DRN-5014560

The complaint

Mr M has complained that The Royal Bank of Scotland Plc ("RBS") failed to protect him from falling victim to a scam.

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

Mr M was exposed to an investment-related scam after a friend introduced him to an opportunity to invest in a new type of cryptocurrency, but the scheme he invested in was fraudulent. He sent payments to purchase the alleged cryptocurrency between October and November 2023.

Mr M explains that he was new to investing and following extensive research, he believed he was dealing with a genuine investment company. He says that although he was sending funds to a cryptocurrency exchange, and the payments were out of line with his usual account activity, RBS failed to ask any questions or give him appropriate warnings about the risks involved with cryptocurrency. It appears from the information provided that Mr M was added to a group chat in a messaging app, where other participants discussed their successes investing in this scheme.

The payments Mr M sent to the cryptocurrency exchange, as part of the scam, were as follows:

	Date	Amount (£)
1	17/10/2023	250
2	23/10/2023	250
3	26/10/2023	1000
4	26/10/2023	1000
5	26/10/2023	1000
6	30/10/2023	1000
7	30/10/2023	1000
8	01/11/2023	1000
9	01/11/2023	1000
10	13/11/2023	35
11	13/11/2023	500
12	13/11/2023	500
13	14/11/2023	500
14	14/11/2023	500
15	22/11/2023	500

16	22/11/2023	500
17	24/11/2023	20
18	27/11/2023	50
19	27/11/2023	50
	Total	**10,705**

Mr M realised what had happened when his account became "locked for maintenance" and he then says he saw social media posts alerting him to the scam.

Mr M reported the scam to RBS on 25 November 2023. RBS said it wouldn't reimburse Mr M for the losses, so Mr M made a complaint. In its response RBS said it shows warnings before customers make payments using online banking, and Had Mr M followed the warning, he wouldn't have fallen victim to the scam. RBS also said it wasn't able to reimburse Mr M for his losses as all of the funds were sent from RBS to another account in Mr M's name, so RBS wasn't the point at which the loss happened. It directed Mr M to raise his complaint with the provider of the account the funds were sent to the scammer from.

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

Our investigator considered everything and thought the complaint should be upheld. He said RBS should've intervened at the point Mr M sent the fifth payment, as a pattern had emerged that was typical of a scam and out of line with Mr M's usual account activity. But he also thought Mr M should share the responsibility for what he lost, as he could've done more to protect himself from what happened.

RBS accepted the investigator's view and agreed to pay Mr M what he suggested.

Mr M didn't accept the investigator's view as he didn't agree that liability for the losses should be split equally between Mr M and RBS. He noted that the scam was so sophisticated that it affected over 500,000 victims.

As the case hasn't been resolved it's 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.

Having done so I'm upholding Mr M's 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 M authorised these payments from leaving his account. It's accepted by all parties that Mr M gave the instructions to RBS and RBS made the payments in line with those instructions, and in line with the terms and conditions of Mr M'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.

RBS says the payments were made via a third-party provider using Open Banking. Open Banking is a system that allows consumers to securely share their financial data with authorised third-party providers, such as budgeting apps other payment services. The idea is

to give people more control over their financial information and allow them to use it to access better deals, new products, or services that can help manage their money.

With open banking, banks are required to provide access to this data (with the customer's permission) through secure technology called APIs (Application Programming Interfaces). Although in its final response letter RBS said it showed Mr M warnings before the payments were made, RBS has since said that as Mr M made the payments from his RBS account via Open Banking, it didn't provide any warnings, nor would its system record any of the beneficiary details. It also says that none of the payments Mr M made were flagged as suspicious or unusual.

But the fact that Open Banking features in this payment journey doesn't mean RBS didn't need to be aware of signs of financial harm to Mr M. Although using Open Banking means the payments was likely initiated by the cryptocurrency exchange where Mr M held his cryptocurrency account, the payments were sent from Mr M's RBS account, so RBS was still responsible for having effective systems and controls in place to monitor and identify potential risks as part of that payment journey.

As our investigator pointed out, by the time these payments were sent in late 2023 cryptocurrency scams were extremely well-known in the industry. The cryptocurrency exchange Mr M sent the payments to is well-known and easily identifiable from his statements, so I'd have expected RBS to identify this and to be on alert – especially where so many high value payments were sent to the payee in a relatively short space of time. Additionally, the values of some of the payments were higher than any other payments Mr M had made in the preceding six months (with the exception of one other to his own account at a different bank). So RBS should've intervened to understand more about the payments, and give Mr M sufficient warnings to allow him to be informed about, and potentially avoid, the financial harm he experienced as a result.

Turning to the point at which I think it would've been reasonable for RBS to intervene, I've kept in mind that it wouldn't be practical, nor convenient, for RBS to block or ask questions about every payment made from its customers' accounts. But bearing in mind the pattern of payments Mr M made, and the values of those payments, I agree that by the fifth payment RBS should've stepped in.

The first two payments were relatively low in value, and not particularly out of character for Mr M's account. By payment three the transaction amount of £1,000 was somewhat unusual, but I don't think that alone means RBS should've intervened, and I also think the same for the following payment. But by the fifth payment, Mr M had sent three payments of £1,000 on the same day. Although this might not always mean a customer is at risk of financial harm, the fact the payments were an unusual amount and being made to an identifiable cryptocurrency exchange means RBS should've been alerted to what was happening by this point.

It's important to note that an intervention can take many forms – and doesn't necessarily have to be a human intervention. So as an example, RBS could've asked Mr M questions and shown him specific written warnings about the payments. But the fact RBS didn't intervene at all means Mr M continued making the payments, and it's my view that this could potentially, and likely, have been avoided.

If RBS had intervened – such as by asking Mr M for the purpose of the payments – I haven't seen anything to suggest Mr M wouldn't have been honest with his answers. And if RBS was made aware that Mr M was buying cryptocurrency on the advice of someone over a messaging app, I think RBS would've been able to easily identify this as a well-known scam and would likely have been able to prevent the losses that Mr M experienced as a result.

With all of the above in mind, like our investigator, I've decided that RBS needs to refund Mr M for what he lost from the fifth payment onwards.

Is Mr M responsible for any of his losses?

Despite RBS's shortcomings, I've also thought carefully about the circumstances surrounding these payments, in order to decide whether I think Mr M could reasonably have prevented any of the losses he's experienced. I know Mr M doesn't believe he should be jointly liable for the losses, but I'm afraid I don't agree. I'll explain why.

I can't see that Mr M did much research on the alleged opportunity he was investing in. And the fact it was recommended to him by a friend who was being financially rewarded for doing so, isn't a typical or particularly failsafe way to choose an investment.

I can also see that the returns Mr M expected to receive – based on discussions in the group chats – were unreasonably high. And Mr M doesn't appear to have received any paperwork or documentation showing what he'd invested, or the details of what he should expect in return, or when. So I think he should've exercised more caution before making the payments that resulted in his losses.

Whilst I understand this scam affected many more people than Mr M, that doesn't take away from the fact that Mr M could've done more to satisfy himself the investment he was making was genuine. As an example, messages in the group chat that Mr M was part of explain how one alleged investor, after investing an initial 500USDT (around £375 at the time of writing), was due to receive 890,000USDT (£667,500 at the time of writing) after one year. This is unrealistically high and should've been a red flag for Mr M.

Whilst I understand Mr M may be disappointed that I'm not asking RBS to refund everything he lost, I hope my decision sets out why I think that's fair in the circumstances.

Putting things right

To put Mr M back in the position he'd have been in had RBS done what it should've, RBS needs to:

- Refund Mr M 50% of the value of the payments he sent from the fifth payment onwards, and;
- Pay 8% simple interest on each amount, from the date each payment left Mr M's account until the date of settlement*.

*If RBS considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr M how much it's taken off. It should also give Mr M a tax deduction certificate if he asks for one.

My final decision

I uphold Mr M's complaint and require The Royal Bank of Scotland Plc to put things right as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 22 October 2024.

Sam Wade
Ombudsman