DRN-5362943

The complaint

Mr U complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund him money he lost in an investment scam.

Mr U is being represented by a professional representative, but for ease of reading I'll just refer to Mr U.

What happened

The circumstances surrounding this complaint are well-known to both parties, so I'll summarise what I consider to be the key points.

Mr U says he was contacted over a messaging platform on 28 March 2024, seemingly by accident, but he struck up a conversation with the messenger, which eventually led to discussions about investment. He says he was encouraged to invest with a company that traded currency and cryptocurrency, but the investment turned out to be a scam.

Mr U researched the investment company, had access to an online portal, read online reviews and articles and found nothing untoward.

He was able to make some withdrawals at first, withdrawing amounts on 31 March 2024, 2 April 2024 and 22 April 2024. This gave him confidence that the investment was genuine. He says he later realised he had been the victim of a scam when he was unable to withdraw any more money from his investment.

Mr U made the following payments:

Transaction	Date	Payee	Payment type	Amount
1	10/04/2024	Own cryptocurrency account	Debit card	£200
2	12/04/2024	Own cryptocurrency account	Faster payment	£2,500
3	12/04/2024	Own cryptocurrency account	Faster payment	£3,000
4	15/04/2024	Own cryptocurrency account	Faster payment	£1,000
5	16/04/2024	Own cryptocurrency account	Faster payment	£2,500
6	17/04/2024	Own cryptocurrency account	Faster payment	£2,500
7	17/04/2024	Own cryptocurrency account	Faster payment	£8,000
8	22/04/2024	Own cryptocurrency account	Faster payment	£15,000
9	22/04/2024	Own cryptocurrency account	Faster payment	£10,000
10	23/04/2024	Own cryptocurrency account	Faster payment	£11,000
11	24/04/2024	Own cryptocurrency account	Faster payment	£455.18
12	02/05/2024	Own cryptocurrency account	Faster payment	£10,000
13	03/05/2024	Own cryptocurrency account	Faster payment	£25,000
14	07/05/2024	Own cryptocurrency account	Faster payment	£15,000
15	07/05/2024	Own cryptocurrency account	Faster payment	£10,000
16	07/05/2024	Own cryptocurrency account	Faster payment	£5,000
17	08/05/2024	Own cryptocurrency account	Faster payment	£24,000
18	10/05/2024	Own cryptocurrency account	Faster payment	£12,000

Mr U says Halifax should have intervened on 12 April 2024 when he made a payment for £3,000 because the payment was out of character. He says Halifax ought to have contacted him and asked probing questions about the transaction. If it had done so, being well versed in fraud and scams, Halifax would have quickly detected the fraud and would have been able to prevent Mr U's losses. It says Mr U was vulnerable at the time and if Halifax had intervened it would have identified this and should then have offered appropriate support, such as taking extra steps to ensure he wasn't being scammed.

Halifax says the Contingent Reimbursement Model (CRM) Code doesn't apply because the payments were made to another account in Mr U's name and under his control. It says it did intervene on one of that transaction and spoke to Mr U on 11 April 2024.

Our Investigator didn't uphold Mr U's complaint. She Considered Halifax ought to have intervened on transaction 3, when Mr U made a second payment on the same day to his cryptocurrency account. It followed within minutes of the previous transaction, the amounts of Mr U's payments were increasing and amounted to £5,500. She thought Halifax ought to have asked Mr U questions to identify the payment purpose and narrow down the scam risks he was facing and then provide a better automated warning about cryptocurrency risks. However, she didn't think this would have prevented Mr U's losses. She noted that Halifax had called Mr U on 11 April 2024, but he considered he hadn't answered Halifax's questions accurately, which prevented it from uncovering the scam. She had listened to other calls between Mr U and his other banks, which were similar and was satisfied further intervention were unlikely to have uncovered the scam.

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.

There is no dispute that Mr U authorised the payments. I appreciate he didn't intend his money to go to scammers. Under the Payment Services Regulations 2017, he is liable for the loss in the first instance. But the matter doesn't end there.

In this case, the CRM code doesn't apply because the transactions were between two accounts held by Mr U. However, taking into account the law, regulatory 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 made 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.

However, having considered everything, I'm not upholding Mr U's complaint.

While Mr U says Halifax ought to have intervened in the transaction on 12 April 2024, when he tried to make a payment for £3,000 to his cryptocurrency wallet, Halifax actually intervened earlier, on 11 April 2024. Halifax blocked an attempted payment of £2,300 and sent Mr U a message asking him to call, which he did.

I have listened to a recording of that telephone call and I consider Halifax asked reasonable and probing questions to try and determine whether Mr U might be a victim of fraud. For example, it said that it had seen many scams involving cryptocurrency. It described a situation where a scammer makes contact and says they are in investment expert and can help people make money, establishes a friendship that builds up trust and then, having done so, they scam their victims. Halifax asked whether anyone was helping Mr U or giving him advice. In my view this was directly relevant to the scam Mr U was facing. He had been contacted by someone unexpectedly, who had built up a friendship, who had suggested they, or a relative of theirs was an expert in investment and had persuaded Mr U to invest. I consider this was a reasonably probing line of questioning and Halifax's warnings about this type of situation were tailored to Mr U's particular circumstances, as far as Halifax was aware of them.

Mr U indicated that he was familiar with the risks, but he was just attempting to send a few thousand pounds to a safe wallet for some years to see if the value rose.

Mr U demonstrated a reasonable awareness of fraud and scam risks during the call. He talked about people sending money to cryptocurrency wallets without truly knowing where they were sending money and not being able to get their money back. He related a story about a situation of one person he knew of, who had sent money to a fake investment platform, on the advice of someone pretending to work in investments and who was later unable to recover their money. Again, this demonstrates an awareness of the risks on the part of Mr U and I don't consider Halifax could have reasonably added much more to Mr U's understanding or awareness of the risks at that time. And I don't consider it had reasonable grounds to refuse to lift the block on Mr U's account.

I've considered whether further interventions ought to have been made by Halifax and whether they would have been successful.

I consider further intervention was warranted. The size of payments made by Mr U escalated sharply from 17 April 2024, with two payments totalling £10,500 on that day, and two more payments of £10,000 and £15,000 on 22 April 2024, all being sent to Mr U's cryptocurrency account. Further large payments were made on 23 April and 2,3,7,8 and 10 May 2024. I consider this large escalation in payment size and multiple payments on the same day in some cases, was sufficiently unusual that Halifax ought to have intervened again.

But I don't consider it likely that any further intervention on these dates would have prevented Mr U's losses.

I say this because I'm aware that Mr U's other bank spoke to him later in the series of payments, on 3 May 2024, and I've listened to a recording of that call. The call ran along similar lines to Halifax's call on 11 April 2024. Mr U was not open with his other bank when it asked similar questions about whether anyone else was advising him, whether he had been contacted about the investment over social media or messaging apps and whether he had been asked to mislead his bank. He once again sounded confident about the investment and again showed an understanding of fraud risks.

If Halifax had intervened on other occasions, I do consider it would have been harder for Mr U to suggest he was simply investing a small amount of money to see whether the value of cryptocurrency rose after a few years. Halifax would have known that Mr U had sent

substantial amounts of money to his cryptocurrency account, certainly by 22 April 2024. But there is little or nothing to indicate Mr U had any concerns or would have been more open with his answers or responsive to Halifax's warnings at any point throughout April and May 2024, especially in light of the content of the calls he had with his banks during this period.

The chat with the scammer, by messaging app, suggests Mr U was nervous about the amount of money he had invested, but doesn't suggest he had any particular doubts or concerns he was being scammed. That realisation seems to have started after the final transaction had taken place. There is little to suggest that an intervention would have been successful at any particular point before that.

While Mr U says he was vulnerable and Halifax would have discovered this if it had intervened, it did intervene and having listened to the call recording, nothing in the call suggests Mr U was vulnerable. Mr U only informed Halifax of his vulnerabilities after the final transaction. On balance, I'm not persuaded Halifax was at fault for not identifying Mr U's vulnerabilities.

Overall, while I think Halifax ought to have intervened on further occasions, the content of the calls I've listened to from his three banks, on 9 and 11 April and 3 May 2024, covering most of the period in which the scam took place, suggests to me that Mr U's answers to probing questions, whenever interventions might have been attempted, wouldn't have changed much. He's unlikely to have been open with Halifax because he wasn't in each of the three calls I've listened to. He demonstrated awareness of the scam risks, was given warnings but appears to have been confident he was investing in a genuine investment. I'm not persuaded further intervention would have prevented the fraud.

My final decision

I don't uphold Mr U's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr U to accept or reject my decision before 30 April 2025.

Greg Barham
Ombudsman