

The complaint

Miss M complains that Bank of Scotland plc won't give her a full refund of the money she lost in a work tasks scam.

What happened

The circumstances surrounding this complaint are well known to both parties, so I won't repeat them here. Instead, I've set out what I consider to be the key points.

Miss M applied for a remote working position she found on a legitimate recruitment website. She was contacted over a popular messaging application and was given more details about the role. The job involved rating software applications to earn money. Miss M was interested and started her new role but was soon told that she would need to occasionally deposit money into her 'work account' to remove 'negative balances' that sometimes showed on the account. She was assured that she would then be able to withdraw all her money when she had completed any outstanding tasks.

Unfortunately, each time she completed a set of work tasks, another set appeared and her account once again showed a negative balance, requiring her to deposit further, increasing amounts of money.

She struggled to pay some of the amounts needed to remove the negative balances from her account and she took out a loan and borrowed further sums from family and friends.

Eventually, she was asked to deposit £12,000 to unblock her account and she realised she had been scammed. She reported the fraud to Bank of Scotland on 4 July 2025 and subsequently complained that it didn't do enough to protect her from fraud.

Miss M made the following transactions as part of this scam:

Transaction	Date	Amount	Payment type	Destination
1	26/06/2025	£20	Faster payment	Own cryptocurrency account
2	27/06/2025	£4,315	Faster payment	Own cryptocurrency account
3	30/06/2025	£500	Faster payment	Own cryptocurrency account
4	30/06/2025	£500	Faster payment	Own cryptocurrency account
5	30/06/2025	£500	Faster payment	Own cryptocurrency account
6	30/06/2025	£500	Faster payment	Own cryptocurrency account
7	30/06/2025	£500	Faster payment	Own cryptocurrency account
8	30/06/2025	£485	Faster payment	Own cryptocurrency account
9	01/07/2025	£500	Faster payment	Own cryptocurrency account
10	01/07/2025	£1,180	Faster payment	Own cryptocurrency account
11	01/07/2025	£290	Faster payment	Own cryptocurrency account

Miss M says Bank of Scotland intervened twice, but its interventions weren't sufficient. These transactions were clearly out of character for her account and shouldn't have been allowed. She was vulnerable and was coerced and manipulated by the scammers into making these payments and giving Bank of Scotland incorrect information, through fear and

confusion. While Bank of Scotland offered to refund her £1,227.50, plus interest and paid her £40 for some poor customer service, this wasn't enough. The whole situation has had an impact on her mental health and has left her in debt, causing relationship issues with family and friends. She wants Bank of Scotland to review her complaint in light of the coercion and psychological manipulation she suffered and thinks it should refund her in full in accordance with its legal and regulatory obligations.

Bank of Scotland says it could have taken further steps and intervened in payments 8-11 and so it has refunded Miss M 50% of the value of these transactions, plus interest and £40 for not making this offer sooner. It considers 50% was reasonable because Miss M ought to bear equal responsibility for her losses. It said spoke to Miss M on 27 June 2025 and 1 July 2025, it asked her probing questions and gave her relevant warnings and information, but she wasn't honest with it and she provided inaccurate answers to its questions.

Our Investigator considered Miss M's complaint but didn't uphold it. They said Bank of Scotland intervened appropriately on 27 June and 1 July. It asked probing questions and gave relevant warnings. Further intervention was unlikely to have worked because Miss M didn't follow Bank of Scotland's warnings and she gave it inaccurate answers to its questions. She thought this would have continued if Bank of Scotland had made further contact. The evidence showed that the scammer was guiding Miss M about how to answer Bank of Scotland's questions and it appears Miss M trusted the scammer. The Investigator didn't think it was unreasonable for Bank of Scotland to find that Miss M ought to bear some responsibility for her loss in those circumstances and she thought the bank's offer was reasonable overall. She didn't think there was any prospect of Bank of Scotland being able to recover Miss M's money.

Miss M didn't agree and asked for an ombudsman's decision. She said her vulnerability and the extent to which she was manipulated and coerced had not been properly considered. The Investigator had no factual basis for concluding that further intervention wouldn't have worked. Bank of Scotland's intervention wasn't sufficient as the transactions were clearly out of character. She hadn't knowingly misled Bank of Scotland but was acting through fear and coercion to try and recover her money. The £40 Bank of Scotland paid for distress didn't reflect the impact of its delays, poor communication and other issues.

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'm not upholding Miss M's complaint. While I understand this will come as a disappointment to Miss M and I am conscious of the impact this cruel and distressing scam has had on her, I'm not persuaded that I can fairly conclude that Bank of Scotland is responsible for her losses. I say this because I don't consider further intervention would have uncovered the scam. I'll explain why.

In broad terms, the starting position is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the accounts terms and conditions and with the Payment Services Regulations (PSRs). It isn't in dispute that Miss M authorised these payments, although I accept her point that she did so thinking they were part of a legitimate job opportunity or due to manipulation from the scammer. Bank of Scotland had an obligation to process the payments, but that isn't the end of the story.

Miss M mentioned the Contingent Reimbursement Model (CRM) Code in her submissions but that doesn't apply here and nor do the APP scam reimbursement (ASR) rules introduced on 7 October 2024. These rules do not apply where payments are made between two

accounts controlled by the same customer, as was the case here.

I've taken into account the regulator's rules and guidance; relevant codes of practice, along with what I consider to have been good industry practice at the time. Having done so, I consider Bank of Scotland should have fairly and reasonably been on the lookout for the possibility of authorised push payment scams (amongst other things) at the time, and should have intervened if there were clear indications its customer might be at risk.

Bank of Scotland does have a difficult balance to strike in how it configures its systems to detect unusual activity that might indicate its customers are a higher risk of fraud. It would not be reasonable or possible for Bank of Scotland to intervene in every transaction it processes. I would expect intervention to be proportionate to the circumstances of the transaction.

In Miss M's case, I wouldn't have expected Bank of Scotland to intervene on the first payment, given that it was a very small payment and wouldn't have represented a significant risk of harm to Miss M.

Bank of Scotland did intervene on the second payment. It called Miss M on 27 June 2025 and asked her a number of questions about the payment. I consider that was an appropriate action to take, given the size of the payment on 27 June, the fact it was out of character with previous transactions and it was being paid to a cryptocurrency exchange, which Bank of Scotland should have recognised was an additional risk factor.

I consider the questions it asked were relevant and probing, although I think they could have gone further. For example, Miss M was asked about a loan she had taken out a short time before this payment was attempted. She was warned about work tasks scams and Bank of Scotland advised how these worked. Miss M indicated she was making the payment as an investment and was asked whether she was part of a social media group chat. Some of Miss M's responses weren't accurate and I think this made it more difficult for Bank of Scotland to uncover what was really happening.

The information and warnings Bank of Scotland gave Miss M were also relevant to her situation, but they didn't prevent her from making the payment. Bank of Scotland described work task scams in a reasonable level of detail – being contacted about remote working job opportunities, being asked to complete sets of tasks and then being asked to send money via a cryptocurrency exchange and loans being applied for to fund the payments. These features were similar to those Miss M had experienced so they ought reasonably to have resonated with her in my view.

I can also see from the copies of the messages Miss M exchanged with the scammer that she expressed her doubts about what was going on. For example, on 25 June she told the scammer that she didn't think the job sounded genuine and that she was starting to think it was a sophisticated scam. On 26 June she told the scammer she wasn't going to continue because she didn't think the platform was genuine. She said no job requires someone to send money to people they don't know. But even with those doubts and the warnings that were being provided by Bank of Scotland, Miss M made the payment.

A further intervention took place on 1 July 2025. Bank of Scotland asked clear, probing questions, in my view. For example, it asked if anyone had asked Miss M to lie to it, it asked what the payment was for, it asked about the purpose of loan she had taken out on 25 June, what cryptocurrency she was investing in and what she intended to do with it. Miss M's answers were not accurate.

In that call, Miss M was warned about customers being asked to complete tasks in order to

earn money through optimising apps or leaving reviews, involving cryptocurrency and people contacting customers through social media. Bank of Scotland asked whether she had been asked to carry out tasks in order to earn money. Miss M said she had not, which was also inaccurate.

I agree that Bank of Scotland could have intervened in some of the other transactions because there was an emerging pattern of transactions that had some similarity to known patterns of fraudulent transactions. But the circumstances set out above lead me to conclude that if Bank of Scotland had intervened in some of the other payments, Miss M is more likely than not to have continued to give Bank of Scotland inaccurate information and is unlikely to have acted on its warnings. While Miss M said the Investigator had no factual basis for drawing a similar conclusion, I consider it's a reasonable conclusion for me to reach based on what actually happened on the occasions Bank of Scotland did intervene.

I do understand Miss M's point that she was vulnerable, was being manipulated by the scammer and she was not deliberately misleading Bank of Scotland. She says she was coerced into doing so because she had already made significant payments via other banks and she feared she would lose her money. But that isn't enough for me to uphold her complaint. I need to be satisfied that Bank of Scotland was at fault and that this led to her loss.

While I have a great deal of sympathy for Miss M and I can see her distress coming through in the messages she exchanged with the scammer, I don't think Bank of Scotland could reasonably have prevented her loss. By the time she started making payments through Bank of Scotland, the messages with the scammer suggest she had already considered the possibility this was a scam. But I think there was a degree of desperation, understandably, to try and recover her money. That seems to have overridden the clear and relevant warnings that Bank of Scotland gave her, at the time of the second transaction and subsequently. So I don't think further intervention and warnings would have helped or prevented her losses. On that basis, Bank of Scotland's offer is more than I would award.

In terms of recovering Miss M's money, I don't think there was any reasonable chance of that. The payments were made to her own cryptocurrency account and paid on to the scammers promptly. If Bank of Scotland had contacted the cryptocurrency exchange, it's likely it would have confirmed that no funds remained.

While Miss M says Bank of Scotland's payment of £40 is not sufficient for the errors it made when communicating with her after the scam, on balance I think it is reasonable. I accept this situation has been very distressing, but largely due to the scam rather than Bank of Scotland's handling after the scam was reported. While Bank of Scotland didn't initially make an offer of compensation and later reviewed its findings, any errors were very minor in my view and not material.

Overall, I consider Bank of Scotland's payment of compensation was fair and reasonable in circumstances where I wouldn't have made an award because I'm not persuaded further intervention would have prevented Miss M's losses, for the reasons I've explained above.

My final decision

I don't uphold Miss M's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 10 February 2026.

Greg Barham
Ombudsman