

The complaint

Miss S complains that Bank of Scotland plc trading as Halifax (Halifax) 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 several 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 another 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 him 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.

In April 2022, Miss S made payments from one of her other bank accounts to PSP2 totalling £21,928.

Miss S then made further payments from her Halifax account to PSP2 and then to B - totalling £17,290. These payments are the subject of this complaint.

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 were made from another bank account.

The payments made from Miss S’s Halifax account are the subject of this complaint::

Date	Type/ Beneficiary	Amount
24 January 2022	Faster payment/ PSP2	£190
19 April 2022	Faster payment/ PSP2	£500
19 April 2022	Faster payment/ PSP2	£4,500
26 April 2022	Faster payment/ PSP2	£10,050
28 April 2022	Faster payment/ PSP2	£2,050
Total		£17,290

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 the payments weren’t typical. She said Halifax should’ve done more to protect her. She says the bank should refund the money she paid from her Halifax account.

What Halifax said:

In July 2022, Halifax said Miss S hadn’t put the details of the scam to their fraud department and therefore couldn’t properly investigate it. They’d tried to contact both Miss S and her solicitor, but without success. If Miss S could provide more details – they would review her complaint.

Our investigation so far:

We asked Halifax for their report and information and based on that; our investigator looked at what had happened. Miss S had provided her version of events to her solicitor, who had put this to us in support of her complaint. Our investigator felt we had enough information to investigate Miss S’ complaint.

He didn’t uphold it. He said Halifax correctly held the larger payments of £4,500 and £10,050 – as these were out of character for the way in which Miss S used her account. And Halifax then contacted Miss S to discuss those payments. He was satisfied that Halifax asked the right questions – on the calls on 25 April 2022 and 26 April 2022. Halifax’s call handler:

- alerted Miss S to cryptocurrency scams.
- asked if anyone else had access to her account.
- how she found out about the platform.
- whether she'd experienced any problems.
- whether she'd been able to withdraw funds.
- whether anyone was asking her to make the payments.
- whether anyone was asking her to invest more money.

He was satisfied that Miss S's responses were such that it was reasonable that Halifax then made the two payments.

He considered that Halifax couldn't make any attempt recover the funds – as Miss S hadn't made contact with them, and it was likely that the funds had been moved from PSP2 to B in any case.

Miss S asked that an ombudsman look at her complaint, and so it has come to me to make a final 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.

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 Halifax 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 Halifax 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 Halifax. It's reasonable to say she used her account for day-to-day expenditure, with no payments for more than £500 – in the 12 months before the payments to PSP2.

Payments: £190, £500, and £2,050:

I considered these payments. And - there's a balance to be struck: Halifax 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 Halifax acted reasonably in processing the payments, as they were relatively low value.

Payments: £4,500 and £10,050:

Halifax correctly held these payments and contacted Miss S. I listened to the calls between her and Halifax's fraud team. They're important calls in the context of this complaint.

Call – 25 April 2022 (£4,500)

The relevant parts of the call are:

Halifax: *who is the payment to?* Miss S: *PSP2*

Halifax: *Have you used PSP2 before?* Miss S: *yes*

Halifax: *Any issues in the past?* Miss S: *No*

Halifax: *How did you get the account details?* Miss S: *from my account 'on there'.*

Halifax: *How did you find out about this crypto exchange?* Miss S: *my own research*

Halifax then gave a warning: *there are a lot of scams at the moment, people being contacted by WhatsApp and Facebook messenger.* Miss S said to go ahead.

Call - 26 April 2022 (£10,050):

Halifax: *does anyone else have access to the account or just you?* Miss S: *just me.*

Halifax: *have you been able to withdraw any funds since you put money in?* Miss S: *yes.*

Halifax: *did you use a broker?* Miss S: *no.*

Halifax: *Has anyone asked you to make these transfers?* Miss S: *no.*

Halifax: *has anyone said you should put more money in because you're making so much money?* Miss S: *no.*

Halifax: *are you happy to make the payment?* Miss S: *yes.*

I noted that Halifax asked the open questions they were expected to. I also noted that Miss S' answers weren't consistent with the complaint she put to us – she had been asked to invest more money by the account manager because she was apparently making a lot of money; and it was the account manager who said she should make the payments. Also – she hadn't at that stage asked to make any withdrawals.

I considered whether Miss S had been coached by the account manager to respond in the ways she did – but I reviewed the WhatsApp chats and couldn't see that she was.

So – I don't think Halifax could've reasonably done any more.

Therefore, based on the calls, I don't think I can reasonably hold Halifax 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 Halifax took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

But in this case, as Miss S hadn't contacted Halifax with details of the scam, I don't think I can reasonably have expected Halifax to attempt to recover the money. But even if Halifax had done so, it was unlikely there would 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 Halifax to do anything here.

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 7 November 2023.

Martin Lord
Ombudsman