

## **The complaint**

Ms R complains that Nationwide Building Society ('NWide') wouldn't refund money she lost in an investment scam.

## **What happened**

*What Ms R says:*

In 2021, Ms R was looking for ways to improve her financial security and, in the longer term, to be able to leave money to her grown up children. She saw a pop-up advertisement on social media which said people could invest as little as £200 and still make returns. She clicked on the advert and found the service was provided by an investment firm (which I will call A).

Ms R explored A's website and it appeared genuine and professional. She was contacted by an advisor who seemed charismatic and reassuring. He said he had worked in the finance industry for more than 20 years. He built a rapport with Ms R.

The advisor downloaded software onto her computer so he could remotely access her crypto wallet, and then move funds to A to help her trade. He advised her to open bank accounts (with two other banks which I will call bank X and bank Y), together with the crypto wallet accounts. Ms R authorised him to do that.

A first, small deposit was made by payment from her bank account with NWide to Ms R's crypto wallet. She then saw the credit appear in her account at investment firm A, and saw it was making good returns. The adviser could access Ms R's account with A and traded with her money. She then went ahead and made further deposits.

The advisor then opened a 'loan facility' within A's portal for £40,000 – without her authority – to invest this sum. The adviser said Ms R had to pay off the loans and otherwise, debt collectors would visit her.

Ms R didn't want to be in debt and took out loans totalling £50,000 with four third party loan companies to pay off the loan with A. The adviser controlled her computer and applied for the loans on her behalf. The advisor said the loans were then paid off the loans with A, but then said she was still £40,000 in debt – he said because of the accumulated interest and because of the successful trades he had placed. The adviser put more pressure on Ms R to pay the further debt off.

The proceeds of the four loans (£50,000) were paid into her account with NWide, and payments were then made from her NWide account to her account with bank X. The funds were then transferred from bank X to Ms R's crypto wallet with a payment service provider. The advisor (who had control of Ms R's computer) then transferred the funds to investment firm A.

Ms R allowed the adviser to access her computer to apply for a further loan with NWide – in July 2021, but this was declined. Ms R later took out a secured mortgage with another firm

for £39,853 (under guidance or control of the advisor) and this was drawn on 10 December 2021. It was paid into Ms R's NWide account.

Then, in December 2021, the adviser told Ms R to open an account with bank Y - he said it was easier to make crypto payments from that bank. Under his guidance, Ms R opened her account with bank Y. From NWide, the loan funds were sent to Ms R's account with bank Y, and payments were made to Ms R's crypto wallet account with a payment service provider. The funds were then transferred to the investment firm A – by the adviser.

There were three banks involved in this scam – NWide, bank X and bank Y and I set out the receipts and payments for all three for clarity:

There were two periods in the scam:

*Period one:*

Date	Payment type	Beneficiary	Amount
24 June 2021	Card payment	Payment service provider – crypto wallet	£192.93
1 July 2021	Card payment	Payment service provider – crypto wallet	£200
7 July 2021	Loan rec'vd	Ms R's account – NWide	(£20,000)
7 July 2021	Card payment	Payment service provider – crypto wallet	£200
7 July 2021	Faster payment	Ms R's account – Bank X	£20
7 July 2021	Faster payment	Ms R's account – Bank X	£10,000
7 July 2021	Faster payment	Ms R's account – Bank X	£10,000
20 July 2021	Loan rec'vd	Ms R's account – NWide	(£10,000)
20 July 2021	Loan rec'vd	Ms R's account- NWide	(£10,000)
20 July 2021	Faster payment	Ms R's account – Bank X	£10,000
20 July 2021	Faster payment	Ms R's account- Bank X	£10,000
28 July 2021	Loan rec'vd	Ms R's account- NWide	(£10,000)
28 July 2021	Faster payment	Ms R's account- Bank X	£10,000
30 July 2021	Card payment	Payment service provider – crypto wallet	£500
10 August 2021	Card payment	Payment service provider – crypto wallet	£1,000
31 August 2021	Card payment	Payment service provider – crypto wallet	£150

*Summary for period one:*

Total loans received into NWide – July 2021	(£50,000)
---	-----------

Payments from NWide to Mrs R's account with Bank X – July 2021	£50,020
Payments from NWide direct to Ms R's account with Payment service provider – crypto wallet	£2,242.93
<b>Total payments</b>	<b>£52,262.93</b>

*Period two:*

Date	Payment type	Beneficiary	Amount
10 December 2021	Loan rec'vd	Ms R's account – NWide	(£39,853)
18 December 2021	Faster payment	Ms R's account – Bank Y	£10,000
18 December 2021	Faster payment	Ms R's account – Bank Y	£5,000
18 December 2021	Faster payment	Ms R's account – Bank Y	£100
18 December 2021	Faster payment	Ms R's account – Bank Y	£10,000
18 December 2021	Faster payment	Ms R's account – Bank Y	£10,000
18 December 2021	Faster payment	Ms R's account – Bank Y	£3,000
21 December 2021	Card payment	Payment service provider – crypto wallet	£400

*Summary - period two:*

Total loans received into NWide – December 2021	(£39,853)
Payments from NWide to Mrs R's account with Bank Y – December 2021	£38,100
Payments from NWide direct to Ms R's account with Payment service provider – crypto wallet	£400
<b>Total payments</b>	<b>£38,500</b>

After the amounts were sent to A, Ms R asked for funds to be withdrawn from A, but that wasn't possible. Contact with the adviser stopped. Ms R realised she had been the victim of a scam. Ms R contacted NWide on 23 August 2022 to advise them of the scam.

Ms R says the scam has destroyed her life. She has lost the money she wanted to invest for her children, who she feels no longer trust her. She suffers from sleepless nights and is emotionally distressed. She has taken out loans totalling £88,000 with six lenders and is struggling to make the payments. One loan is secured in her house. As a result, she is having to work longer hours to make ends meet.

*What NWide said:*

NWide said none of the payments had been flagged on their systems as being unusual and needing intervention. They said the payments were to Ms R's accounts with bank X, bank Y and then to her account with the payment service provider (her crypto wallet). They couldn't therefore be held liable for the scam payments – as those were too far removed from the payments made from NWide.

*Our investigation so far:*

Ms R brought her complaint to us. Our investigator said NWide should've intervened from the first large payment on 7 July 2021. Had they done so, the scam would've been uncovered and the payments prevented. If they'd contacted Ms R she would likely have said she was investing on the advice of the advisor and she'd taken out loans to do so; and that she had done limited research into A.

He said that NWide could've realised what was going on when they declined Ms R's loan application for a home improvement loan in July 2021 – when they could've asked why she needed the money and why she was going to pay it into an account with bank X. Ms R could then have been given a tailored warning and the payments prevented.

Our investigator said Ms R should be held responsible for 50% of her losses as she could've done more to protect herself – she acted on the advice of a third party whose details were sourced from the internet; she cooperated in applying for six loans to pay back the loan in A's portal; and she told NWide she wanted a loan for home improvements, when it was really for bitcoin investment.

During our investigation, bank X agreed to meet 80% of the losses due to payments made by that firm – they refunded £40,016 of the payments made from bank X – which totalled £50,000.

Our investigator said NWide should pay Ms R £15,551.75 – being their share of Ms R's total losses. This included £10,004 (less a deduction of 50% for contributory negligence) – in respect of Ms R's unrecovered losses at bank X.

Ms R accepted this, but NWide didn't agree and asked that an ombudsman look at Ms R's complaint, and so it has come to me to do that.

*I made a provisional decision which said:*

I'm sorry to hear that Ms R 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 Ms R 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 NWide 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.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) 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 by Ms R to her own account – with bank X and bank Y.

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

The first consideration here is: if the payments were of a sufficient size and was out of character with how Ms R normally used her account – then we would expect NWide to have intervened and spoken to her about them. I looked at Ms R's account for 2021 - and it's fair to say that she used her account only for typical day to day living expenses.

*First four payments:*

Looking at the first four payments (£192.93, £200, £200, and £20) – these were low value and we wouldn't have expected NWide to have intervened. There's a balance to be struck: NWide has obligations 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 NWide acted reasonably in processing those payments.

*First payment £10,000:*

But after that, the first payment of £10,000 on 7 July 2021 was unusual compared to the way in which she used her account. And the payment was to a new payee.

So – I think it's reasonable to say that NWide could be expected to have stepped in at that time and contacted Ms R about it.

But I also must consider whether that would've made a difference here. And on balance, I don't think it would have. I say that because:

In this case, multiple accounts under Ms R's control were involved, and the payments from NWide were to her bank accounts with bank X and bank Y – and then moved to the payment service provider (her crypto wallet) via those banks. So, NWide were the first bank in a series of payments involving another two payments firms. In such circumstances, it's less likely that we'd hold NWide responsible for Ms R's losses.

On the other hand, Ms R's accounts with bank X and bank Y had been opened by her (under the guidance of the scam advisor) for the purposes of the scam. So – there is an argument that NWide could've asked questions about those accounts and how Ms R intended to use them - and discovered what was going on.

But - I must be persuaded that Ms R would've revealed the extent of the scam to NWide – or whether she would simply have said the payments were going to her other bank accounts in her name. And here:

- We know that Ms R was firmly under the spell of the advisor and believed what she was being told. She was thought the investment opportunity was a genuine one.
- We know that Ms R had downloaded software onto her computer and the advisor was controlling her interactions with banks (and was moving money from her crypto wallet to her account with A). He had applied for the loans with finance providers in her name and on her behalf.
- I therefore think it more likely than not – that the adviser would've either responded to any online warnings from NWide himself; and if NWide had called Ms R, he would've coached her as to her responses.
- For NWide to have uncovered the scam – where payments were being made to Ms R's own account with bank X and bank Y - before being moved from those accounts to her crypto wallet – seems to me to place an unreasonable obligation on NWide in this case.

Our investigator argued that NWide should've been put on alert because of Ms R's failed application for a home improvement loan in July 2021 – that during the loan approval process, they could've uncovered her real reason for wanting to borrow money, and therefore uncovered the scam. But – I think this places an unreasonable obligation on NWide to do that, so I set that aside. And – as we know, the loan application was carried out by the scam advisor, so responses to any questions would likely have been from him.

Therefore on balance, and in the circumstances of this case, I don't think I can reasonably hold NWide liable for Ms R's losses here.

#### *Recovery*

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether NWide took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. Here, I didn't see any evidence that NWide did take such action. But – as the scam took place in 2021, and Ms R didn't report it to NWide until August 2022, it's very unlikely that any funds would've been available – as normally in such scams, funds are removed from the recipient bank immediately.

NWide did attempt to get the amount of the debit card payments refunded by the card scheme which issued the card. The claim failed. I haven't looked at this further as this was an authorised payment by Ms R, and a chargeback had no reasonable prospects of success.

I intend to not uphold this complaint against NWide, and say that NWide are not liable for the payments made. But – I intend to uphold the complaint about bank Y and say that bank Y are liable for the payments made through that bank. As noted, bank X have refunded £40,016, being 80% of payments made through that firm. For the reasons I've explained, I don't think it's fair to ask NWide to bear a share of the amount not refunded by bank X.

#### *Responses to the provisional decision:*

Mrs R accepted the provisional decision. Nationwide didn't make any comments.

I now need to make a final decision.

**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.

As Mrs R accepted the provisional decision, and Nationwide didn't make any comments, my final decision is unchanged from the provisional decision.

**My final decision**

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 24 November 2023.

Martin Lord  
**Ombudsman**