DRN-6112531

The complaint

Miss B complains that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY (NatWest) won't refund her the money she lost in a romance and investment scam.

What happened

The circumstances surrounding this complaint are well known to both parties, so I've simply summarised what I consider to be the key points.

Miss B met someone online, on 5 November 2024. The conversation quickly turned to cryptocurrency trading and Miss B was told about the potential profits that could be made through investing. Her friend said he had made significant amounts through buying cryptocurrency. He encouraged Miss B to invest in a trading platform he said he used and he spoke about the profits he had made. He took her through the process of investing and setting up an account with the trading platform, which was to be funded through deposits of cryptocurrency from a cryptocurrency wallet held by Miss B.

She started to invest and made a small initial investment of £500, which quickly made a return of around 45%. She was able to make a withdrawal of £227.86 on 18 November 2024 and this gave her greater confidence that the investment was genuine, so she invested more. Her profits appeared to be growing, and she continued to invest. She took out a loan through NatWest, at the suggestion of her friend and she says she told NatWest the loan was for home improvements, but she actually transferred the money to her cryptocurrency account and from there to her investment account.

Eventually, when she wanted to withdraw from her investment, she was told she needed to pay taxes before she could access her money. After discussing the investment with someone independent, on 5 December 2024, she realised she was the victim of a scam.

Miss B made the following payments as part of the scam.

Payment	Date	Amount	Payment type	Destination
1	14/11/2024	£500	Faster payment	Own cryptocurrency account
2	17/11/2024	£2,000	Faster payment	Own cryptocurrency account
3	17/11/2024	£2,500	Faster payment	Own cryptocurrency account
4	19/11/2024	£3,000	Faster payment	Own cryptocurrency account
5	19/11/2024	£5,000	Faster payment	Own cryptocurrency account
6	19/11/2024	£6,000	Faster payment	Own cryptocurrency account
7	19/11/2024	£6,000	Faster payment	Own cryptocurrency account
8	26/11/2024	£1,000	Faster payment	Own cryptocurrency account
9	27/11/2024	£5,000	Faster payment	Own cryptocurrency account
10	28/11/2024	£8,000	Faster payment	Own cryptocurrency account
11	28/11/2024	£7,000	Faster payment	Own cryptocurrency account
12	28/11/2024	£3,500	Faster payment	Own cryptocurrency account
13	28/11/2024	£3,000	Faster payment	Own cryptocurrency account
14	29/11/2024	£1,000	Faster payment	Own cryptocurrency account
15	04/12/2024	£5,000	Open banking	Own bank account

Miss B complains that NatWest failed to protect her from scams and that due to her vulnerabilities, she was more susceptible to scams. She says NatWest blocked transactions to her cryptocurrency account on 4 December 2024 but failed to block earlier transactions. She believes NatWest ought to have identified the scam and intervened earlier to prevent her losses because the transactions were unusual for her account.

NatWest didn't refund Miss B's money and it didn't uphold her subsequent complaint. It says it became aware, on 29 November 2024, that the sort code for the beneficiary account the payments were being made to was associated with cryptocurrency. As a result, it declined two attempted payments on 4 December 2024. It says it was not aware of any vulnerabilities before the scam.

Our investigator upheld Miss B's complaint. He thought NatWest ought to have intervened on 19 November 2024 and asked further questions before making the £5,000 payment Miss B had instructed it to make. He thought the pattern of transactions was noticeably unusual by that point and he noted that Miss B had also taken out a loan with NatWest the day before. He considered NatWest would have uncovered the scam if it had intervened and asked Miss B probing questions. He said Miss B ought to bear some responsibility for her loss because she hadn't taken steps to protect herself from the scam and hadn't recognised clear warning signs. For example, she was making an investment with someone she had never met in person, who was promising unrealistic investment returns, who suggested she lie to her bank and who suggested she take out a loan to fund her investment. He also noted that Miss B hadn't carried out any research on the investment platform. As a result, he considered NatWest should refund Miss B 50% of each of the payments she had made from transaction 5-14 (inclusive) listed above and Miss B should bear responsibility for the other 50%.

NatWest accepted the investigator's assessment, but Miss B did not. She says there should be no deduction from the compensation because her vulnerabilities made her more susceptible to this scam. Miss B says she has a heightened level of trust in people due to her vulnerability and does take things very literally, which led to her absolute trust in the scammer. She said the payments were highly unusual for her account and NatWest never intervened in a substantial way. If it had done so, she would have listened.

I issued a provisional decision, in which I said, in summary:

- Taking into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice, I think NatWest ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances;

- From 16 March 2023, NatWest introduced limits on payments it identified as going to cryptocurrency exchanges. The limits were £1,000 per day and £5,000 in any 30-day period. All these payments, aside from the final payment, were to a cryptocurrency provider, so if NatWest had identified this, it would have blocked payment two;

- NatWest says it wasn't aware the beneficiary account was associated with cryptocurrency until 29 November 2024 and it did block payments to this beneficiary after that. It says it can be challenging to identify the end beneficiary;

- I considered the beneficiary account was identifiably associated with cryptocurrency and NatWest should have made this connection sooner than it did. For example, publicly available websites contain sort code checkers that show the payee was a subsidiary of a large cryptocurrency exchange. I had asked NatWest why this

connection had only been made on 29 November 2024, but it didn't answer that point directly;

- I considered NatWest ought to have blocked payments two and three, as identifiable payments to cryptocurrency that were above NatWest's limits. I thought the collective value of these attempted payments, to a recently established payee associated with cryptocurrency, ought to have led to NatWest contacting Miss B to provide at least a tailored written warning;

- I thought such a warning would have likely contained warnings that would have resonated with Miss B, because the scam she was falling victim to shared many common features of investment scams that would have likely been covered by such a warning, including contact by social media, being advised on investments by a third-party, unrealistic returns being promised. Overall, I thought she would have heeded those warnings and her further losses could have been prevented;

- I thought Miss B had missed some clear warning signs and opportunities to prevent her loss and as a result I considered she should bear equal responsibility for her loss;

- I didn't uphold Miss B's complaint about the affordability of a loan she had taken out with NatWest and which she had used to fund some of the payments. I found that affordability checks had been made and there was evidence the loan was affordable;

- I considered NatWest should refund 50% of payments 2-15, with interest of 8% from the date of each payment to the date of settlement.

Miss B said she didn't have anything further to add and she accepted my provisional decision.

NatWest didn't accept my provisional decision. It said:

- It was concerned that Miss B had not raised a complaint with her other bank about the final payment. It queried whether that bank had made any intervention in that payment. It thought that if no intervention had been attempted, it might be reasonable for Miss B to raise a complaint with that bank. It was also concerned that her bank did not intervene on the final payment, but it was expected to have intervened on smaller payments with similar additional risk factors. In effect, it suggested it was being held to a different standard to Miss B's other bank;

- It thought my conclusion that Miss B would have responded to a tailored written warning was speculative and said there was limited evidence that such warnings were effective;

- Its established approach was to block payments, above certain limits, where it identified the payment was being sent to a cryptocurrency exchange. In this instance, its systems didn't identify the payment was being sent to a cryptocurrency exchange and the relevant control wasn't triggered. It was not aware of any requirement to use a sort code checker to determine the destination of payments

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, I remain of the view that NatWest ought to have intervened earlier than it

did. NatWest accepted the Investigator's view that it should have intervened in payment five, while my view was that intervention should have come at payment two.

Starting with the issue of whether these payments were identifiably being made to a cryptocurrency exchange, I consider they were. They were being made to one of the larger and better-known cryptocurrency exchanges, through its subsidiary. While there was no requirement for NatWest to use a sort code checker to identify the beneficiary, my point was that it seems to have been easily discoverable that this payee was associated with cryptocurrency, through information that was publicly available. It wasn't clear to me why this association had only been made by NatWest in late November 2024, considering it might have access to further information about the identity of beneficiaries it makes payments to. Despite asking NatWest for comment on this point, it hasn't really explained why that association wasn't made until 29 November 2024, other than suggesting that it can be difficult to identify beneficiaries. On balance, I consider transactions two and three were reasonably identifiable as cryptocurrency transactions and I think NatWest ought to have intervened, as they exceeded NatWest's limits for cryptocurrency transactions. Even if NatWest's cryptocurrency transaction limits hadn't been a factor, I would have expected it to have intervened in transaction three, based on the cumulative size of payments two and three, being made to a beneficiary that was, in my view, identifiably associated with cryptocurrency.

I note NatWest is concerned it is being held to a different standard to Miss B's other bank, to which payment 15 was made. That isn't the case. I would have expected similar intervention from Miss B's other bank when it sent on the money it had received through transaction 15. But I have not been asked by Miss B to consider a complaint about that bank and I cannot compel Miss B to make a complaint to that bank. Miss B has told us she hasn't made a complaint to that bank. In considering the complaint I do have, against NatWest, I find that if NatWest had intervened at an earlier stage, as I consider it should have, that would have likely uncovered the scam and so transaction 15 wouldn't have taken place, so I consider it is reasonable to find NatWest responsible for Miss B's loss and require NatWest to refund that payment (in part).

I consider a tailored written warning, based on the payment purpose, would have been a proportionate intervention, given the cumulative size of payments two and three, the payment destination being associated with cryptocurrency and it being a recently established payee.

NatWest says there is limited evidence that tailored written warnings are effective and it considers it speculative to suggest Miss B would have been likely to have responded positively to such a warning.

It is difficult to determine how Miss B might have reacted if she had received a tailored written warning from NatWest. There is evidence that suggests Miss B trusted the scammer and was quite taken in. Miss B says she is generally very trusting of people. But I think that argument goes both ways – if Miss B had received a tailored warning from her own bank about the features of common investment scams, that were relevant to her circumstances, I think that would have resonated with her and given her pause for thought.

I consider it's likely such warnings would have resonated with Miss B because the evidence shows she hadn't been coached by the scammer at this point about what to say if her bank intervened, she wasn't heavily invested and the warnings she would likely have received would have been highly relevant to her circumstances. For example, for a warning tailored to investment scams I might have expected to see warnings that included some of the following common features of investment scams; being contacted over social media, being promised unrealistic investment returns with little or no risk, receiving investment advice from an

unregulated third party, being put under pressure to invest more and more, amongst other things. The scam Miss B was falling victim to shared many of the features commonly found in investment scams. It's also clear Miss B wasn't completely under the influence of the scammer, even later on in the scam, because she refused to borrow money from her friends and be dishonest with them, even though the scammer suggested it.

Overall, for the reasons given above, I'm persuaded NatWest should have provided Miss B with a tailored written warning on 17 November 2024 and that if it had done so, it's more likely than not that Miss B would have taken notice of it and wouldn't have invested further. On that basis, I'm upholding her complaint.

I remain of the view that Miss B bears equal responsibility for her losses as there were some warning signs that I think she missed and she could have done more to prevent her losses. As Miss B said she accepted my provisional decision, I will not repeat my reasoning in detail here.

I also didn't uphold Miss B's complaint about unaffordable lending in relation to a loan she had taken out with NatWest. Again, as Miss B said she accepted my provisional decision, I haven't repeated my reasoning in detail, but I remain of the view the loan was affordable and affordability checks were carried out by NatWest.

Putting things right

NatWest must pay Miss B 50% of payments 2-15 and add interest to each of these amounts at the rate of 8% simple per year from the date of each payment up to the date of settlement.

My final decision

I uphold Miss B's complaint and I require NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY to compensate Miss B as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 26 February 2026.

Greg Barham
Ombudsman