DRN-5762318

The complaint

Mr H is unhappy Bank of Scotland plc (BoS) will not refund the money he lost as the result of a scam.

What happened

As both parties are aware of the details of the scam I will not repeat them in full here. In summary, Mr H fell victim to a job/task scam. He was contacted via WhatsApp and offered the opportunity to complete tasks (optimising apps) to earn commission. He was told that to access the tasks he first needed to make deposits in cryptocurrency. On 3 December 2024 he made a debit card payment for £3,011.32 to his existing digital wallet at a cryptocurrency exchange. From there he sent on the cryptocurrency he'd bought to the scammer's account, believing he was paying to access tasks. He had already sent smaller amounts from funds he already had in his digital wallet.

When he was told to send increasingly higher amounts, he realised he had been scammed. Mr H says BoS did not do enough to protect his money and should have invoked the Banking Protocol. He was vulnerable at the time. BoS says it made no error, it was not the point of loss and Mr H had authorised the transaction using a one-time passcode.

Our investigator upheld Mr H's complaint in part. He found BoS ought to have intervened as the payment was out of character. And a tailored warning would likely have broken the spell of the scam. However, as Mr H could have done more to prevent his loss the bank should refund 50% of the payment.

Mr H accepted this assessment. BoS did not and asked for an ombudsman's review. It said the payment was not unusual for Mr H's account: he had made higher debits and five other payments to the same recipient account, which was in his name, in the previous 12 months. Also, it was not the point of loss so should not be held liable.

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.

First, to address BoS's argument that it was not the point of loss: in the circumstances of this case, which can be characterised as a continuous scam without a break in the chain of causation, I am satisfied that it has a case to answer here and its acts and/or omissions can be considered when determining liability for the losses. I accept that Mr H had control of the account that the payment was made to. However, the transfer was made at the behest of the scammer, and by December 2024 multi-stage scams involving cryptocurrency were common, so it is reasonable to assess whether Mr H's loss could have been prevented by BoS.

There's no dispute that Mr H made and authorised the payment. Mr H knew who he was paying, and the reason why. At the stage he was making this payment, he believed he was transferring funds to allow him to buy access to tasks he would earn commission for

completing. I don't dispute Mr H was scammed and he wasn't making the payment for the reason he thought he was, but I remain satisfied the transaction was authorised under the Payment Services Regulations 2017. As BoS has evidenced, the debit card payment was authorised by Mr H using a one-time passcode, but it does not end there.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider that by December 2024 BoS should fairly and reasonably have:

• been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
• had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
• acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
• in some circumstances, irrespective of the payment channel used, taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
• been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving particularly the increase in multi-stage scams involving cryptocurrency, and the different risks these can present to consumers, when deciding whether to intervene.

To note as the payment was made by debit card the mandatory scam reimbursement rules that the Faster Payment Service introduced on 7 October 2024 do not apply in this case.

In this context I find BoS can be held liable in part for Mr H's loss. I'll explain why.

BoS argues that the payment was not unusual for Mr H's account for two reasons. In the previous 12 months he had other higher-value payments, and he had sent money to this account five times. So it had no reason to intervene. I disagree with this position and will explain why.

The combination of the value here and the nature of the recipient meant BoS ought to have identified that it presented possible financial harm to Mr H. His other high value payments did not involve cryptocurrency and the payments he had previously made to this account had an average transaction value of £217.20, with the highest being £500. It also swiftly followed a credit onto his account for £3,000. So, this payment was out of character. And as it was to an identifiable cryptocurrency provider there was an inherently higher risk, so BoS needed to pause before processing it.

This means I need to decide what the impact of a proportionate intervention would most likely have been. Since 31 July 2023, when the FCA's new Consumer Duty came into force, there has been an obligation on firms to avoid foreseeable harm to customers. The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23) gives an example of foreseeable harm:

"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"

This means a proportionate warning should ask a series of questions in order to try and establish the actual scam risk. And by December 2024 given the prevalence of job/task scams we'd expect a firm to have both questions and warnings tailored towards the key risks of those scams. So, in this case that could have included issues such as lucrative pay in exchange for little work; how did the customer find the opportunity; no employment contract; and the 'employer' asks for upfront payment.

Had BoS provided a tailored warning that highlighted these traits, then on balance, I think Mr H would most likely not have progressed with the payment. There is no evidence that he had been given a cover story by the scammer so I find it likely he would have answered the questions honestly. And there is evidence in the WhatsApp chats between Mr H and the scammer that he was already uncertain about what he was doing prior to making this payment. On 28 November 2024 he wrote *'to be honest started to be concerned as this can lock my fund'* and later that evening he paused before progressing with the 'job' saying *'not sure to be honest'* and to close the evening's messaging with the scammer *'not sure, I'll think about it'*. So, I find he would have taken a warning from BoS seriously and stopped the payment.

This means I find it is fair to hold BoS liable for the loss from the payment.

Should Mr H bear some responsibility for the overall loss?

I've considered carefully whether Mr H should hold some responsibility for his loss by way of contributory negligence. Accepting that he is not the fraud expert - that is the role of BoS, I do think he missed some clear signs that the opportunity might not be legitimate.

Having to pay money upfront to do a paid job is unusual and should have raised Mr H's suspicions, particularly as it seems Mr H had no contractual terms of employment to review and accept, nor was there any documentation setting out the terms of the payments. And to have to make such payments in cryptocurrency should also have been a red flag. The rate of pay was also too good to be true - £4,800 a month for two hours of work a day.

In the round, I have not seen that Mr H carried out an adequate level of independent checks before going ahead despite there being a number of red flags.

It follows I think the parties are equally liable.

I am therefore instructing BoS to refund 50% of Mr H's loss from the payment.

Did BoS do what it should to try to recover Mr H's money?

As the payment was made by debit card the opportunity to recover the funds would be through the chargeback scheme. But I don't consider that a chargeback claim would have had any prospect of success. There would have been no valid chargeback right given there was no dispute that the platform provided the service it 'sold' to Mr H – i.e. the cryptocurrency. Overall, this means I can't find there were any failings in this regard on BoS's part.

Finally, I am sorry to read about how Mr H was vulnerable at the time, and how the scam has made that worse. BoS was not aware at the time of the scam so I cannot fairly have expected it to have done anything differently. I can see it signposted various resources in its final response letter and I hope these have helped Mr H to rebuild his financial confidence.

Putting things right

• Refund 50% of £3,011.32 (so £1,505.66); and

• Pay interest on the above amount at the rate of 8% simple per year from the date of the payment to the date of settlement.*

*If BoS considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr H how much it has taken off. It should also give Mr H a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

I have found no grounds to make the additional compensatory award of £300 that Mr H asked for.

My final decision

I am upholding Mr H's complaint in part. Bank of Scotland plc must put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 3 December 2025.

Rebecca Connelley
Ombudsman