DRN-5039612

The complaint

Mr D has complained that Bank of Scotland plc trading as ("Halifax") failed to adequately warn him against becoming the victim of an investment-related 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 D has used a professional representative to refer his complaint to this service. For the purposes of my decision, I'll refer directly to Mr D, but I'd like to reassure Mr D and his representative that I've considered everything both parties have said.

Mr D explains that in November 2023 he was recommended a cryptocurrency investment by a friend, and after being told about several people who'd made money from the investment, Mr D decided to take part. He opened an account with a cryptocurrency exchange downloaded an application for the specific type of cryptocurrency he was investing in – which he could use to track his profit and loss and make deposits and withdrawals. The way Mr D invested was by sending payments to the cryptocurrency exchange, converting the funds into cryptocurrency, and then transferring the cryptocurrency to his wallet at the supposed investment platform. Mr D has provided a step-by-step guide he was given by his friend on how to set up his accounts with the two platforms, and how to deposit and withdraw funds.

Mr D says he was told that he could double his initial investment within a month but this didn't materialise as the app he was using closed down within a matter of weeks of Mr D starting to invest. He says he didn't receive any paperwork, but word of mouth recommendations made it seem like an easy and legitimate way to earn money using this method.

The payments Mr D made as part of the scam were as follows:

<u>From his current account</u>

Date	Amount
16/11/2023	£200
20/11/2023	£502
20/11/2023	£20
21/11/2023	£371
21/11/2023	£375
22/11/2023	£515

Total	**£1,983**

From his savings account

Date	Amount
20/11/2023	£510
21/11/2023	£100.20
22/11/2023	£270
22/11/2023	£2,735
Total	**£3,615.20**

Mr D says he realised he'd been scammed when he couldn't withdraw any of his money,, and the app stopped working.

Mr D made a complaint to Halifax on the basis that it should've been monitoring his account for unusual transactions, but he says it didn't give him any warnings or intervene when he made the payments to the cryptocurrency exchange. He says the payments in question were uncharacteristic compared to other transactions on his account, which suggests they should've trigged a security check by Halifax.

Halifax didn't uphold Mr D's complaint. In its response it said that Mr D had made similar payments previously, and that the payments made as part of this scam weren't made in quick succession. It also said its detections systems didn't have reason to flag the transactions as suspicious.

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

Our investigator considered everything and didn't think the complaint should be upheld. She explained that she didn't think the payments were particularly out of character for Mr D's account, such that Halifax ought to have realised and intervened.

As Mr D didn't accept the investigator's opinion, the case has 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.

I'm sorry to disappoint Mr D but having considered everything I'm afraid I'm not upholding his 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 D authorised these payments from leaving his account. It's accepted by all parties that Mr D gave the instructions to Halifax and Halifax made the payments in line with those instructions, and in line with the terms and conditions of Mr D'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.

Halifax 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). Halifax says that as Mr D made the payments from his Halifax account via Open Banking, it didn't ask for the purpose of the payments, nor did it provide any warnings before they were sent. It also says that none of the payments Mr D made were flagged as suspicious or unusual.

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

Whilst this is relevant to all complaints Halifax considers where Open Banking is involved, having considered it in the context of Mr D's complaint, I don't think Halifax should've done more to intervene before these payments were sent.

I say this because having reviewed the values of the payments, and the pattern in which they were made, I don't think Halifax ought to have been aware they may've been part of a scam, so I don't think it missed an opportunity to intervene when it should have.

Looking at the activity on Mr D's account in the six months before these payments were made, I can see that he'd made other transactions of similar values to those involved in this scam. Whilst I acknowledge that the larger transactions in Mr D's account history with higher values – such as the ones for £1,938 and £2,515 – were made by debit card rather than bank transfer, I don't think that in itself means Halifax should've considered the bank transfers as suspicious. I also say this because Mr D regularly uses bank transfers as a method of payment, so this wouldn't have seemed out of character to Halifax.

I also note that the majority of the payments he sent to the cryptocurrency exchange were for modest amounts, and their values fluctuated, as opposed to increasing over time. This, as well as the fact that the payments were spread out over several days, rather than being sent in rapid succession, satisfies me that Halifax didn't miss the opportunity to intervene, as these features aren't typical patterns I'd usually expect to see in a scam. I've considered the fact that on three days, three payments were sent each day, but the cumulative value of those payments remained fairly low. So this doesn't change my decision here.

I do appreciate that the total value of these transactions is significant to Mr D, and I can understand why he says Halifax should've been aware of that. But I wouldn't expect a business to intervene in all payments that are slightly different to usual – as it needs to balance what's practical with the risks it identifies, as well as not unduly inconveniencing its customers. And although I don't agree with Halifax that the payments being made by Open Banking is a reason not to intervene, the other reasons I've explained satisfy me that Halifax didn't act unfairly.

In fairness to both parties I've also considered the part Mr D played – if any – in the financial harm he's now complained about. Although Mr D says he spoke to a friend about the investment, I can't see that he did much other research on the alleged opportunity he was investing in. And the fact it was recommended to him by a friend isn't a typical or particularly failsafe way to choose an investment.

I'm also mindful that the returns Mr M expected to receive – double his initial investment in a month – 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 although I understand the messages he exchanged with other investors, which he's provided copies of, convinced him, I do think he could've exercised more caution before making the payments that resulted in his losses.

Recovery of the funds

These payments were sent to Mr D's own account at the cryptocurrency exchange, and he then converted the funds into cryptocurrency which he then forwarded on to the scammer. Halifax wasn't able to recover any of what Mr D lost, as the loss didn't happen at the point the payments left Halifax, but instead when the cryptocurrency left Mr D's cryptocurrency wallet.

I'm very sorry that Mr D has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Halifax responsible for that.

My final decision

I don't uphold Mr D's complaint against Bank of Scotland plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 25 October 2024.

Sam Wade
Ombudsman