

The complaint

Mr M is unhappy that Bank of Scotland plc trading as Halifax (Halifax) won't refund all the money he's lost as a result of a third-party scam.

What happened

Mr M told us he saw an advert for cryptocurrency endorsed by a celebrity on a social media platform. He says he clicked on a link which took him to a website for an organisation - I will refer to as K - where he completed his details to set up an account. Someone from K called Mr M and initially he made a card payment of €250. Between 21 August 2018 and 28 May 2019 Mr M made a further 12 transactions (summarised in the table below) totalling over £300,000 towards the scam; the majority of which went via two cryptocurrency wallets (I will refer to the providers as C and E) in his own name.

Table of transactions:

Date	Payment	Debit	Credit
13/08/2018	debit card to K	£224.81	
21/08/2018	debit card to K	£897.75	
21/08/2018	transfer foreign payment	£8,334.70	
24/08/2018	credit from K		£89.70
03/09/2018	credit from K		£134.06
27/09/2018	faster payment to C	£10,000.00	
01/11/2018	credit from K		£884.24
27/11/2018	faster payment to C	£25,000.00	
28/11/2018	faster payment to C	£25,000.00	
29/11/2018	faster payment to C	£18,000.00	
11/01/2019	in branch transfer to C	£131,000.00	
14/01/2019	faster payment to C	£12,500.00	
23/05/2019	faster payment from C		£2,895.59
23/05/2019	transfer foreign payment E	£50,000.00	
24/05/2019	credit transfer		£47,699.86
28/05/2019	transfer foreign payment E	£18,204.99	
28/05/2019	transfer foreign payment E	£18,204.99	
28/05/2019	transfer foreign payment E	£13,653.74	
20/11/2020	credit transfer		£46,353.75

Halifax didn't uphold the complaint. It explained the payments were not covered by the Contingent Reimbursement Model (CRM) Code as they were either international payments or payments made to Mr M's own cryptocurrency accounts. It said the loss occurred once the funds moved from Mr M's cryptocurrency accounts to his account with K.

It also felt the transfers were in line with transfers made in the previous 12 months and it didn't feel intervention would have made a difference.

Our investigator upheld the complaint from the first bank transfer on 21 August 2018 to the last payment towards the scam on 28 May 2019. However, he felt that Mr M should share in the responsibility for his losses from the transaction on 23 May 2019 onwards.

Halifax accepted it should have intervened for the payment on 27 November 2018 onwards and offered to refund this less any credit with a 50% reduction for Mr M's share in his losses. Mr M said he would accept the offer but wanted 100% of the transaction that happened in branch on 11 January 2019.

I issued my provisional decision on 28 June 2023. Both parties confirmed they had nothing further to add.

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.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

As neither party has provided any further evidence or arguments for consideration, I see no reason to depart from the conclusions set out in my provisional decision. For completeness, I have set this out below.

Did Halifax do enough to protect Mr M?

Mr M accepts he made the payments himself by transferring money from his Halifax account to the scammer directly through international payments or via his own cryptocurrency accounts. So, while I recognise he didn't intend for the money to ultimately go to scammers, he did authorise these payments. And so, under the Payment Service Regulations, the starting position is that he is liable for the payments.

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 think 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.

- For branch transactions, such as the one on 11 January 2019, follow the Banking Protocol where appropriate.

So I've considered whether Halifax should have identified that Mr M was potentially at risk of fraud as a result of the payments he made, or otherwise done more to protect him.

The first two payments Mr M made towards the scam were relatively small. So I wouldn't have expected Halifax to have identified these payments as unusual or out of character. But the third payment Mr M made was for £8,334.70. This was a large amount, larger than any other transactions made on the account in the previous 12 months – it was also to a new payee and an international payment. I appreciate Halifax feels this payment was only slightly higher than the payments Mr M made previously on his account but having looked at the previous transactions the next highest was £5,358.22 some seven months earlier. Whilst I wouldn't say the difference was 'slight' (more than half as much again) – this transaction in itself looks to be unusual compared to other historical transactions. So I think Halifax should have identified that Mr M was at risk of fraud as a result of the £8,334.70 payment and asked him further questions about it.

Halifax should take steps designed to protect its customers from the risk of financial harm. And, in these circumstances and due to the size of this payment, I think it would be reasonable to expect those checks to include questions about the purpose of the payment and how well the customer knew the company they were dealing with. I've not seen anything to suggest that Mr M had been told to lie about the purpose of the payments. So if Halifax had asked about it, I think Mr M would have told Halifax that the payments were for investments using cryptocurrency, that he had been contacted by the company after filling in a form from a link he'd seen on social media with a celebrity promoting the investment. And that he was mostly communicating with the company via a social media messaging platform. As this kind of contact is unusual for a genuine company and Mr M came across the company from an advert linking a celebrity to the investment, I think Halifax should then have asked further questions about the company Mr M was dealing with and how the investments were supposed to work. I think these details would have made it apparent that Mr M was likely the victim of a scam. Halifax is in a position of knowledge and authority in financial matters. So if it had warned Mr M at this point that he was likely the victim of a scam, I think this warning would've carried considerable weight with him. And I think he would have accepted he had been the victim of a scam and I don't think he would have made this or any further payments to the scam. So I think Halifax should refund this payment and those that followed to Mr M.

I've thought about the interaction in branch on the 11 January 2019. Halifax says its branch staff can't now recall the transaction and has no evidence about what was discussed at the time – although it has provided its high value checklist as to what it says would have been asked in line with its procedures. But there is no evidence this checklist was actually completed and although Mr M's testimony confirms he was asked about the purpose of the payment – his recollection of the conversation is that *that was about it*. The checklist covers a variety of different scams and there are some warnings listed – but when thinking about cryptocurrency scams specifically by this point (January 2019), as a financial services professional, I think Halifax could have done more.

Halifax would have been aware at the time that fraudsters use genuine firms offering cryptocurrency as a way of defrauding customers. Cryptocurrency scams had been increasing in frequency and both the Financial Conduct Authority (FCA) and Action Fraud had published specific warnings about these scams in 2018. In my view, by the time of the branch transaction, Halifax had had time to understand these warnings and put mechanisms in place to detect and prevent this particular type of fraud.

So, it may have appeared on face value to have been a legitimate payment to a legitimate organisation. But even though the money appeared to be going somewhere safe or on (as it did) to the consumer's own wallet, I don't think the conversation should have stopped there. Based on the industry warnings at the time, I think Halifax ought to have had a good enough understanding of how these scams work – including that consumers often move money to buy genuine cryptocurrency before moving it on again to a fraudster.

If Halifax had asked who Mr M was paying his cryptocurrency to, how he had been contacted, and whether he'd opened a trading account, I think Mr M would have told them about K. With further questioning, I think Halifax would have been on notice that Mr M was falling victim to a scam. And if Halifax had given Mr M some warnings about cryptocurrency scams including pointing out that scam firms can manipulate software to distort prices and returns and scam people into buying non-existent currency – I think this would have caused sufficient doubt in Mr M's mind not to proceed with the payments. In other words, if Halifax had carried out further or better questioning in line with the bank's duty of care, it seems probable that Mr M would have become credulous about the scam in time and stopped the £131,000 payment (and any subsequent payments) in its tracks. The fraud would have failed; and Mr M would not have lost £131,000 or the transactions that followed.

Did Mr M's actions contribute to his loss?

While I do think Halifax failed to take sufficient steps to protect Mr M, I also need to consider Mr M's own actions and whether he should bear some responsibility for the money he lost.

This was a sophisticated scam. Mr M says he visited the website directly to look before investing and he says it contained testimonials. Mr M says he checked the FCA website and questioned K why they weren't authorised. Mr M says K told him it was because cryptocurrency wasn't regulated which Mr M thought was a plausible explanation. Whilst there were warnings on the FCA website relating more generally to cryptocurrency scams – I wouldn't have expected Mr M to trawl through the website for this information. He says he checked the internet and saw positive reviews and queried any negative reviews with K. Again, Mr M appears to have received a plausible explanation from K. I can't see any reviews referring to this being a scam at the time Mr M initially invested. And although some warnings appeared whilst he continued to invest – I don't think he ought reasonably to have been continuing to check unless there was a cause for concern. From what Mr M has described it seems K gave him access to a fake trading platform, where he could monitor the apparent profits he was making. Mr M said he checked what he was seeing, and it was showing profits in real time and in line with what was happening in the genuine cryptocurrency market at the time.

I've looked through the messages Mr M has with the scammer and whilst I think the method of contact and some of the communications might be unusual – there is nothing specific within them that I think ought to have caused Mr M concern. Overall, I'm satisfied that he made some attempts to assure himself of the legitimacy of the investment opportunity, but those checks did not raise any red flags because of the scam's sophistication. Of course, with the benefit of hindsight, there is more that Mr M could've done to protect himself. But I don't think it was unreasonable for him to proceed with the payments in the circumstances.

But by May 2019 I think there were some red flags. From the documentation issued by the scammer, it appears the returns he was told he could receive were too good to be true. I also agree with Halifax that it seemed unusual to be told to invest more to keep his account manager. There were also signs that something was not quite right as between 14 and 16 May 2019 several payments made to C were returned and his account with C closed. Mr M knew there was a problem but didn't explore this further. Of course, by this point if Mr M had checked things further – there was a wealth of information that would have pointed to this being a scam. The FCA had published a warning about K and Mr M has also provided us with further warnings that would have been available from a quick internet search.

In the circumstances, I think Mr M must bear some responsibility for his loss from 23 May 2019 onwards. And I think it would be fair to reduce the refunds from this point by 50%.

Putting things right

In the circumstances, I am satisfied Halifax should fairly and reasonably reimburse Mr M for the loss he suffered (transactions made less returns received) from the £8,334.70 transaction onwards. A 50% reduction should be applied to losses from 23 May 2019. Interest should be added to compensate him for being deprived of the money he lost.

Interest

In assessing what would be fair compensation, I consider that my aim should be to put Mr M as close to the position he would probably now be in if Halifax had intervened and prevented the scam.

But for the scam, Mr M would have used his money differently. It is not possible to say *precisely* what he would have done differently. This is not straightforward in this case because, Mr M transferred money from investments (including ISAs) and Halifax says it can't re-instate them and offered a return of 8%. I could investigate this further, but I still don't think I could be certain what Mr M would have done. Neither party has objected to the interest rate applied in this case. With that in mind, I am satisfied that what I have set out below is fair, reasonable and proportionate given Mr M circumstances and objectives.

Award limits

Where I uphold a complaint, I can award fair compensation to be paid by a financial business of up to £160,000 for originating acts and omissions up to 1 April 2019 (where the complaint was referred to us between 1 April 2020 and 31 March 2022 - as it was here).¹

In addition, I can award any interest and costs that I consider appropriate.

If I think that fair compensation is more than the limits mentioned above, I may recommend that the business pays the balance.

Decision and award: I uphold the complaint in part. I think fair compensation in this case is £230,283.96 (this figure is net of returns received in the table above and less 50% for Mr M's share in the losses from 23 May 2019).

My decision is that Halifax should pay Mr M £160,000.

¹ There are different maximum award limits based on the date of the act or omission by the business, and the date the complaint is referred to us they can be found here <https://www.financial-ombudsman.org.uk/businesses/resolving-complaint/understanding-compensation>

Because Halifax can't reinstate Mr M's investments and I can't be certain what Mr M would have done but for the scam, I consider it fairest that Halifax pays simple interest at the rate of 8% simple per annum from the date of each transaction to the date of settlement.²

Recommendation: I think fair compensation is more than £160,000 so I recommend that Halifax pays Mr M the balance of £70,283.96 with simple interest on that sum at 8% per annum from the date of loss to the date of refund.

This recommendation is not part of my determination or award. Halifax doesn't have to do what I recommend. It's unlikely that Mr M can accept my decision and go to court to ask for the balance. Mr M may want to get independent legal advice before deciding whether to accept this decision.

My final decision

My final decision is I uphold the complaint in part and I require Bank of Scotland plc trading as Halifax to put things right for Mr M as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 7 August 2023.

Kathryn Milne
Ombudsman

² If Halifax is legally required to deduct tax from the interest should send Mr M a tax deduction certificate so he can claim it back from HMRC if appropriate.