DRN-4172498

The complaint

Mr G 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.

Scam 1

In May 2022, Mr G received an unsolicited message via Telegram about an opportunity to invest in cryptocurrency. He was interested because the interest rates on his bank account were low and so he completed an online form.

On 6 June 2022, he was contacted by someone I'll refer to as "the scammer" and they exchanged photographs and messages about their lives, which led Mr G to believe she was interested in a relationship.

After a while, the scammer told Mr G she'd been investing in cryptocurrency. She told him she earned £18,000 per month in interest from the investment and if he invested £5,000, he would earn £2,000 in interest. She said he could begin by investing as little as £200. She advised him to open an account with an investment platform which I'll refer to as "M", which he researched online and found no cause for concern. He was also reassured because the scammer told him she was being advised by a world-renowned economist about whom he was able to find lots of information online.

The scammer asked him to first purchase cryptocurrency and then load it onto an online wallet. Between 6 June 2022 and 22 March 2023, he made eight faster payments from Bank L to two cryptocurrency merchants totalling £40,805. And during the period, he received two credits totalling £1,030.26.

Mr G remained in daily contact with the scammer and was able to see live updates about his investment on the trading platform. On 29 June 2022, the scammer showed him how to open an account with a cryptocurrency exchange company which I'll refer to as "C" and he successfully withdrew £534.11 into Bank L.

On 4 July 2022, Bank L blocked a payment of £2,400 to another cryptocurrency merchant which I'll refer to as "F", and it was concluded that he'd been scammed. So, on 9 July 2022, he opened and account with Bank S because he was keen to carry on investing. Between 11 July 2022 and 8 September 2022, he made ten faster payments and three debit card payments from Bank S to two cryptocurrency merchants and one debit card payment to an account he held with an EMI I'll refer to as "R". These payments totalled £52,126.55.

When Mr G ran out of money, he cashed in an ISA and some Premium Bonds and transferred funds into Bank S before transferring £10,000 to F on 4 August and 13 August 2022.

On 17 August 2022, he was contacted by a man who he understood was the scammer's advisor. The advisor said the scammer had told him he wished to make a withdrawal from the mining pool and that if he could invest a further $35,000 it would force his mining pool to over $100,000.00. He also said that if he didn't invest further funds he would be 'kicked out'. Mr G eventually realised he'd been scammed in September 2022 when he was told he would need to pay $20,000 for a 'tutor fee'.

Scam 2 –

In July 2022, Mr G came across advert on social media for another investment company which I'll refer to as "B". The advert had a celebrity endorsement and he thought it was genuine because he believed fraudulent adverts would be filtered out by the platform. Mr G checked B's website and noted it had 4.5 stars on Trust Pilot. He clicked on the link and completed the online form and was immediately contacted by someone I'll refer to as "the scammer" who told him he could invest in cryptocurrency, oil, and gold. He told the scammer about the other investment and that he was being pressured into making further payments. The scammer seemed very knowledgeable and said he'd be able to recover the money he'd lost.

The scammer told him to open an account with B and that the more he invested the more money he would make. He would also recover any money he'd lost on the other platform. Mr G told the scammer he didn't have any money to invest, so the scammer advised him to take out a loan and to download AnyDesk remote access software so he could help him with the application. On 12 September 2022, Mr G was granted a £20,000 loan, which was paid into Bank L before he transferred two payments to C. On 14 September 2022, he received a £15,000 loan into Bank L before he transferred it to C. And on 20 September 2022, he received a further loan for £10,000 into his RBS account, before he made two transfers C for £5,000 each on 21 September 2022 and 27 September 2022.

He realised he'd been scammed when he tried to make a withdrawal and was told he'd have to send further funds and pay taxes. He told the scammer he couldn't make any more payments and they eventually lost contact.

Mr G complained to RBS when he realised he'd been scammed, but it refused to refund any of the money he'd lost. It said it was unable to refund the payments because he'd paid cryptocurrency wallets in his own name and so it wasn't the point of loss.

It said that before a consumer makes a transfer or adds a new payee, a message is displayed on its online banking facility to warn customers about scams. A tailored scam warning is displayed, and the customer must confirm they are confident they have read and understood the advice and they are satisfied they have taken relevant steps.

It said it had no concerns about the validity of the payments and the transfers didn't result in Mr G's loss. Further the payments weren't covered by the Contingent Reimbursement Model ("CRM") code because the payments were to an account in Mr G's name.

Mr G wasn't satisfied and so he complained to this service with the assistance of a representative who said it had failed to raise a chargeback dispute. The argued he'd authorised the payments in the belief that the scam was genuine. His representative said Mr G made two large payments to a new payee which was linked to cryptocurrency, and this

was unusual, especially considering the frequency of the transactions and the fact the account was left significantly depleted. So, RBS should have intervened.

They said it should have contacted Mr G and asked him why he was making the payment, how he found out about the company, whether he'd researched the company, whether he'd been promised unrealistic returns and whether he'd made any withdrawals, and had it done so it would have realised he was likely falling victim to an elaborate Advance Fee scam because he would have fully explained what he was doing and that everything had originated from a broker.

RBS said that when Mr G first contact it to report the scam, it said the payments were made to a wallet in his own name so he should contact the wallet provider directly. It said that assuming he selected 'Making an Investment' when he made the payment, the warning message would have prompted him to go to the Financial Conduct Authority ("FCA") website and to look at Take Five which is a trusted organisation providing guidance on how to stay safe from fraud and scams. It also said the payments weren't covered under the Contingent Reimbursement model ("CRM") code.

Our investigator didn't think the complaint should be upheld. He noted that as Mr G had opened the account a few days before the payments were made, there was almost no account history to compare the payments with, so they couldn't be considered as unusual or suspicious. And as Mr G didn't speak to or interact with RBS staff at the time of the payments, it didn't miss an opportunity to identify that they were being made in relation to a scam.

Mr G has asked for the complaint to be reviewed by an Ombudsman. His representative accepts there was no account history, but they've argued that the first significant payment into the account was a £10,000 loan, swiftly followed by two £5,000 payments out of the account, which should have been cause for concern, particularly as the payments out were to a cryptocurrency merchant. They've argued that the sequence of setting up a new account and receiving a large credit before making two payments to a cryptocurrency merchant is indicative of fraud and RBS should have intervened.

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, for similar reasons. I'm sorry to hear that Mr G 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 Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr G says he's fallen victim to, in all but a limited number of circumstances. RSB has said the CRM code didn't apply in this case because Mr G paid an account in his own name, and I'm satisfied that's fair.

I'm satisfied Mr G '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 G is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr G didn't intend his money to go to scammers, he did authorise the disputed payments. RBS 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 RBS could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange. RBS 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 G when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect RBS to intervene with a view to protecting Mr G from financial harm due to fraud.

The payments didn't flag as suspicious on RBS's systems. There was no account history to compare the payments with because it was a newly opened account and Mr G was paying a legitimate cryptocurrency exchange in his own name. But he received a £10,000 loan into the account before making two payments out very quickly afterwards, and I think this should have triggered an intervention because of the size of the payments and the fact that this type of activity can be indicative of fraud. So, I think RBS missed an opportunity to intervene.

Because Mr G made a payment of £5,000 to a cryptocurrency merchant the day after receiving loan funds into the account, he ought reasonably to have been presented with a written warning which was tailored to cryptocurrency scams. However, I don't think this would have made any difference to his decision to go ahead with the payments because when Bank L intervened on 4 July 2022, the call handler said she was certain he was being scammed and not to make any further payments to the scam.

Unfortunately, he continued to make payments to the first scam from Bank S having been told by Bank L that he'd been scammed. So, I don't think a written warning from RBS on 21 September 2022 would have made any difference to his decision to make payments from that account, especially as a written warning wouldn't have had as much impact as the conversation with Bank L in July 2022.

I've thought about whether anything had changed since 4 July 2022 when Mr G was told by Bank L that he was being scammed which might mean he'd have been more inclined to listen to a tailored warning and advice on due diligence, but I don't think it had.

Mr G has further commented that he doesn't recall being warned by Bank L about scams and therefore the warning it gave ineffective. His representative has also argued that Mr G was honest about the fact he was investing in cryptocurrency, and he should have been asked more probing questions.,

I accept Mr G responded to Bank L's questions honestly, but, whether or not he now recalls the warning, he continued to make payments to the scam after being told unequivocally that he was being scammed. So even though I think RBS missed an opportunity to intervene, I don't think a written warning would have made any difference to his decision to go ahead with the payments and so I don't consider this was a missed opportunity to have prevented his loss.

Compensation

Mr G isn't entitled to any compensation.

Recovery

I don’t think there was a realistic prospect of a successful recovery because Mr G paid an account in his own name and moved the funds onwards from there.

I’m sorry to hear Mr G has lost money and the effect this has had on him. But for the reasons I’ve explained, I don’t think RBS 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 G to accept or reject my decision before 25 July 2024.

Carolyn Bonnell
Ombudsman