

The complaint

Miss D has complained that NATIONAL WESTMINSTER BANK PUBLIC LIMITED COMPANY (NatWest) won't refund the money she lost after falling victim to a scam.

What happened

Miss D found a cryptocurrency investment scheme from an online group she was a member of. However, this was actually a scam.

Over the course of late 2021 to late 2022, Miss D sent around £16,000 to the scammers. She did this by making transfers from her NatWest account to her own account at a well-established cryptocurrency exchange, then she sent crypto on to the scammers. In the end, she couldn't withdraw her holdings and lost access to the scammers' platform.

In 2024, Miss D complained to NatWest about the scam. She feels that NatWest failed in their duties to her, and pointed out that customers had received refunds in other cases. NatWest didn't think they were liable for Miss D's loss.

Our Investigator looked into things independently and didn't uphold the complaint. Miss D didn't agree, so the complaint's 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.

I understand that Miss D fell victim to a scam, and so she has my sympathy. I appreciate this cannot have been an easy matter for her to face, and I appreciate why she would like her money back. It's worth keeping in mind that it's the scammers who are primarily responsible for what happened, and who really owe Miss D her money back. But I can only look at what NatWest are responsible for. Having carefully considered everything that both sides have said and provided, I can't fairly hold NatWest liable for Miss D's loss. I'll explain why.

It's not in dispute that Miss D authorised the payments involved. So although she didn't intend for the money to end up with scammers, under the Payment Services Regulations she is liable for the loss in the first instance. And broadly speaking, NatWest had an obligation to follow her instructions – the starting position in law is that banks are expected to process payments which a customer authorises them to make.

NatWest should have been on the lookout for payments which could be the result of fraud or scams, to help prevent them. But a balance must be struck between identifying and responding to potentially fraudulent payments, and ensuring there's minimal disruption to legitimate payments. I've thought carefully about whether NatWest should have done more in Miss D's case.

However, while I acknowledge that this was a substantial total amount for Miss D to lose, and that the payments went to a crypto exchange, I don't think the payments involved were quite so unusual or out of character that NatWest needed to intervene. The payments were each of relatively unexceptional amounts, and were spread out over the course of nearly a year. The spending was never quite so large or rapid enough to have been of particular concern here, not least given Miss D's other account activity. Customers do occasionally make larger payments or spend on things other than day-to-day expenses, and Miss D had made a number of other similar payments, such as of similar or far larger amounts, during the period in question and the period before. She had a healthy balance throughout – the crypto payments did not empty her account. And they went to another account in her own name, which would've made them look less risky. While the crypto exchange was not yet regulated during some of this period, it was a well-established genuine exchange. And unregulated investments can be legitimate, even if they're often higher risk. NatWest didn't have to intervene every single time a customer paid a crypto exchange. And NatWest were not Miss D's investment advisers here, so they didn't need to warn her about the potential higher risk of her investment. Overall, I do not find that NatWest needed to intervene here, and I do not find that they failed in any particular duty to Miss D in not intervening.

Miss D pointed out that NatWest had intervened during other payments she'd historically made. But while I understand why she thought that might be relevant, I'm afraid it has no bearing on the fact that – for the reasons set out above – they were not required to intervene on *these* particular payments.

Next, I've considered what NatWest did to try to recover Miss D's money after she told them about the scam. But as the payments had gone to Miss D's own account at the crypto exchange, and she'd then sent the money on, there was nothing that NatWest could reasonably do to get the funds back at that point. And as these were payments to Miss D's own crypto account, they weren't covered by the CRM Code for scams either.

Lastly, Miss D pointed out that in other cases, customers had got refunds. But again, while I understand why she thought this might be relevant, I'm afraid it's not a deciding factor. Different people get scammed in different ways, they react differently, different accounts have different historic activity, there were different policies and trends in place at different times, and so on. And in some cases, banks will agree to settle pro-actively even when they don't actually have to. We look at each case on its individual merits. And in the particular circumstances of this particular case, I've found that NatWest do not have to give Miss D a refund.

So while I'm very sorry to hear about what the scammers did to Miss D, I don't think NatWest can fairly be held responsible for her loss. And so I cannot fairly tell NatWest to reimburse Miss D in this case.

My final decision

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

This final decision marks the end of our service's consideration of the case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 15 July 2025.

Adam Charles
Ombudsman