

The complaint

Mr M says Nationwide Building Society (“Nationwide”) refuses to refund him money he says he lost to a scam.

What happened

The circumstances of this complaint are well known to both parties, so I won’t repeat them in detail here.

In short, Mr M says he fell victim of scam where he was tricked into sending money to a scammer via cryptocurrency. Mr M says he believed he was speaking to a lottery winner who he’d messaged online to ask for a donation for his charity. The scammer agreed to give him a donation, but before receiving any money he was tricked into sending money for taxes, admin fees, money laundering checks, and for certificates to prove the money was for a charitable donation. Mr M paid a total of £4,233.92 to the scammer between May 2023 and February 2024, but he never received any of the donation money.

The payments were all visa debit transactions made to cryptocurrency wallets with Coinbase and Moonpay. The details are listed below:

Payment Number	Date	Amount	Paid to	Notes
1	08/05/2023	£250	Coinbase	
2	25/05/2023	£100	Coinbase	
3	25/05/2023	£150	Coinbase	
4	25/05/2023	£200	Coinbase	
5	25/05/2023	£250	Coinbase	
6	14/06/2023	£50	Coinbase	
7	13/01/2024	£100	Moonpay	
8	13/01/2024	£275.24	Moonpay	
9	17/01/2024	£200	Moonpay	
10	17/01/2024	£300	Moonpay	
	29/01/2024	£300	Moonpay	Transaction blocked by Nationwide Fraud team.

11	30/01/2024	£530	Moonpay	
12	05/02/2024	£174.45	Moonpay	
13	06/02/2024	£320	Moonpay	
14	08/02/2024	£23.83	Moonpay	
15	08/02/2024	£31.78	Moonpay	
16	08/02/2024	£198.62	Moonpay	
17	10/02/2024	£530	Moonpay	
	14/02/2024	£530	Moonpay	Transaction blocked by Nationwide Fraud team.
18	15/02/2024	£550	Moonpay	

Mr M made a complaint to Nationwide about the above payments. It said the transactions to Moonpay did raise suspicion, and the fraud team contacted Mr M. However, Mr M wasn't honest about the nature of the payments and the third-party involvement - so it wasn't able to protect him from the scam. Nationwide refused to refund any of the payments, so, Mr M brought his complaint to us.

Our investigator considered this complaint and decided not to uphold it. Mr M wasn't happy with this outcome, so the complaint has been passed to me for 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.

Should Nationwide have recognised that Mr M was at risk of financial harm from fraud?

There is no dispute that Mr M authorised these payments himself from his Nationwide account. Generally speaking, consumers are liable for payment transactions they have authorised, and the business are liable for transactions they didn't authorise. So, in this case, the starting point is that Mr M should be liable for all the payments he made.

However, that is not the end of the story. This is because even if a payment is authorised, there are regulatory requirements and good industry practice which suggest firms/banks – such as Nationwide – should be on the look-out for unusual and out of character transactions to protect their customers from financial harm. And, if such payment transactions do arise, firms should intervene before processing them. That said, firms need to strike a balance between intervening in a customer's payment to protect them from financial harm, against the risk of unnecessarily inconveniencing or delaying a customer's legitimate transactions.

In this case Nationwide did intervene and blocked a payment Mr M attempted on 29 January 2024. Which was Mr M's first payment to Moonpay using his new debit card. Having

considered the order of transactions and the circumstances surrounding them, I think this was an appropriate place to intervene. I say this because the initial ten payments are all for a relatively low value compared to Mr M's general spending. And there were no other factors which would've caused suspicion at the time, so, I think it's reasonable that Nationwide didn't intervene earlier.

So, the question I will now consider is whether this intervention was proportionate, before considering whether Nationwide should've exercised further interventions.

Were Nationwide's interventions proportionate?

The payment attempted on 29 January 2024 was flagged by Nationwide's fraud team and blocked. Mr M contacted Nationwide via phone to discuss the payment he was trying to make. I've listened to this call, and I'm satisfied that Nationwide's intervention was proportionate to the risk identified. I say this because Mr M was directed to speak to a representative from the fraud team who explained that there are many scams taking place where customers have been asked to deposit money into cryptocurrency.

During this call Mr M was asked whether anyone has asked him to make these transactions on his behalf. Mr M responded to say he had received such calls in the past and was aware of the scams the representative was talking about. But he confirmed that he had not been asked to make this payment, and that he was making some personal investments in cryptocurrency. Mr M explained that he had been doing so for about a year, and the payment in question was for further investing. The representative on the call presented another scam warning before ending the call.

From this call it is clear that Mr M was asked about why he was making the payment and whether there was any third-party involvement. However, Mr M chose not to mention that he had been speaking to someone on Facebook regarding the payments and he failed to disclose the real reason he was purchasing cryptocurrency. And he gave no indication that there had been any third-party involvement at all. But I am satisfied that Nationwide asked appropriate questions and gave Mr M appropriate scam warnings.

Should Nationwide have exercised further interventions in relation to Mr M's other payments?

As I have outlined above, no intervention was made by Nationwide from payment 1 to payment 10. But these payments were all of relatively low value in relation to Mr M's regular spending. I say this because the payments 1 – 10 ranged from £50 to £300 – which is not unusually high. They were also made to the same beneficiary, which after the first few payments which weren't disputed at the time, the beneficiary would've become a known beneficiary on Mr M's account. So, I don't think it's reasonable to have expected Nationwide to intervene prior to payment 10.

I have thought about whether Nationwide should've provided another intervention at some point and whether this would've prevented Mr M from sending more money to the scammer.

A payment was declined on 14 February 2024; however, no further scam warning was given at this time, and no other questions were asked of Mr M when he called to enquire about this.

Having considered the payments made in detail, I've seen that after the intervention there were another eight payments made to Moonpay in under a month. However, Mr M had confirmed with Nationwide during the intervention call that he was making genuine cryptocurrency payments, and he continued to make payments to the same payee of a

relatively low value compared to his general spending. So, I think it's reasonable that Nationwide didn't have any further concerns, and didn't feel it necessary to intervene again.

However, even if it could be argued otherwise, I am not persuaded that any interventions made after payment 10 would've likely on balance made a difference. I say this because I have not seen anything to suggest that Mr M would've responded any differently to how he responded to the intervention following payment 10. Which means he is likely to have denied any third-party involvement and would not have been honest about the reason for purchasing cryptocurrency. Even though Mr M says he had become suspicious, the scammer sent him further fictitious evidence which seemed to persuade Mr M to continue to send him money. So, I don't think any further intervention would've made a difference to the sequence of events.

I am also not persuaded this is a case where Nationwide, contrary to Mr M's instructions, should have refused to put the payments through.

Recovery of funds

I have considered whether Nationwide acted appropriately to try to recover Mr M's funds once the fraud was reported.

Mr M's card payments were made from his Nationwide account to a cryptocurrency account in his own name. Thereafter, those funds were either moved directly to the scammers, or, if not – Mr M should be able to withdraw them from his account. Further or alternatively, as Mr M's payments were made to purchase cryptocurrency – which would have been forwarded on in this form – there would not have been any funds to recover and there are no valid grounds for a chargeback.

For these reasons, I am satisfied that it is unlikely Nationwide could have done anything to recover Mr M's funds.

Vulnerabilities

Since receiving the initial outcome on this complaint there is evidence that Mr M may have been vulnerable at the time the scam took place due to a change in his medication which could've affected his behaviour. However, I have not been provided any details about this or any evidence to support what has been said.

I have also not seen anything to suggest Nationwide knew or ought to have known about Mr M's personal issues at the time. Further, he did not exhibit any signs of them during the telephone calls concerned. Therefore, I do not find that Nationwide should have dealt with Mr M's payments any differently in this regard.

Conclusion

Having considered Mr M's complaint in full, I do not think Nationwide has done anything wrong in the circumstances of this complaint. Therefore, I will not be asking Nationwide to do anything further.

My final decision

For all the reasons outlined above I am not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 2 September 2025.

Sienna Mahboobani
Ombudsman