

The complaint

Mr L complains that Nationwide Building Society ('Nationwide') won't refund the money he lost to an investment scam.

He's represented by a firm of Solicitors. For simplicity, I'll refer to Mr L throughout this decision.

What happened

The background is known to both parties, so I won't repeat all the details here. In summary, in early 2024, Mr L came across an online advert for a company (I'll call 'X') that was offering crypto-investment opportunities. He registered his interest and was contacted by individuals claiming to be 'financial advisers'. He later discovered he'd connected with a scammer.

He started small at first but, believing the opportunity was genuine, he went on to 'invest' more heavily as instructed. To make the scam more convincing, he was given access to a professional-looking platform where he could monitor his funds and 'returns'. He was also asked to download remote access software as part of the process.

He suspected something was wrong when he tried to withdraw his 'profits' and was told he needed to pay more for 'tax' on his 'investment' (which he'd been led to believe stood at over £310,000) for that to happen. He realised X was a scam when he continued to be pressured into paying more money and the contact with the scammer then stopped.

By that time, a total of £49,000 had been sent from his Nationwide account, across two payments of £25,000 and £24,000 on 17 July 2024, to his new account with another firm ('R'). The funds were sent on from there and lost to the scam. Other scam payments were made or attempted from accounts Mr L held with other firms also ('B' and 'M').

A complaint was made to Nationwide in October 2024 and later referred to our Service. Our Investigator didn't uphold it. In brief, she didn't think Nationwide needed to intervene on the disputed payments. She noted that when it had intervened on earlier payments, Mr L asked for account closure. And that when other firms intervened Mr L was coached on how to respond. She didn't think an intervention from Nationwide would have prevented his losses.

Mr L disagreed. He said Nationwide should have intervened and Banking Protocol should have been enacted. He also referenced the CRM Code and that Nationwide should have done more to attempt recovery once the scam was reported.

As the matter couldn't be resolved informally, it's been passed to me to decide.

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've decided not to uphold it for similar reasons as the Investigator.

In broad terms, the starting position at law is that a firm (like Nationwide) is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (the 2017 regulations) and the terms and conditions of the customer's account. It's not in dispute Mr L authorised the payments in question, so he's presumed liable for his losses in the first instance.

But that's not the end of the matter. Taking longstanding regulatory expectations and requirements into account, and what I consider to have been good industry practice at the time, Nationwide should have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

In this case, looking at the account activity, I think it's arguable there was enough about the payments for Nationwide to have stepped in on concerns that Mr L might be at a heightened risk of financial harm from fraud. But, like the Investigator, I'm not convinced a proportionate intervention would have made a difference to what happened, such that I can reasonably hold Nationwide responsible for Mr L's losses. I say this for the following reasons.

Contact with X started in early 2024. Mr L has himself described the aspects that made him think the 'opportunity' was legitimate. And I think it's significant that the relationship with the scammer had been ongoing for several months when the disputed payments came about. I can also see that, by July 2024, Mr L had already 'invested' significant amounts despite earlier blocks by other firms and some relevant warnings. He'd also closed and then opened new accounts during the scam journey to continue his payments for 'investment'.

For example, in April 2024, Mr L reverted to the scammer asking him to produce documents needed for B to release his funds to a third-party platform, as it was concerned of a "*possible scam*" and that "*[Mr L] didn't know enough about the company*". Before then, B had provided automated warnings, based on the 'payment purpose', for the reported scam payments sent from there, including one relating to crypto-investments. This warned about criminals offering to help invest in cryptocurrency, setting up fake crypto-accounts, taking control of accounts, and the lack of access or ability to withdraw from a wallet. It warned "*this is a scam and you should stop making payments immediately*". It also warned it's unusual for genuine crypto-investment opportunities to be on social media. And provided a link to the FCA for advice.

The scam chat shows the scammer asking Mr L if B had called about his payments. On 11 April 2024 "*any calls from your bank?*". Mr L "*No call yet*". The scammer "*That's good, I think we might have pulled it off*". There was a similar exchange the next day. When B still refused to release a payment, Mr L decided to close that account. On 29 April 2024, he told the scammer "*B blocked my account, The only way out was to close it in branch. I had to quote them FCA rules because right to the end the fraud dep were putting obstacles in my way*".

It looks like Mr L then opened a new one with another bank ('M'). And when in June 2024, M wouldn't release his funds on concerns that he was dealing with a "*scam company*", he went on to close that account too and opened a new one with R instead. To add, the scam chat shows Mr L had told M he was "*buying gold, had already received the goods and was paying the bill*". The scammer responded "*Tell them [M] to close your bank account with them and for them to return your money*" – again, that's what Mr L did.

The evidence then shows Mr L attempted two transfers from Nationwide to R, on 25 June 2024. I note Mr L was called into branch with ID. I also note that, according to the scam chat, as a result of Nationwide's refusal to make the payments, Mr L told the scammer "*I have told them [Nationwide] I want to close the acct...is there a high street bank you recommend?*".

I'm mindful Nationwide did later process the payments to R on 17 July 2024. At the same time, I can't overlook that Mr L had already told Nationwide he wanted to close that account.

He was asked to go into branch to complete the process. As before, he was actively looking for a way around the blocks so he could continue payments to X. I also don't overlook that when, the next day, R stopped his payment (funded by money from Nationwide), Mr L again returned to the scammer about that and went on to mislead R about his circumstances. I don't consider it necessary to set out all the contact between Mr L and R, given also some of the language used. But I note Mr L was given warnings in the automated payment flow. There was also a 'live' *in-app* chat and an intervention call.

In the automated payment flow, Mr L selected *"Buying or renting goods or services"* even though the option *"As part of an investment"* was available for him to choose from. He'd been asked *"Please answer truthfully. If you're being scammed, the fraudster may ask you to hide the real reason for this payment"*. In the 'live' chat, Mr L maintained he was paying for *"digital services/marketing materials/website development"*. He added *"I'm going to their office or a person comes to my place with their laptop and we go over everything"*. For me, it's clear Mr L wasn't prepared to reveal anything significant about what he was involved in, despite being told that the payment had been paused to protect him from a potential scam.

In his submissions to our Service, Mr L has said *"Although the bank made an attempt to contact him to query the payment, the scammer coached him on what to say, ensuring that all communication with the bank was controlled by them. They used sophisticated methods, including screensharing, to guide [Mr L] through the process of transferring funds and to answer any questions from the bank, thus evading detection"*. If that's right, then it's difficult to see that a proportionate intervention would have succeeded in exposing the scam.

Like the Investigator, I'm not persuaded a proportionate intervention would have likely made a difference to what happened. In my view, Mr L was heavily under the scammer's 'spell'. On balance, even if Nationwide had questioned him to find out more, it's unlikely this would have prevented his losses. I'm not convinced he wouldn't have found a way around the truth (as he did with R) or wouldn't have found other ways to make payments (such as opening new accounts) if necessary, for him to pay towards what he thought was a *"lucrative"* opportunity.

In reaching this view, I note Mr L's concerns regarding the request for 'tax' started in August 2024 (after the payments in question). And while Mr L says Banking Protocol should have been invoked, I'm not persuaded the situation was such that this was the only proportionate response, considering also the amounts involved and that the money was going to his account. Nor is it clear such a step would necessarily have stopped the scam, again given he was prepared to give misleading information when questioned, returned to the scammer on blocks, moved past warnings, and opened new accounts to get around blocks.

As for Mr L's reference to Quincecare Duty, this doesn't change my view that it's unlikely things would have played out differently, if Nationwide had intervened, to how they did when other firms blocked payments/intervened. As a matter of causation, I can't reasonably hold it responsible for Mr L's losses in these circumstances. Mr L has also referred to the CRM Code and a lack of recovery attempts. But the CRM Code didn't apply to transfers to a customer's own account. And as the transfers went to his own account with R, he would have been able to access the money himself, if any remained to be recovered.

This isn't a decision I've made lightly. I'm very sorry Mr L was the victim of a scam and about the impact the whole experience has had on him. I don't imagine he would have gone along with any of it thinking he would lose his money in the way he did. However, for the reasons I've given, I can't fairly and reasonably hold Nationwide responsible for what happened here.

My final decision

For the reasons I've given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 25 November 2025.

Thomas Cardia
Ombudsman