DRN-5337371

The complaint

Ms B complains that National Westminster Bank Public Limited Company (NWest) won't refund money she lost in an investment scam.

What happened

What Ms B says:

In 2022, Ms B was contacted by someone who introduced her to an investment firm (which I will call 'firm X'). He showed her the investment platform and got her to download screen sharing software. She joined a WhatsApp group and was sent various documents from firm X about its investment strategies and claims.

He coached her to move funds from her NWest account to a crypto wallet, and then to firm X. The payments were:

Date	Payment	Amount
4 January 2022	Mobile banking – to crypto exchange	£800
10 February 2022	Mobile banking – to crypto exchange	£750
18 February 2022	Mobile banking – to crypto exchange	£50
18 February 2022	Mobile banking – to crypto exchange	£4,250
Total		**£5,850**

Firm X then went out of business and was dissolved in April 2023. It was the subject of a warning from the Financial Conduct Authority (FCA) in November 2019.

Ms B contacted NWest through her advisors in July 2024. She says the payments were unusual for her to make and NWest should have stopped them and protected her. She says the bank should refund the money she's lost plus interest and compensation of £1,000. She says the bank should refund the money under the Contingent Reimbursement Model (CRM) Code.

What NWest said:

The bank didn't refund any money. They said customers are shown warnings about scams when they add a new payee or make a payment. The payments didn't flag for a security alert.

Our investigation so far:

Ms B brought her complaint to us. Our investigator didn't uphold it. She said the payments weren't large or unusual enough to have expected NWest to have intervened. The payments were to known payee – as Ms B made a number of payments over the period.

Ms B didn't agree and through her advisors, said:

- The pattern of payments – four payments over six weeks – should've caused concerns. There was an accumulation of payments.

- The payments were to a crypto wallet which Ms B was manipulated into opening.

- NWest should've intervened and had they done so, the scam would've been stopped – as firm X had been the subject of a warning from the FCA; and there were other online warnings at the time about it.

Ms B asked that an ombudsman look at her complaint and so it has come to me.

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 that Ms B has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although she didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider NWest should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out 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 are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make 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.

I need to decide whether NWest acted fairly and reasonably in its dealings with Ms B when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK

beneficiary– and in this case, the payments were made to Ms B's own account with the crypto exchange.

And while I accept this was a lot of money to Ms B, the payments in question were in fact fairly low value ones. There was also nothing else about the payments that ought reasonably to have concerned NWest. There's a balance to be struck: NWest has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments.

In this case, I think NWest acted reasonably in processing the payments. I considered the points made by Ms B's advisors about the accumulated effect of the payments – but they were over quite a long period – six weeks. And by the time the larger payment of £4,250 was made, it was to an established payee as far as NWest were concerned. And so, considering also the relatively low value of that payment, that means the I'm not persuaded it would've been reasonable to have expected NWest to have intervened at that stage.

Recovery: We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether NWest took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. NWest tried to get the money back in August 2024 after the scam was reported.

And here, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover. This was especially the case as Ms B didn't contact NWest until July 2024 – more than two years after the scam took place.

I'm sorry Ms B has had to contact us in these circumstances. I accept she's been the victim of a cruel scam, but I can't reasonably hold NWest responsible for her loss.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 26 May 2025.

Martin Lord
Ombudsman