

## **The complaint**

Miss S complains that The Royal Bank of Scotland Plc (RBS) wouldn't refund money she lost in an investment scam.

## **What happened**

*What Miss S says:*

In January 2022, Miss S read an article about bitcoin investment – and how someone had made good returns. She went online and looked at a bitcoin trading platform and was then contacted by someone who said he was an investment advisor.

She was told how to set up an account with an investment platform ('B') and was given an account manager, who then contacted her. Miss S researched the website of B and it looked credible. She saw reviews from other customers of B – who said they were making good returns. The account manager said she could double her money within six months.

He coached her to set up an app for the investment platform (I will call the investment company 'B') and helped Miss S open an account with a payment services provider (which I will call PSP1). This was a 'crypto wallet' for the purposes of receiving money from a bank account and then transferring it to B.

Miss S made a number of small trades – by sending funds from her bank accounts to PSP1 and then to B. And saw her investment growing by looking at her account in B's website. She was encouraged to make further investments – and sent £15,610 from another bank. These payments are the subject of a separate complaint brought to our service.

The account manager sent her WhatsApp messages every day to make sure she could see the 'profits' she was making. And sent regular investment reports. He pressurised her to invest more money.

In March 2022, she received a warning from PSP1– to say her account had been frozen due to suspected suspicious activity. The account manager told her how to respond to PSP1, and she was then encouraged by the account manager to open another account with a second payment services provider ('PSP2'). The account manager showed her how to transfer money from her bank accounts to PSP2, and then onto the investment company.

Miss S then made further payments from another bank account to PSP2 and then to B - totalling £17,290. These payments are the subject of another complaint brought to our service.

Miss S was in touch with the account manager by WhatsApp messages from January 2022 to June 2022.

In May 2022, the account manager said the bitcoin market was crashing and her account was falling into deficit – her initial investment was going down. Miss S went into 'panic mode'. He said she had to buy insurance (costing £20,000) to protect her investment – but

she would still make a profit. Miss S said she had no money left – but under pressure from the account manager, she took out a loan for £4,000 and sent that to PSP2 and then to the investment company. These payments made from her RBS account and which are the subject of this complaint:

Date	Payment type/beneficiary	Amount
1 June 2022	Faster payment / PSP2	£3,000
1 June 2022	Faster payment / PSP2	£1,000
23 June 2022	Credit from PSP2	(£117.15)
<b>Total</b>		<b>£3,882.85</b>

Miss S believed she would immediately get her investment money back, but she couldn't then get access to the website of B, and the WhatsApp messages to / from the account manager were blocked. She then realised she had been the victim of a scam.

She had sold her house the year before and a lot of the money had been lost. She was now finding it difficult to pay bills. She now had a high interest loan to make repayments to; and had to move in with her partner to enable her to live. Her losses were putting pressure on her relationship. She feels anxious and angry.

Miss S said her account with RBS was new and the payments weren't typical. She said RBS should've done more to protect her. She says the bank should refund the money she paid from her RBS account.

#### *What RBS said:*

Miss S contacted RBS in June 2023. RBS said they hadn't investigated the case – as Miss S needed to report it to their scams investigation department. They gave Miss S referral rights to our service – and so the complaint came to us to look at.

#### *Our investigation so far:*

Miss S brought her complaint to us and our investigator asked RBS for details as to what had happened. RBS said to us:

- Miss S hadn't raised a case with their fraud team.
- When Miss S made the online payment to a new payee she was asked what the payment was for – and was presented with a warning message. Depending on the option she chose, she would then have received a further warning about 'investing in cryptocurrency', together with a link to the Financial Conduct Authority's (FCA) website – which gave guidance on crypto scams.
- RBS matched the beneficiary successfully using the 'Confirmation of Payee' tool.
- The payments weren't flagged by RBS' systems as being unusual or suspicious.
- Miss S had authorised the payments. And she was given a one-time passcode – which she input to confirm the payments.

- RBS said Miss S hadn't done sufficient due diligence – the FCA register would've shown that A wasn't registered.
- Online research on B showed it was not authorised by the FCA and was a scam.
- She put a lot of trust in the account manager.
- There wasn't a contract for the investment.
- The point at which funds were lost was when they were sent from PSP2 to B – so Miss S should contact PSP2.

Our investigator didn't uphold Miss S' complaint. He said the payments didn't seem unusual, considering Miss S' account had just been opened. RBS hadn't tried to recover any of the funds – as they had likely left the crypto wallet and transferred to B immediately.

Miss S didn't agree and asked that an ombudsman look at her complaint.

### **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.

I'm sorry to hear that Miss S has lost money in a cruel and sophisticated scam. It's not in question that she authorised and consented to the payments in this case. So although she didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider RBS should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have 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 banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary– and in this case, the payments were made to Miss S' own account with the payment service (PSP2).

The important matter here is whether these were payments that RBS might reasonably have considered unusual, and therefore whether they should've held or stopped the payment and contacted Miss S about them.

I looked at Miss S' account history with RBS. It was a new account – the opening deposit was made on 19 April 2022. But then, there were ten payments of £1,000 (and one for £500) between then and the payments to PSP2 on 1 June 2022. So, I don't think the payments of £3,000 and £1,000 were unusual for her.

I'm also mindful that there's a balance to be struck: RBS has obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think RBS acted reasonably in processing the payments.

I also noted that RBS sent Miss S a scam warning when she set up the payments; with a link to the FCA's further information on scams.

So, I don't think I can reasonably hold RBS liable for these payments,

#### *Recovery:*

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether RBS took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

Miss S says she contacted RBS as soon as she realised she had been scammed, but RBS have said they have no record of this – until Miss S complained in June 2023. And by that time, there were never going to be any funds left – as it's usual in scams of this type that funds are removed by the scammers within hours. In addition, the account with PSP2 was in Miss S's own name, and she then moved the funds onto the investment company – so there weren't any funds to be reclaimed.

Miss S has lost a lot of money. She's explained why the money was important to her, and the impact her losses have had. I was sorry to learn of her circumstances. She will therefore be disappointed by my decision, but I'm not going to ask RBS to do anything here.  
**(continued)**

#### **My final decision**

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 6 November 2023.

Martin Lord  
**Ombudsman**