

The complaint

Mr A has complained that Bank of Scotland Plc failed to protect him from falling victim to a cryptocurrency investment scam and hasn't refunded the money he lost.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mr A has used a professional representative to refer his complaint to this service. For the purposes of my decision, I'll refer directly to Mr A, but I'd like to reassure Mr A and his representative that I've considered everything both parties have said.

Mr A says that in October and November 2023 he made two payments to an online cryptocurrency investment platform that he believed to be legitimate. The company, which branded itself under various names, claimed to use AI-driven quantitative trading to generate profits for its users. Investors were required to deposit funds in the form of USDT (a form of cryptocurrency) and then use the platform to supposedly scan the cryptocurrency market for investment opportunities. Mr A says he understood that the system would buy cryptocurrency at a lower price on one platform and sell it at a higher price on another, and he'd keep the profits. He's also explained that the platform operated a tiered structure, whereby the more cryptocurrency deposited, the more transactions he was allowed to carry out each day.

Mr A's first payment was for £4,900 and he was initially impressed that he was able to withdraw £3,618.44 in supposed profit just over a week later. He then made a further payment of £515 as he engaged with the platform daily and he could see his balance growing. He's explained that as he was encouraged by this, he continued to use the platform as he believed it was a genuine investment opportunity. In addition he says he'd been introduced to it by a friend who assured him that other people had also made successful withdrawals.

Mr A says that although he initially had concerns that the opportunity might be too good to be true, an online search didn't reveal any obvious warning signs or red flags. He also says he found promotional material suggesting the company had a large global investor base.

At the end of November 2023 Mr A explains he was no longer able to access the investment platform, so he lost the funds it held, amounting to £1,796.56. He says that as this was his first time investing in cryptocurrency he was unaware that such investments were unregulated or that scams of this nature existed.

Mr A made a complaint to Bank of Scotland on the basis that it didn't intervene or question the payments he made at any stage. He said he didn't receive any calls asking about the purpose of the transactions, nor were the payments delayed for verification. Bank of Scotland didn't uphold Mr A's complaint. It said that Mr A had made high value transactions from his account in the past, and the two payments seen in this scam were made three

weeks apart, so they didn't raise alarm bells as potentially fraudulent. So it didn't agree it should've intervened before the payments were made, and it therefore didn't refund what Mr A had lost.

Mr A remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that although she thought Bank of Scotland should've done more to warn Mr A about the risks of cryptocurrency investments, she didn't think any warnings would've resonated with Mr A, based on how he'd been introduced to the opportunity and the research he'd already done.

As Mr A didn't accept the investigator's opinion, the case has been passed to me to make a 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'm sorry to disappoint Mr A but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr A authorised these payments from leaving his account. It's accepted by all parties that Mr A gave the instructions to Bank of Scotland and Bank of Scotland made the payments in line with those instructions, and in line with the terms and conditions of Mr A's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I'd like to start by explaining that there's no dispute about whether Mr A was scammed; but that in itself doesn't automatically mean that Bank of Scotland is responsible for the resulting losses. I'd need to think that it ought to have taken action to try to prevent the scam from taking place, and failed to do that, before concluding that it's responsible for refunding Mr A.

To decide what's fair in this case I've firstly considered whether Bank of Scotland ought to have identified Mr A's payments as high-risk or unusual, and consequently, whether it should've taken action before following Mr A's instructions to process them. To do that I'd have expected Bank of Scotland to consider various characteristics about the payments, including their values, the payees, the pattern of the payments, and Mr A's usual account activity.

I've carefully reviewed Mr A's account history in the six months prior to the scam taking place and I can see that he'd previously made several payments larger than those seen here. For example, he made two payments of £2,000 in May 2023, one of £100,000 in June 2023 and one of £5,550 in July 2023. So I'm satisfied that the values of the payments alone weren't enough to trigger Bank of Scotland to be suspicious or intervene.

But I'm also mindful that the payments were made to a well-known cryptocurrency platform – which was clearly identifiable from the merchant's name. I'd have expected Bank of Scotland

to take this into account as cryptocurrency investment scams had been known to payment providers since at least mid-2018, as warnings had been published by the Financial Conduct Authority and Action Fraud. So by the time these payments were made in late 2023 Bank of Scotland had had more than enough time to understand and digest these warnings, amongst other information about scams that was available to it.

With this in mind Bank of Scotland ought to have done more to understand more about what was going on from the first payment Mr A made. The payment was made to a new payee which was an identifiable cryptocurrency provider, and the value of £4,900 is large enough to cause a significant loss if it were part of a scam. So as a minimum I'd have expected Bank of Scotland to show Mr A a warning, specifically tailored to cryptocurrency investments, possibly by asking him a series of questions to narrow down the payment's purpose before it was made. Had it done this, it could've provided a clear and relevant warning that had a good chance of resonating with Mr A at that point. Bank of Scotland didn't intervene before Mr A made either of the payments, so my starting point is that it's responsible for Mr A's losses.

But I've also gone on to consider whether a clear and effective warning could've prevented the scam from taking place – and like our investigator, I don't think it could.

There's a fine balance to be made between Bank of Scotland protecting Mr A from financial harm, and unnecessarily inconveniencing him, and I accept that I can't say for certain how Mr A would've reacted to any such warnings. But based on everything I've seen, I'm not persuaded that any form of written warning would've resonated to a point that Mr A would've changed his decision and not made the payments. I say this because by the time he made the payments he'd been convinced by a friend, whom he clearly trusted, that they were part of the same investment and that they were making returns. He's also said other friends and family had been successful, and although the opportunity seemed too good to be true, an online search didn't reveal anything that concerned him.

Even if Mr A had been warned about cryptocurrency investment scams by Bank of Scotland, I think it's likely the warning would've warned him to do independent research into the opportunity and speak to family or friends before proceeding. Based on the series of events Mr A has described that led to him investing in the first place, I think it's more likely than not that he'd have thought he'd already done enough research to satisfy himself that the investment was genuine. On this basis, although I commend the additional research Mr A did before investing, I do think it would've led to any form of warning issued by Bank of Scotland being ineffective, as I've set out above.

I understand Mr A's point that if Bank of Scotland had intervened by speaking to him on the phone he wouldn't have made the payments that resulted in his loss, as he'd have taken its advice. But an intervention can take many different forms and doesn't always need to be a human intervention. The facts of Mr A's case satisfy me that an automated written warning would've been a proportionate intervention, and not a human intervention. So this doesn't change my decision because I can't hold Bank of Scotland to a higher standard than I believe was necessary in the situation.

I'm very sorry that Mr A has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Bank of Scotland responsible for that.

My final decision

I don't uphold Mr A's complaint against Bank of Scotland Plc.

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

Sam Wade
Ombudsman