

The complaint

Mrs P complains that The Royal Bank of Scotland Plc (“RBS”) failed to prevent her from becoming a victim of a scam.

What happened

What Mrs P says

Mrs P said she received a phone call from someone (scammer) who claimed to be from her bank’s fraud department. I’ll refer to the scammer as J.

Mrs P said that she was initially suspicious of the call, but J knew personal details about her that convinced her he was a genuine employee of RBS.

J told Mrs P that her account was at risk from fraudulent activity and that he was going to help her secure it.

Mrs P explained that over the course of several hours, J persuaded Mrs P to send him copies of various identity documents including her driving licence and images of her debit card including the three-digit security number. Mrs P was told to download various apps that all related to crypto currency trading (although Mrs P said she wasn’t aware of their purpose at the time).

Mrs P was also given a “secure email address” and a password for it to use when opening the apps. In the background, loans were being applied for in Mrs P’s name, to which she was unaware of at the time.

Mrs P was told to move funds between various RBS accounts and did so, making several transfers between her accounts. At some point, a loan from a company I’ll refer to as B for £9,500 was approved and paid into Mrs P’s account. Another loan from a different company was also paid into a different bank account held by Mrs P that was later repaid.

There were then a number of transactions using her debit card (apart from one bank transfer) to various crypto currency accounts set up by Mrs P. Mrs P was required to confirm the payments using her bank’s app on her phone. It then appears that J accessed the crypto currency accounts and removed the funds to his own “wallet”, effectively making them disappear.

The table sets out payments related to this complaint:

	Date	Time	Merchant	Amount (£)
1.	29/01/2022	15:51	Coinbase	490.00
2.	29/01/2022	16:01	Coinbase	490.00
3.	29/01/2022	17:03	Betterborrow Loan	(£9,500.00)

4.	29/01/2022	17:45	Coinbase	950.00
5.	29/01/2022	18:37	Mercuryo.io	1,345.80
6.	29/01/2022	19:07	Mercuryo.io	1922.58
7.	29/01/2022	19:50	Banxa.com	1,900.00
8.	29/01/2022	17.22	open banking	900.00
			Total Paid	£7,998.38

J told Mrs P that he would call her the next morning to continue securing her account. Overnight, Mrs P became concerned about what had happened and called her bank. Mrs P was advised to speak with B and contacted them about the loan. Mrs P also reported the matter to the Police and Action Fraud.

What RBS said

RBS held numerous calls with Mrs P and told her to contact B about the loan. They didn't believe any of the funds lost were Mrs P's and as the loan was from another company, there was nothing further for them to do. Mrs P raised a complaint against RBS and after they again looked into the matter, they didn't uphold it. In their final response to Mrs P, they said:

- that J wasn't a member of their fraud team.
- The loan was from another company.
- Her RBS account wasn't involved.

The investigation so far

Mrs P remained unhappy with how RBS had dealt with her issue and brought her complaint to the Financial Ombudsman Service for an independent review. It was looked into by one of our investigators who asked for information from both parties.

Mrs P explained what had happened and copies of some of the apps she'd opened. She didn't provide any other information related to her interaction with J.

RBS provided details of the transactions and copies of her statements. They also provided numerous phone calls they'd had with Mrs P.

After considering the evidence, the investigator concluded that some of Mrs P's testimony was inconsistent – whether or not she opened the crypto currency accounts and was/ was not responsible for making the payments. It was also thought that the various money transfers/ incoming loan and payments to crypto currency merchants were, at some point, unusual enough for RBS to have intervened. But, the investigator didn't think it would have stopped Mrs P from making the payments and didn't uphold her complaint.

Mrs P disagreed with the investigators outcome and was concerned about some of the conclusions reached that indicated Mrs P had changed her story.

As no agreement could be reached, the complaint has now been passed to me for a

decision.

I issued my provisional findings on the merits of Mrs P's complaint on 2 October 2023. In my provisional findings, I explained why I intended to partly uphold Mrs P's complaint and offered both sides the opportunity to submit further evidence or arguments in response. An extract of that decision is set out below and forms part of this final decision:

What I've provisionally 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.

If there's something I've not mentioned within this complaint, it isn't because I've ignored it, it's because I'm satisfied that I don't need to comment on every individual argument to be able to reach what I think is the right outcome.

I was sorry to hear of the impact this scam has had on Mrs P. The first matter I need to address is the authorisation of the payments. Having considered all the available evidence on this complaint, including all the phone calls and evidence from another linked complaint, I found it difficult to precisely pin down what actually happened during this scam.

At various times, Mrs P has given slightly conflicting statements about her involvement in the loan and subsequent payments made (principally) using her debit card. I would expect some variations in a complex story that's retold a number of times over a number of months, so I don't draw much inference from this, but it has made it difficult to unpick what actually went on.

I also noted a lack of evidence of Mrs P's contact with J – even though she mentioned a messaging service and that she sent him details of her documents. I was surprised that none of these were provided, so if they are still available, I'd encourage Mrs P to provide them.

When assessing the overall evidence, I do think that Mrs P was caught up in a scam that started out by persuading her that her account was at risk. It then went on to moving funds from a loan to various crypto currency accounts. Also, I think the evidence points to Mrs P being involved in the payments herself using her card. So, even though she didn't intend to pay a scammer, the payments were 'authorised' under the Payment Services Regulations.

RBS had an obligation to follow Mrs P's payment instructions, and Mrs P is presumed liable for the loss in the first instance. But that's not the end of the story.

RBS also has to be on the lookout for, and help to prevent, payments that could involve fraud or be the result of a scam. Although, there has to be a balance struck between RBS identifying payments that may indicate a customer is potentially at risk of financial harm and then responding appropriately to those concerns – and ensuring minimal disruption to legitimate payments.

Should RBS have prevented these payments from being made?

I think the activity on Mrs P's accounts was, when compared to how they normally operated, unusual in that they didn't receive loans or make payments to crypto currency merchants in a relatively short space of time.

Here, Mrs P was also asked to make transfers between some of her accounts which also muddled the picture of what was happening, and I appreciate she later said she wasn't aware of the various funds at her disposal. So, I can see that the account was operating outside of its normal usage and at some point, would have expected RBS to take some

action (such as blocking payments and contacting Mrs P.)

None of the payments on their own would likely have been spotted by the banks, it's the accumulation and timing that are unusual. Plus, receiving a loan and immediately making payments to crypto merchants can be an indicator of scams. So here, I think payment number 6 in the table above is the point that I think RBS should have intervened. That's because by this time, several earlier transactions increasing in value had been made, after receiving a large loan into the account.

It was previously suggested that an intervention wouldn't have made a difference. I don't think that's the case and if RBS had intervened, such as a phone call to check what was happening, Mrs P would probably have explained what she'd been told (about the threat to her account). RBS would have easily been able to determine they weren't calling her (as J claimed) and determined she was likely been scammed. I think this piece of information would have stopped the scam in its tracks – there's also no evidence to think that Mrs P was actively engaged in the scam herself or asked to lie, just a victim who was so confused by the scammer that she appeared to be acting on his every instruction without having chance to think about it.

I think that RBS missed an opportunity to intervene when they should have done, but I also need to assess what type of refund is both fair and reasonable.

Did Mrs P contribute to some of the losses herself?

In cases such as this, an assessment also has to be made to understand if the complainant's actions (Mrs P) contributed to the losses – so called contributory negligence. If so, it wouldn't be fair to ask RBS to refund 100% of them.

There are a number of factors here which I think contributed to the loss which I think Mrs P should bear responsibility for.

- Mrs P set up the crypto currency apps herself – she says she was unaware of what they were at the time, but I don't think this is a plausible explanation. These apps are only for one main purpose and that's crypto currency purchase and trading. I think it's unlikely she wasn't aware of what they were.*
- It's likely she was aware of the loan and the spending from her account was in excess of her available funds. It doesn't make sense that Mrs P made over £7,000 in payments when that money simply wasn't available in her accounts at the time.*
- She was told the original call was to protect her money, so why was Mrs P making payments in excess of her own funds from a recent loan to crypto currency merchants?*

The overall picture from this leads me to the conclusion that Mrs P acted in a way that contributed to the losses. I think there were several unusual aspects to this which Mrs P could have questioned and her involvement in the payments led to the loss of funds from the loan.

I think that Mrs P should bear equal responsibility (50%) for the losses, and that's only from the point that I think that RBS should have intervened (6 in the table above).

My provisional decision

I'm currently intending to uphold this complaint and recommend that:

- *RBS refund 50% of the disputed transactions from 6 onwards in the table above. I'd note here that I've not seen the timing on the £900 payment – so if it occurred prior to payment 6, then I don't currently intend to include it in the redress calculation. I'd ask RBS to put a time against this transaction if possible. If that's not possible, then I intend to include it in the redress calculation as it would be unfair to exclude it without evidence it happened before I think RBS should have intervened.*
- *I've also considered (in relation to the outcome of this complaint) the linked complaint concerning the repayment of the loan itself.*

I invited Mrs P and RBS to give me any more evidence and information they wanted me to consider before issuing my final decision. RBS accepted my provisional decision and provided payment details for the open banking payment (8 in the table above) which showed it took place prior to payment 6 in the table above, so for the purposes of this complaint, it won't be included in the final refund figure. Although RBS have offered to settle the complaint in line with the provisional decision, I'm issuing a final decision in order to explain the timing of payment 8 (and how it impacts the final settlement) and to take into account the additional comments received.

Mrs P had no further evidence for me to consider but reiterated that she had no understanding of crypto investments at the time of the payments, and she was completely taken in by the scammer.

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, and as neither party had anything further to add, I see no reason to reach a different conclusion. So, this final decision confirms the findings set out in my provisional decision.

I appreciate Mrs P's further comments, and I recognise she was the victim of a cruel scam, but my assessment of her complaint (detailed in my provisional decision) sets out the various elements of the situation. This has led me to what I think is a fair and reasonable conclusion that both parties should share some responsibility for her losses.

Putting things right

As the open banking payment (number 8 in the above table) was shown to have been made prior to the point I think that RBS should have intervened, it won't be included in the calculation for the refund.

So, in order for the complaint to be finalised, RBS should now refund 50% of the payments from number 6 onwards in the above table (being payments 6 & 7).

My final decision

My final decision is that I uphold this complaint, in part, against The Royal Bank of Scotland Plc and they're required to settle the complaint as detailed above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs P to accept or reject my decision before 1 December 2023.

David Perry
Ombudsman