DRN-5144676

The complaint

Mr W complains that Bank of Scotland plc, trading as Halifax, won't refund the money he lost when he fell victim to an investment scam.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr W was initially represented in his complaint, but I'll refer to him as it's his complaint.

Mr W explained that due to difficult family and personal circumstances he had a lot on his mind in 2023, and he feels this potentially clouded his judgment and made him more susceptible to the scam.

There are two parts to this scam.

Part 1

Mr W used a well-known photo / video sharing social networking service and received a follow me request from person X (the scammer) which he accepted. X promoted herself as an investment guru trading in cryptocurrency and had a number of followers and testimonials from people making money from an investment.

Although Mr W had no experience in cryptocurrency he got in touch with X. X's communications and testimonials gained Mr W's trust and he started to invest.

Mr W explains how X promised him high returns and put him under pressure to set up accounts with crypto exchange companies (Companies A, B and C) and Firm R to credit a cryptocurrency wallet X controlled:

Mr W made three payments (payment 1,3 and 4 in the following table) totalling £2,139.42. However, when Halifax blocked further payments and Mr W spoke to their agents, he realised had lost his money to a scammer and agreed to block their number.

Payment Number	Date	Time	Amount	Payment method	Payee	Paid / Blocked
1	22/05/23	23:56	£300.00	Debit card	Company A	Paid
	23/05/23	10:06	£0.10	Debit card	Company B	Blocked - unknown
2	23/05/23	10:10	£255.76	Debit card	Company C	Paid
3	28/07/23	15:14	£1,583.66	Debit card	Company B	Paid
	29/08/23	14:58	£999.00	Debit card	Company B	Blocked - unknown
	29/08/23	14:58	£999.00	Debit card	Company B	Blocked - unknown
	29/08/23	15:04	£999.00	Debit card	Company B	Blocked -

						unknown
	29/08/23	15:04	£999.00	Debit card	Company B	Blocked - unknown
	29/08/23	15:17	£1,000.00	Debit card	Company A	Blocked
	29/08/23	17:36	£1,000.00	Debit card	Firm R	Blocked

Part 2

Several months later, at the start of 2024, Mr W received messages about the money he had invested with X, his profit and how he could retrieve this. He communicated with Person Y. Y made himself out to be the account manager and both apologised and criticised X (but may have been X or an accomplice of X). Mr W was told that to release the proceeds of his investment he needed to pay further money. Y explained release issues (blaming X for poor communications and delays) and pressured Mr W for more and more payments until Mr W ran out of money (in April 2024) and realised he had been scammed.

Mr W made the following additional payments, totalling £5,240.71.

Payment Number	Date	Time	Amount	Payment method	Payee	Paid / Blocked
4	11/03/24	18:08	£538.57	Debit card	Company C	Paid
5	21/03/24	19:35	£805.66	Debit card	Company C	Paid
6	22/03/24	16:47	£833.58	Debit card	Company C	Paid
7	25/03/24	21:04	£639.32	Debit card	Company C	Paid
8	26/03/24	10:43	£605.76	Debit card	Company C	Paid
9	26/03/24	21:10	£95.18	Debit card	Company C	Paid
	04/04/24	21:33	£871.18	Debit card	Company C	Blocked – insufficient funds
	04/04/24	21:34	£870.92	Debit card	Company C	Blocked – insufficient funds
10	04/04/24	21:36	£869.89	Debit card	Company C	Paid
11	05/04/24	09:16	£852.75	Debit card	Company C	Paid

As can be seen in the tables Mr W's loss to the scammer was £2,139.42 (table 1) plus £5,240.71 (table 2), totalling £7,380.13.

Mr W contacted Halifax seeking a refund and compensation. Mr W considered that:

- Halifax failed to provide due diligence, security checks and warnings to protect him.
- His account activities were out of character and they should've raised red flags.
- Halifax didn't offer sufficient guidance to prevent future scams.

Halifax didn't agree that they could've done more to stop Mr W sending further payments. So, Mr W brought his complaint to our service. But our investigator couldn't see that Halifax had done anything wrong.

As Mr W remains dissatisfied his complaint has been passed to me to look at.

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.

Having done so, my decision is to not uphold this complaint, and I'll explain why.

I'd first like to say:

- I'm very sorry that Mr W has been the victim of a cruel scam and lost a significant amount of money here.
- Although I don't underestimate the severe impact this has had on Mr W I must approach this matter objectively.
- I've carefully considered all the points Mr W and Halifax have made, and I've focused on what I think are the important points to reach a final decision.
- Whilst Halifax is a signatory of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code which requires firms to reimburse customers who have been the victim of a scam in most circumstances, I'm satisfied this code doesn't apply here. This is because the CRM Code doesn't apply to card payments.
- Regarding efforts to recover Mr W's loss. As the payments were made to the scammer card to his account with a crypto exchange and then onto the scammer, I don't think Halifax could've been expected to recover the funds. This is because the goods and service were rendered, and no funds would've remained.

Payment Services Regulations 2017 (PSR)

Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr W made the payments here, so they are considered authorised.

However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have 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.

Also, the FCA's Consumer Duty was in force at the time these payments were made. This requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams. Halifax was also required to look out for signs of vulnerability. However, I can't see that Mr W made Halifax aware of his personal issues for them to be able to check whether he needed support.

With the above in mind, I looked closely at the file and considered whether the two intervention calls that Mr W had, with Halifax fraud and scam agents, on 29 and 30 August 2023 were:

- Triggered at the right point.
- Effective.
- Adequate.

The first call appears to have been due to a system intervention after three payments to crypto exchange companies had gone through. For the following reasons, I consider this to have been a proportionate intervention:

- Although cryptocurrency transactions were new to Mr W and cryptocurrency does carry a higher risk and isn't a regulated activity, it isn't unusual for consumers to use or invest in cryptocurrency and it is common for them to use crypto exchange companies. So, I wouldn't expect a financial firm to intervene for relatively small payments where they've identified they are going to a cryptocurrency account / firm.
- Halifax process thousands of payments each day and, as mentioned above, they have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm.
- Although the attempted payment of £999, after payment 3, was a relatively low amount, Halifax would've seen that Mr W was unusually making payments to more than one crypto exchange company and his transactions in high-risk crypto currency investments were increasing.

<u>Call 1 on 29 August 2023</u>

I found the first call to be effective because:

- Halifax's agent warned Mr W:
    - About crypto currency scams.
    - That his payment was at a higher-than-normal risk of being fraudulent.
    - That once the payments had left his account the money would be gone, and they were unlikely to be able to recover it.
    - About investment scam tactics, including platforms, and how believable they were.
    - Investing in crypto was high risk and he should be prepared to lose his money.
    - If it does transpire to be a scam, they wouldn't be able to provide a refund.
- Halifax's agent asked probing questions to quickly ascertain Mr W was acting upon a third party, could only see his profits on their platform and was being asked to pay money to release his profits.
- Halifax's agent said it was highly likely to be a scam and strongly recommended he didn't go ahead.
- Mr W commented that he was glad he spoke to the agent, thanked her and decided

not to go ahead.

- Mr W realised he had lost approximately £2,000.

Call 2 on 30 August 2023

I found that the second call was also effective because:

- Halifax's agent asked several similar probing questions about the scammers' involvement, platform and discovered withdrawal issues and quickly said these were 'massive red flags' and that it 'definitely sounds like a scam'.
- Halifax's agent strongly warned Mr W of the risks, advised he didn't go ahead and urged him to speak to the debit card fraud and scam team to try and recover his lost funds.
- Mr W accepted his financial loss to a scam, spoke about his experience as 'horrible' and was critical of himself believing the scammer.
- When the agent didn't feel fully assured by Mr W's words that he wouldn't make any further payments and contemplated suspending his online account, she then pressed him for confirmation, which he gave, and said she would write a file note confirming he knew he would lose his money and wouldn't go ahead.
- Mr W clearly understood the risks and the call concluded with him saying he definitely wouldn't go ahead.

Considering Mr W's above comments, the education that had taken place together with the warnings and balance a bank has to achieve, I don't think it would've been proportionate for the agent to have suspended Mr W's account. Also, Mr W expressed an interest in crypto investment and I don't think it would've been reasonable or proportionate for Halifax to have either blocked future transactions to the crypto exchange companies that he had set up or set up automatic interventions on every future transaction.

Having looked closely at the eight payments (numbers 4 to 11) that took place approximately six months later these were all for relatively low amounts (under £1,000) and I can't see that there were any payment patterns, such as a high velocity of increasing same day payments that should've triggered a further intervention.

Furthermore, Mr W had been given information (including Halifax's fraud hub and contact details) and warnings, that were directly relevant, that he chose to ignore despite thinking it was a scam and having previously acknowledged this was the case. I appreciate Mr W wanted to get his lost money back; however, even if Halifax had intervened again, I think it more likely than not that he would've wanted and found a way to make the payments.

In conclusion, I recognise Mr W has been the victim of a cruel scam and I'm very sorry he's lost this money. I realise the outcome of this complaint will come as a great disappointment but, for the reasons I've explained, I think Halifax acted fairly and reasonably in its dealings with him, so I won't be upholding this complaint.

My final decision

For the reasons set out above, my final decision is that I'm not upholding this complaint against Bank of Scotland plc, trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 15 September 2025.

Paul Douglas
Ombudsman