DRN-5354457

The complaint

Mrs R complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund her after she was the victim of an investment scam.

Mrs R is represented by a professional representative, but for ease of reading I'll just refer to Mrs R.

What happened

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

Mrs R says she found out about an investment through a networking event and was added to a chat group in a popular messaging app.

She says she participated in a lot of group calls, where hundreds of people attended and asked the hosts questions about the investment and the legitimacy of the investment company. Mrs R says there were various videos posted online too. She conducted research on the companies involved. She saw online testimonials, presentations, marketing information, company information and all her research suggested the investment was legitimate. This gave her the confidence to invest.

Mrs R made the following payments to several cryptocurrency platforms and received a number of credits back from her cryptocurrency accounts into her Halifax account:

Transaction	Date	Payee	Payment type	Amount
1	7 January 2021	Own cryptocurrency acc.	Transfer	£2
2	7 January 2021	Own cryptocurrency acc.	Transfer	£5
3	7 January 2021	Own cryptocurrency acc.	Transfer	£1,500
4	7 January 2021	Own cryptocurrency acc.	Transfer	£3,500
	7 January 2021		Credit	£3,500
5	7 January 2021	Own cryptocurrency acc.	Transfer	£1,500
	7 January 2021		Credit	£1,500
6	10 January 2021	Own cryptocurrency acc.	Transfer	£5
7	10 January 2021	Own cryptocurrency acc.	Transfer	£995
8	10 January 2021	Own cryptocurrency acc.	Transfer	£500
9	06 February 2021	Own cryptocurrency acc.	Transfer	£1,000
10	13 February 2021	Own cryptocurrency acc.	Transfer	£600
11	20 February 2021	Own cryptocurrency acc.	Transfer	£200
12	13 March 2021	Own cryptocurrency acc.	Transfer	£200
13	02 April 2021	Own cryptocurrency acc.	Transfer	£350
14	10 April 2021	Own cryptocurrency acc.	Transfer	£100
15	15 April 2021	Own cryptocurrency acc.	Transfer	£500
16	19 May 2021	Own cryptocurrency acc.	Transfer	£1,000
17	27 May 2021	Own cryptocurrency acc.	Transfer	£1,000
18	14 June 2021	Own cryptocurrency acc.	Debit card	£272.56

19	20 July 2021	Own cryptocurrency acc.	Transfer	£1,000
20	29 July 2021	Own cryptocurrency acc.	Transfer	£500
21	30 July 2021	Own cryptocurrency acc.	Transfer	£50
22	10 September 2021	Own cryptocurrency acc.	Transfer	£500
23	13 October 2021	Own cryptocurrency acc.	Transfer	£1,000
24	18 October 2021	Own cryptocurrency acc.	Debit card	£1,066.46
25	18 October 2021	Own cryptocurrency acc.	Transfer	£500
26	25 October 2021	Own cryptocurrency acc.	Transfer	£10,000
27	25 October 2021	Own cryptocurrency acc.	Transfer	£10,000
28	25 October 2021	Own cryptocurrency acc.	Transfer	£4,000
29	26 October 2021	Own cryptocurrency acc.	Transfer	£6,000
30	02 November 2021	Own cryptocurrency acc.	Transfer	£10,000
	02 November 2021		Credit	£633.05
	06 November 2021		Credit	£194
	14 November 2021		Credit	£43.90
31	09 December 2021	Own cryptocurrency acc.	Transfer	£1,100
32	16 December 2021	Own cryptocurrency acc.	Transfer	£1,050
	16 December 2021		Returned	£1,050
33	16 December 2021	Own cryptocurrency acc.	Transfer	£9,000
	16 December 2021		Returned	£9,000
	18 December 2021		Credit	£1,874.77
34	20 December 2021	Own cryptocurrency acc.	Transfer	£5,020
35	23 December 2021	Own cryptocurrency acc.	Transfer	£1,020
36	26 December 2021	Own cryptocurrency acc.	Transfer	£1,020
	26 December 2021		Credit	£64.54
37	28 December 2021	Own cryptocurrency acc.	Transfer	£150
	02 January 2022		Credit	£1,995.91
38	02 January 2022	Own cryptocurrency acc.	Transfer	£5,020
39	03 January 2022	Own cryptocurrency acc.	Transfer	£1,020
40	07 January 2022	Own cryptocurrency acc.	Transfer	£960
41	10 January 2022	Own cryptocurrency acc.	Transfer	£5,000
42	12 January 2022	Own cryptocurrency acc.	Transfer	£1,500
43	19 January 2022	Own cryptocurrency acc.	Transfer	£100
44	21 January 2022	Own cryptocurrency acc.	Transfer	£1,000
	03 February 2022		Credit	£2,613.41
45	04 February 2022	Own cryptocurrency acc.	Transfer	£1,050
46	07 February 2022	Own cryptocurrency acc.	Transfer	£740

47	08 February 2022	Own cryptocurrency acc.	Transfer	£1,080
48	10 February 2022	Own cryptocurrency acc.	Transfer	£970
49	13 February 2022	Own cryptocurrency acc.	Transfer	£1,210
50	14 February 2022	Own cryptocurrency acc.	Transfer	£305
51	14 February 2022	Own cryptocurrency acc.	Transfer	£310
52	16 February 2022	Own cryptocurrency acc.	Transfer	£3,650
53	23 February 2022	Own cryptocurrency acc.	Transfer	£100
54	23 February 2022	Own cryptocurrency acc.	Transfer	£2,000
55	26 February 2022	Own cryptocurrency acc.	Transfer	£450
56	20 March 2022	Own cryptocurrency acc.	Transfer	£300
57	23 March 2022	Own cryptocurrency acc.	Transfer	£100
58	29 March 2022	Own cryptocurrency acc.	Transfer	£5
59	05 April 2022	Own cryptocurrency acc.	Transfer	£2,000
60	06 April 2022	Own cryptocurrency acc.	Transfer	£1,000
61	28 April 2022	Own cryptocurrency acc.	Transfer	£1,000
62	03 May 2022	Own cryptocurrency acc.	Transfer	£2,000
63	04 May 2022	Own cryptocurrency acc.	Transfer	£1,000
64	05 May 2022	Own cryptocurrency acc.	Transfer	£1,000
65	06 May 2022	Own cryptocurrency acc.	Transfer	£8,200
	13 May 2022		Credit	£3,150.05
66	27 July 2022	Own cryptocurrency acc.	Transfer	£100
67	07 November 2022	Own cryptocurrency acc.	Transfer	£2,200

The funds were transferred from Mrs R's cryptocurrency accounts to wallets controlled by the scammers.

Mrs R says she did receive some returns from her investment, of around £10,000 in total, but there started to be issues with withdrawals from around April/May 2022. The scammers provided reassurance, but by November 2022 the platform was no longer accessible.

Mrs R realised she had been the victim of a scam when she was unable to make withdrawals from the investment.

She considers Halifax ought to have intervened to stop the transactions because the transactions were clearly unusual and out of character for her account, particularly the size of the transactions. She considers any interventions Halifax did attempt weren't sufficient, that conversations were broad and the questions it asked should have been more specific. She considers that if she had been asked more probing questions, the scam would have been revealed and her losses prevented. On 25 October 2021, she made significantly higher payments and the FCA had issued notices about this particular company earlier in 2021, but Halifax didn't intervene when it should have on 25 October 2021.

She says when Halifax did intervene on 3 November 2021, it related to an attempted payment from 1 November 2021 for £10,200 to a different company. In previous and subsequent transactions, Mrs R paid money from her Halifax account to her cryptocurrency account and then invested directly into the scam investment company. For this payment, Mrs R had attempted to make a payment to a broker and the broker was supposed to make the payment to the scam investment company. This payment was blocked, she heeded the risk warnings given to her during the call and she didn't try to use that broker again. She doesn't see how this call can be interpreted as an intervention relevant to any of the other payments. There was mention, in that call, of a further payment of £10,000 she had made on 2 November 2021. That payment wasn't challenged.

Mrs R doesn't feel the 3 November 2021 call should be taken into consideration, as it related to a payment that didn't go ahead and related to a different company, which she didn't ultimately use. She believes, if there had been stronger intervention, particularly around October 2021, she would have reconsidered the transactions.

Halifax says the Contingent Reimbursement Model (CRM) Code doesn't apply because the transactions took place between accounts which were in Mrs R's name and under her control. It said the payments weren't out of character for her account. And it said Mrs R didn't carry out sufficient research into the investment.

Our investigator noted that Halifax did intervene in the transactions, on 7 January 2021 and 3 November 2021. Mrs R was asked some relevant questions on each occasion and was given warnings about the transactions. They concluded that Mrs R was given suitable warnings and appears to have been determined to carry on with the transactions. The investigator considered that even if further interventions had taken place, it would have likely resulted in similar warnings and conversations but would have been unlikely to have prevented Mrs R's losses.

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 Mrs R authorised the payment, even though she didn't intend her money to go to scammers. Under the Payment Services Regulations 2017, she is liable for the loss in the first instance. But the matter doesn't end there.

The Contingent Reimbursement Model Code (CRM) requires firms to reimburse customers who have been the victims of Authorised Push Payment scams, like the one Mrs R says she has fallen victim to. But there are some circumstances in which the CRM code doesn't apply. Halifax says this is one of them because the code doesn't apply to transactions between accounts in the customer's own name, as was the case here. I'm satisfied that's correct in this case. 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 Mrs R's complaint.

I've considered whether Halifax could have done more to prevent the scam, having blocked one of the first few payments on 7 January 2021 and having talked to Mrs R that same day.

I've listened to the call recording of the conversation between Mrs R and Halifax. I've borne in mind that the call happened some years ago.

Halifax asked Mrs R how long she had had the account she was transferring money to and Mrs R told Halifax she had had it for a couple of years, it had been dormant, but she was starting it back up. She was asked whether anyone told her to make the payment and she said not. She was asked if she had been contacted by anyone and she said she was making of payment of her own accord and had not been told to lie to her bank.

I consider it was right for Halifax to have intervened on 7 January 2021, given the size and number of payments being made to a cryptocurrency provider on that day. I don't consider the call was particularly effective or that the questions were sufficiently probing. Since it knew the payment was being made to a cryptocurrency account, Halifax might have asked probing questions about how Mrs R had heard of the investment and whether anyone else was helping her, whether she had been able to make any withdrawals, whether she had carried out research, for example. But on balance, I don't think further and more probing questions would have prevented the fraud or uncovered it at this point. I consider it likely Mrs R would have answered that she had researched the investment (as she says she had), she hadn't yet made any investments or withdrawals, this being the first day of her investment and that she had heard about the investment through a networking event – essentially, how she answered similar questions in a subsequent call. There were no warnings about the company, for example on the FCA website, at that point.

For some months after that, the payments were for lower amounts, of £1,000 or less, and were made less frequently, between one day and over one month apart. I don't think that pattern of occasional, relatively low value payments ought to have triggered particular concerns with Halifax.

This pattern continued until 25 October 2021, when Mrs R made two payments of £10,000 and one of £4,000 on the same day. I consider those payments ought to have triggered intervention, given the significant amount of the payments, individually (for the two £10,000 payments) and cumulatively, being paid on the same day and representing a significant escalation in size from previous payments. The payments appear to have been processed without intervention from Halifax, but I consider it most likely that even if Halifax had intervened at this point that the scam wouldn't have been uncovered, as I will go on to explore.

A further payment of £10,000 took place on 2 November 2021 and an attempted payment of £10,020 on or around that same day appears to have caused Halifax to suspend Mrs R's account and ask her to contact it. She spoke to Halifax on 3 November 2021 by telephone.

From that call, it seems Mrs R had only intended to make the one payment for £10,000 on 2 November 2021, but had been having difficulties and so she attempted another transaction. Halifax asked Mrs R the purpose of the payment and she advised that it was for investment in cryptocurrency. Halifax asked how she heard about the investment and she said she knew other people who were investing and had heard through word of mouth from trusted sources, who had also invested. She said she invested through a platform she had always worked with. Halifax asked about the payee and Mrs R answered that this particular payee was a new third-party platform she was going to use as it might be quicker and she had experienced problems with making other payments. Halifax asked for more information and Mrs R said it was a platform that supported customers wanting to invest in cryptocurrency and also mentioned a "rewards programme". Halifax said cryptocurrency was a risky investment, but Mrs R replied she'd been doing it for two years and understood the risks. Halifax said there was a lot of fraud in this area and scams involving people claiming to be investment managers and conning people into moving money to them. It asked if Mrs R was

sure the investment was genuine. Mrs R responded to say she wasn't going to use this particular platform and didn't want to go ahead with the payment. But she said she knew the investment she was making was genuine and knew people involved in it.

I do consider this call is relevant. It provides evidence of Mrs R's responses to Halifax when it did intervene on a suspicious transaction, even if the payment in question didn't go ahead and was intended to be paid to a company she didn't attempt to pay again. Some of her answers were clearly not limited to the individual transaction. For example, she told Halifax she invested through a platform she always worked with and that she had been investing for two years and that she knew the investment was genuine. Overall, the call informs my view of how Mrs R might have responded had similar questions been asked on other occasions.

Halifax established that Mrs R was trying to invest in cryptocurrency, it asked how she'd heard about the investment, it warned her about people claiming to be investment managers and conning people into moving their money to them. It asked if she was sure the investment was genuine. These questions and warnings were relevant to the particular scam Mrs R was falling victim to. Having listened to the call, it seems that Mrs R was convinced she knew what she was doing, she had carried out research before investing and she believed the investment was genuine.

I also note that Mrs R appears to have received money into one of her cryptocurrency accounts and been able to withdraw it to her Halifax account on 2 November 2021. This deposit into her cryptocurrency account doesn't appear to have been funded from her Halifax account and appears to have been a return on her investment. Mrs R says she did receive returns from her investment at first and so it seems likely that this also would have given her a degree of confidence that the investment was legitimate.

I do consider other interventions should have taken place, on 25 October 2021 and 16 December 2021. But if interventions had taken place on those dates, even human interventions over the telephone, I consider the conversations are likely to have gone along similar lines to the conversation on 3 November 2021. In that conversation Mrs R comes across as having been confident in the research she had undertaken and convinced the investment was legitimate. Halifax warned that it had seen a lot of fraud in relation to cryptocurrency in general. It warned specifically about people claiming to be from investment companies and tricking people into sending them money, which was relevant to the scam Mrs R was falling victim to. Mrs R said she was aware of this issue but she appears to have been convinced the investment was legitimate. On that basis, I'm not persuaded further warnings from Halifax, reiterating the risks would have made a difference. Nor do I consider further calls asking whether she had taken steps to check the legitimacy of the investment are likely to led to Mrs R undertaking further research into the company. She maintained in the 3 November 2021 call that she knew the investment was genuine and knew people who had invested and had already undertaken research.

I understand Mrs R has been the victim of a cruel scam and has lost a lot of money. The scam was sophisticated and convincing and seems to have involved some initial returns, which made it appear more credible. But, while I don't think Halifax did all it could have done in terms of intervening when it ought to, for the reasons given, I don't think further intervention is likely to have uncovered the scam.

My final decision

I don't uphold Mrs R's complaint.

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

Greg Barham
Ombudsman