DRN-4474610

The complaint

Mr S complains that The Royal Bank of Scotland Plc didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In May 2021 Mr S came across an advertisement on social media for an opportunity to invest in cryptocurrency with a company I'll refer to as "L". He clicked on the advertisement, which was endorsed by two well-known celebrities and was required to input his contact details.

Mr S googled L and couldn't see any bad reviews, noting the website featured "about us," "legal," "financial," "support," and, "contact us" sections, and had photographs of stock trades showcasing currency values. He sent a copy of his photo ID and a utility bill as proof of address and received an email confirming his registration had been successful.

He then received a phone call from someone claiming to be a broker working for L, who I'll refer to as "the scammer". The scammer told him he'd been trading for several years, and Mr S thought he seemed knowledgeable and professional. He also emailed Mr S several case studies of success stories and required him to sign a contract electronically.

The scammer instructed Mr S to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. He told him to send money through an electronic money institution ("EMI") I'll refer to as "W" and then to an e-wallet on L's website. He paid an initial fee on 24 May 2021 and between 24 May 2021 and 6 September 2021, he made 42 transfers to W from his Bank of Scotland account totalling £144,698.

Mr S could log into his trading account every day and see his balance increase or decrease. But when he asked to make a withdrawal, the scammer told him it would take over a month and that he would have to open another e-wallet because the bank would ask questions if he transferred such a large amount into his bank account. He was also asked to pay 'reflection fees' within 24-48 hours or he would incur further charges and might not have access to his funds.

Mr S contacted Bank of Scotland when he realised he'd been scammed. He said the payments weren't flagged and it didn't provide adequate scam education. But Bank of Scotland said it was unable to accept any liability for Mr S's loss because it acted on his genuine instructions to make the payments. It said he had failed to carry out due diligence when using a cryptocurrency wallet and it wasn't the point of loss.

It said it places appropriate and relevant warning messages across its Online Banking Facility to warn customers about scams and information is made available on its websites

and within its branches. It also said messages are displayed before making a payment or adding a new payee and the customer must confirm they have read and understood the advice and are satisfied they have taken relevant steps.

It explained if a transaction matches a known fraud trend, a security check will be generated but there were no concerns about the validity of the payments. And it said it was unable to recover the funds as they were made to Mr S's own account and the payments successfully reached the wallet before being withdrawn.

Mr S complained to this service with the assistance of a representative. He said Bank of Scotland failed to intervene even though the payments were completely out of character. And if he'd known the investment was a scam he wouldn't have gone through with the payments. He said it should have asked him further questions and provided advice on the risk of fraud and that he wanted it to refund the money he'd lost plus £500 compensation.

Mr S's representative said Bank of Scotland should have intervened as he made 42 payments to a new payee linked to cryptocurrency and it was unusual for him to have continuously made such large payments. They said Bank of Scotland's systems should have triggered on 24 May 2021, when Mr S added a new payee and paid £5,000 to the scam.

They said it should have asked why he was making the payments, who he was trading with, how he found out about the company, whether he'd researched the company, whether he'd checked the Financial Conduct Authority website, whether he'd been promised unrealistic returns and whether he'd made any withdrawals, and as he hadn't been coached to lie he'd have said he was being advised by a broker and that he hadn't made any withdrawals. He could then have been directed to attempt a withdrawal, which would have uncovered the scam.

Bank of Scotland further commented that Mr S had a similar complaint about payments debited from another Bank of Scotland account and it has questioned why he would continue to trade in cryptocurrency having already been scammed. And it has questioned why he didn't question why he was told he'd have to make a payment to make a withdrawal.
It said it was unable to refund Mr S under the Contingent Reimbursement Model (CRM) code as Mr S had paid an account in his own name and the returns that he has received from another investment company indicate he is an experienced investor.

Our investigator didn't think the complaint should be upheld. She said the CRM code wouldn't apply to the payments Mr S had made to accounts in his own name. She explained there were five transfers which weren't made into accounts in Mr S's name but there was no evidence they were made as a result of a scam.

Our investigator explained Mr S made most of the initial payments (payments 1, 3, 4, 5, 6, 7) in branch. She explained there was no record of the conversations that took place on each of those occasions, but she was satisfied Bank of Scotland had asked relevant questions on 24 May 2021 or 26 July 2021 (he paid £5,000 on both dates so the notes could relate to either transaction) and on 15 July 2021 when he'd made payments of £5,000 and £15,000. She noted Bank of Scotland had asked relevant questions and Mr S was asked if he was making an investment, which he denied. And the notes for 15 July 2021 showed he said he wanted to send funds back to his Wise account and that he'd had a discussion with the fraud team.

Our investigator explained she didn't think the payments that followed were unusual for the account, as they were lower value and to Mr S's accounts with W and R, which were existing payees. She accepted Bank of Scotland could have done more when Mr S made the transfers in-branch but based on what actually happened when it provided a meaningful

warning in relation to the previous scam, she didn't think a better intervention in the branch would have made a difference.

Our investigator explained that during the call which related to the first scam, Bank of Scotland told Mr S how cryptocurrency scams operated, but he proceeded with the payments, diverting his funds into another account in his name and paying the same beneficiary Bank of Scotland had told him was a scam. So she was satisfied that if Bank of Scotland had refused to make the payments for the second scam, he would have gone ahead via different means.

Our investigator also noted Mr S had misled Bank of Scotland about the reason for the payments when he'd made the £5,000 in branch on 24 May 2021 or 26 July 2021, so she didn't think better questioning would have uncovered the real reason for the payment. And he'd gone ahead with the payments after being given meaningful warnings on both occasions while in the branch.

She also explained there were multiple payments in and out of Mr S's accounts from legitimate investment companies prior to the scam period and he had received credits from a well-known investment company. So she didn't accept he was an inexperienced investor, therefore he should have been concerned that L didn't have a greater online presence. And considering his recent dealings with Bank of Scotland, she thought he should have been more concerned about what he was being asked to do. Because of this, she didn't think there was anything Bank of Scotland could have done to prevent Mr S from continuing with the payments.

Mr S has asked for the complaint to be reviewed by an Ombudsman. His representative has argued that Bank of Scotland never said it was worried about the payments and had the bank told him it thought this was a scam, he wouldn't have proceeded. They also argued that Bank of Scotland should have invoked the banking protocol.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr S has been the victim of a cruel scam. I know he feels strongly about this complaint and this will come as a disappointment to him, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. Bank of Scotland has said the CRM code didn't apply in this case because Mr S was paying an account in his own name and I'm satisfied that's fair. I'm also satisfied that Mr S has failed to produce evidence that payments out of the account during the scam period which weren't to accounts in his own name were payments to the scam.

I'm satisfied Mr S 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr S didn't intend his money to go to scammers, he did authorise the disputed payments. Bank of Scotland is expected to process

payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Bank of Scotland could have done more to prevent the scam from occurring altogether. Bank of Scotland ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr S when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Bank of Scotland to intervene with a view to protecting Mr S from financial harm due to fraud.

The payments didn't flag as suspicious on Bank of Scotland's systems, but payments 1, 3, 4, 5, 6, 7 were made in branch and so I've considered whether Bank of Scotland did enough during those interactions. There is a record of what took place when Mr S attended the branch to make a £5,000 payment to the scam. The note is undated but Mr S made payments of £5,000 on 24 May 2021 and 26 July 2021 and so I'm satisfied the note must relate to either of those dates. The note shows Mr S was told he was being asked questions to ensure he wasn't being scammed. He was asked about the payment and said he was moving his savings to his own account. He was warned about impersonation scams and safe account scams and he confirmed the payment wasn't for an investment.

Because Mr S didn't disclose that he was making the payments for an investment or to buy cryptocurrency, Bank of Scotland didn't have enough information to enable it to identify that he was being scammed or to provide a warning that was tailored to cryptocurrency scams. I agree with our investigator that he could have been asked more probing questions, but as he wasn't open about the purpose of the payments I don't think this would have made a difference to the outcome.

There is a further record of the interaction that took place on 15 July 2021 when Mr S attended the branch to pay £15,000 to the scam. On this occasion he said he was sending money back to the account he held with W, which was an existing payee. It was identified that he had previously invested in cryptocurrency and there was some discussion about previous dealings he'd had with the fraud department. He was warned again about impersonation and safe account scams and the payment was processed.

I've considered the nature of this interaction and I'm satisfied that Bank of Scotland was prevented from identifying that Mr S was the victim of a scam because he failed to disclose that he intended to make an onwards payment from the account he held with W and that he planned to invest in cryptocurrency. Again, I accept that based on the amount of the transaction he should have been asked more probing questions, but as he wasn't open about the purpose of the payment, I don't think this would have made a difference.

While there is no evidence of what took place on the four other occasions that Mr S attended the branch, I think it's likely the interactions would have been very similar and there's nothing to suggest he'd have disclosed any more information about the circumstances of the payments. And even if he had done, I don't think Bank of Scotland could have said anything which would have made a difference to Mr S's decision to go ahead with the payments and I don't think this was a case where it should have invoked the banking protocol.

This is because he went ahead with the payments on 24 May 2021/26 July 2021 and 15 July 2021 having been given a scam warning. And when he spoke to Bank of Scotland on 11 May 2021 about another scam, he went ahead and made payments to that scam from a different account having been given a tailored warning about cryptocurrency scams and

directions to make further checks. He was also blocked from making further payments to the payee, yet he got around that by making payments from an account he held with another bank. Because of that, I don't think there's anything Bank of Scotland could reasonably have done to prevent his loss.

Finally, I've considered the nature of the payments which didn't happen in branch in the context of whether they were unusual or uncharacteristic of how Mr S normally ran his account and I don't think they were. All the payments were to legitimate account in Mr S's own name and most of them were for relatively small amounts. There was a payment of £5,000 on 22 December 2021 but this wasn't unusual for the account and by this time Mr S had been making payments in this way for a sustained period of several months, so it wasn't suspicious. So, I don't think Bank of Scotland missed any further opportunities to intervene.

Compensation

Mr S isn't entitled to any compensation because the upset was caused by the scammers, and I haven't seen any errors or delays in Bank of Scotland's investigation.

I'm sorry to hear Mr S has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Bank of Scotland is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 6 March 2024.

Carolyn Bonnell
Ombudsman