£500
Total				£7,940

Mrs B was led to believe that she'd made a profit of £40,000, which she could access anytime, and that there were thousands of other successful investors.

In December 2024, Mrs B wanted to withdraw her funds and was told she needed to pay release and licence fees. She was subsequently told her funds were being held under investigation and that she needed to pay a penalty fee. Soon after making these payments, she couldn't access her account, and she realised she'd been scammed and lost approximately £30,000.

This financial loss has left Mrs B in a precarious position and she raised refund claims with some of her banks including NatWest.

NatWest said they were unable to refund her as she paid the scammers from another account in her name.

So, Mrs B brought a complaint to our service, but our investigator couldn't see that NatWest had done anything wrong.

As Mrs B remains dissatisfied her complaint has been passed to me to look at.

### **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.

Having done so, although I'm very sorry to hear that Mrs B has been the victim of this very cruel investment scam and lost a significant amount of money, I'm not upholding this complaint. I'll explain why.

I should first say that:

- Although I've read and considered everything Mrs B has said, I won't be responding to every point individually. If I don't comment on any specific point it's not because I've not considered it but because I don't think I need to comment on it in order to reach the right outcome.
- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on balance of probabilities.
- I'm satisfied that the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply to payments where funds are moved to other accounts under their control.
- With regards to recovery, Mrs B's funds were sent to the scammers via other banks and a crypto company, so unfortunately there was no realistic opportunity for NatWest to recover them.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty are relevant here.

#### **PSR**

Under the PSR 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 B made the payments here, so they are considered authorised.

However, 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.

Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider NatWest should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks and building societies are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

### Consumer Duty

Also, from July 2023, NatWest had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, NatWest was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Also, look out for any signs of vulnerability.

With the above PSR and Consumer Duty in mind, I first considered whether NatWest should've recognised Mrs B was at risk of financial harm from fraud or a scam and put in place proportionate interventions.

Mrs B hadn't previously made any payments to her account with Bank H and she called NatWest so they could process payment 1 (for £3,000) for her.

Although the payment was to a payee that was new, the payee was Mrs B's own account with another regulated bank. These are called 'me to me' payments and they are lower risk payments as banks can have confidence in customers having control over payments from the account and another bank conducting due diligence with a better sight of the end destination of the payment.

Had payment 1 been processed by her banking app, I would've expected NatWest to have mitigated the risk of financial harm by issuing general fraud and scam warnings. But as Mrs B purposely called NatWest because she preferred an agent to process the payment for her, she was asked some probing questions and given fraud and scam warnings.

I found that when Mrs B was questioned about the payment, she misled the agent giving her an explanation, which I think they would've found plausible, that she had a card PIN issue and needed to transfer the funds for family Christmas gifts as she wanted to use her Bank H card / account. Also, a conversation took place about Christmas purchases.

Mrs B was also given general scam warnings and asked whether anyone was pressurising her to make the payment or if anyone had told her to lie about the purpose of the payment and, although this was the case, Mrs B said, '*no one asked me*' and '*nothing like that*' and then repeated her cover story.

So, having considered the payments (numbers 1, 2 and 4), I'm satisfied that NatWest put in place a proportionate intervention and there was no reason for them to suspect Mrs B was at risk of financial harm.

Regarding payment numbers 3, 5 and 6, these were to crypto Company C for relatively low amounts – £690 (payment 3), £1,000 (payment 5) and £500 (payment 6).

It isn't unusual for customers to pay crypto and banks like NatWest process thousands of payments. But crypto has an elevated risk as customers can lose their money due to its volatility and fraudsters are known to use it in scams.

Due to this elevated risk, I found that NatWest did put in place measures to protect Mrs B from financial harm. They restricted payments so Mrs B could only make relatively low payments of no more than £1,000 per day five times a month. Also, upon the set-up of the payee customers would receive warnings.

If Mrs B said the reason for her payments were crypto when she set up Company C as a new payee, she would've seen the following warnings that were directly relevant to the scam she was experiencing:

- *'Criminals are increasingly scamming people by setting up fake crypto accounts or taking control of their account.'*
- *Scammers will often contact you to help you invest in cryptocurrency (e.g. Bitcoin) and will offer to guide you through opening a cryptocurrency account.*
- *If you cannot access the crypto wallet or you cannot withdraw money from it, this is a scam and you should stop making payments immediately.*
- *Have you checked the cryptocurrency provider is on the Financial Conduct Authority register.'*

It isn't possible to know if Mrs B gave the correct reason and saw this. Despite it being her responsibility to give NatWest correct information, Mrs B may have possibly selected a different incorrect reason. She has explained that the scammers were manipulative and had brainwashed her, telling her not to listen to her banks and how to answer their questions and, if she didn't follow their instructions, she would lose both her deposit and money. Also, NatWest's system doesn't retain the reason selected.

If Mrs B was told to select an alternative reason, the warning would've likely been about transferring to another account and, although much less effective, she would've seen:

- A warning saying, *'Don't be tricked into moving money to a scammers account'*.
- A link to *'Get further support on scams'*.

I think NatWest had effective measures to protect Mrs B from financial harm and, even if I could be sure Mrs B saw their crypto warnings, I don't think they would've made a difference. This is because when Mrs B tried to make a payment over the phone to Company C for crypto (on 15 January 2025) one of NatWest's fraud and scam agents asked probing questions and Mrs B's answers caused him to be highly suspicious, tell her he was *'almost certain'* she was being scammed.

The agent explained the reasons for him being concerned and although Mrs B said she was convinced it wasn't a scam she indicated she would consider his concerns and speak to professionals about the fees she was being asked to pay. Yet despite the agent's comments and blocking actions and her commitment, which prevented any further payments through NatWest, Mrs B still went on to make further payments through Building Society Y.

So, having considered the above and the information on file, although I empathise with Mrs B's loss and experience at the hands of these cruel scammers, I think NatWest's actions when processing her payments (to Bank H and Company C) recognised the risks and mitigated them in a proportionate way. Unfortunately, their interventions (at payment 1 and 3 and after 6) didn't work because Mrs B was persuaded to mislead them and ignore their warnings. For these reasons, I don't think it would fair and reasonable for me to say NatWest are liable for her loss and to uphold her complaint against them.

### **My final decision**

For the reasons mentioned above, my final decision is not to uphold this complaint against National Westminster Bank Public Limited Company.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 13 January 2026.

Paul Douglas  
**Ombudsman**