

The complaint

Mr R complains that Nationwide Building Society didn't do enough to safeguard his money. He wants the money he lost refunded along with interest and £300 compensation.

Mr R is represented by a third party but for ease of reference I have referred to Mr R throughout this complaint.

What happened

In April 2023, Mr R saw an advertisement on a social media platform for an investment opportunity. Mr R clicked on the advertisement and began communicating with a woman associated with the investment scheme (the 'scammer'). He said that a personal relationship developed, and he trusted the scammer.

Mr R was advised to download a cryptocurrency wallet through a website which he said appeared professional. Mr R said he made three payments totalling £3,193.15 and that, at the time, he had no reason to believe the investment was a scam.

When Mr R wanted to make a withdrawal, the platform flagged his account for potential money laundering, and he was asked to make a further payment. Mr R then realised he had been the victim of a scam when he was unable to reach the scammer.

Nationwide didn't uphold Mr R's complaint. It confirmed the payments that were part of the scam and that these were paid to Mr R's cryptocurrency account. It said that the payments weren't outside of Mr R's usual spending (noting the large payments Mr R had made to another individual around the same time) and therefore didn't believe they should have alerted its security systems for additional checks.

Mr R referred his complaint to this service.

Our investigator noted the payments Mr R made were to a cryptocurrency platform and that by the time the payments took place, Nationwide should have recognised that payments to cryptocurrency carried a higher risk of being associated with fraud. They noted the first two payments were small but given the size of the third payment they thought this should have raised concerns. Therefore, our investigator thought that Nationwide should have asked a series of questions about the payment Mr R was making in an attempt to narrow down the specific scam risk. And then it should have provided a warning which covered off the key features of the scam risk identified.

Our investigator thought that had Nationwide intervened the scam would likely have been identified and payment three not taken place. Therefore, they upheld the complaint in regard to this payment. However, while they thought that Nationwide should have done more to protect Mr R's money, they also thought that Mr R could have done more in terms of adequate due diligence and research. Therefore, they said that the liability should be split.

Our investigator accepted that Nationwide wasn't able to recover the funds as these were transferred to an account in Mr R's name and then on from that account. They also didn't think that compensation was required in this case.

Mr R accepted our investigator's view. Nationwide didn't.

Nationwide said that previous activity on Mr R's account showed higher value payments being made to cryptocurrency payees and whilst the payment method changed, it believed these other payments should still be considered comparable. It said this meant that the payments Mr R made wouldn't have appeared as a scam risk.

As a resolution wasn't agreed, this complaint was passed to me, an ombudsman to issue a decision.

My provisional conclusions

I issued a provisional decision not upholding this complaint. The details of my provisional decision are set out below.

Mr R has said that the following three payments made from his Nationwide account to cryptocurrency accounts were part of a scam. He has provided copies of messages with the scammer dating back to April 2023 and I accept that Mr R appears to have been the victim of a scam. Based on the messages, it appears that Mr R may have lost more than is accounted for by the payments listed, however, as the payments below are the only ones that have been identified as part of the scam I have only considered these.

<i>Payment</i>	<i>Date</i>	<i>Amount</i>	<i>Transaction type</i>
<i>1</i>	<i>10 July 2023</i>	<i>£20.60</i>	<i>Card payment</i>
<i>2</i>	<i>10 July 2023</i>	<i>£82.85</i>	<i>Card payment</i>
<i>3</i>	<i>2 August 2023</i>	<i>£3,089.70</i>	<i>Card payment</i>

Mr R authorised the payments from his Nationwide account. Under the Payment Service Regulations 2017, the starting point is that Mr R is liable for the payments he authorised. However, Nationwide should have systems in place to look out for out of character or unusual transactions, or other signs that might indicate that its customers are at risk of fraud.

Mr R's Nationwide account shows he made frequent transactions of large amounts, higher than the payments included in this decision. He also made payments to other digital payment providers. Nationwide has identified several payments Mr R made to digital providers (which provide trading for cryptocurrency and fiat currencies) in July and August 2023. Therefore, I do not find I can say that the payments Mr R made that are subject to this complaint would have appeared to be unusual activity on his account.

That said, while the first two payments were for low amounts, the third payment was for over £3,000 and given the elevated risk associated with cryptocurrency payments, I think it would have been reasonable for Nationwide to have sent Mr R a tailored cryptocurrency warning before releasing this payment. I do not think, given Mr R's account history that Nationwide was required to make human contact at this time.

I have considered what I think would likely have happened had a tailored warning been sent. While I cannot say for certain what would have happened, I find it more likely than not that

even if Mr R had received a warning he would still have gone ahead with the payment. I say this because payments to cryptocurrency platforms formed part of his account history and at the time he believed he was making a genuine investment. He was also transferring money to a third party to enable him to invest larger amounts in his cryptocurrency activities and I can see from the contact log that when Mr R was making the transfers to the third party on 1 August 2023, there was a conversation, and the notes say that initial scam concerns were resolved. Therefore, on balance, I think a further warning when the payment was made to the cryptocurrency platform on 2 August 2023, would have been unlikely to have changed Mr R's view about the investment.

It wasn't until after the above payments were made that Mr R received a message about issues with his trading account stating he needed to make a large deposit. Therefore, in this case, I do not think that a tailored warning sent to Mr R in regard to payment 3, would have prevented him from making the payment and so I do not find I can uphold this complaint.

Nationwide accepted my provisional decision. Mr R didn't.

Mr R said that Nationwide missed an opportunity to discuss the payment he was making in more detail. He said that Nationwide did not provide sufficient intervention on the third payment and it was unfair to suggest that any warnings provided would have been ineffective or ignored. Mr R indicated that if he had been provided with a tailored warning he would have taken this on board and stopped the payment of £3,089.70, preventing the loss.

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 understand that Mr R will be upset that I didn't uphold his complaint in my provisional decision, and I have considered his comments in response to this. However, my conclusions haven't changed.

As I noted in my provisional decision, Mr R's account history showed he made large transactions (higher than the payments included in this decision) and payments to other digital payment providers. Therefore, I do not find I can say that the payments Mr R made that are subject to this complaint would have appeared to be unusual activity on his account. However, given the size of the third payment and the elevated risk associated with cryptocurrency payments, it would have been reasonable for Nationwide to have sent Mr R a tailored cryptocurrency warning before releasing this payment.

I note Mr R's comment about Nationwide missing an opportunity to discuss the third payment with him, but given his account history I do not think that human intervention was required at this time. Instead, I think that a tailored warning would have been reasonable.

Mr R has said that had he received a tailored warning he would have taken this on board and stopped the third payment. While I cannot say for certain what would have happened had the tailored warning been given, for the reasons I have already explained, being that payments to cryptocurrency platforms formed part of Mr R's account history, that he believed he was making a genuine investment, and that he was transferring money to a third party to enable him to invest larger amounts in his cryptocurrency activities, I think it unlikely that a further warning before the third payment was made would have stopped Mr R making this payment.

Therefore, for the reasons I have already explained, I do not uphold this complaint.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 24 October 2025.

Jane Archer
Ombudsman