

The complaint

Mr C complains about Bank of Scotland plc (trading as Halifax). He says Bank of Scotland didn't do enough to protect him from becoming the victim of a scam and wants it to refund him the money he has lost.

What happened

Mr C came across an advert on Facebook offering investment opportunities in cryptocurrency. He submitted his details and was contacted by phone by a 'broker' who persuaded him to invest. This broker turned out to be a scammer.

Mr C made a total of eight payments by debit card and faster payments, totalling £12,470 to purchase crypto from three different crypto providers ('B' 'C' and 'P'), which he then moved on to the scammer.

The scammer then asked Mr C to pay commission in order to withdraw his supposed profits.

Mr C then realised he had been scammed and made a complaint to Bank of Scotland.

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, I've decided not to uphold Mr C's complaint for materially the same reasons as our Investigator. I know that this will be disappointing for him, so I'll explain why.

Was Mr C the victim of a scam?

It is not in dispute Mr C has been the victim of a scam –he was contacted off the back of sending his details to an advert he found on Facebook and was contacted by phone by someone pretending to be a legitimate broker. He was then persuaded to purchase crypto, and when he wanted to access the supposed profits he had made, he was told he needed to pay commission to access them.

Did Mr C authorise the payments?

In line with the Payment Services Regulations 2017 (PSRs), Mr C isn't liable for payments he didn't authorise, unless he failed with gross negligence or intent to comply with the terms of the account or keep his personalised security details safe.

I'm satisfied Mr C did authorise the payments in question here. He confirmed with Bank of Scotland it was him making the payments – and he wanted them to be processed. I understand Mr C had been tricked by the scammer into instructing Bank of Scotland to make the payments – but while Mr C never intended the payments to go to the scammers, this doesn't change the fact he authorised them and is therefore presumed liable for the loss in the first instance.

Recovery of the payments Mr C made

After the payments were made, I wouldn't reasonably expect Bank of Scotland to do anything further until it had been notified there was a scam. Mr C made eight payments in total to the scammer – four by debit card and two by the faster payment system.

The only recourse for potential recovery of the funds for the payments made by debit card would be via the chargeback scheme. Chargeback is a process by which disputes are resolved between card issuers (here, Bank of Scotland) and the merchant (here, C).

However, a chargeback in these circumstances would never have been successful. This is because C provided the services that Mr C had requested of it – the purchase of crypto – and this was provided into an account in Mr C's name. So, a successful chargeback would never have been possible – and so I don't think that these payments were recoverable once they had been made.

Similarly, while Bank of Scotland could have contacted the merchants (B and P) for the payments made by faster payment, again the service of providing crypto had been completed. So, B and P had done what was asked of them here too.

While I understand Mr C then went on to move the crypto to another wallet which was in the control of the scammer, this isn't the fault of B, P or C and therefore, I don't think Bank of Scotland could have recovered any of the payments in dispute.

Should Bank of Scotland have reasonably prevented the payments in the first place?

I can only uphold this complaint if I think Bank of Scotland reasonably ought to have prevented some or all of the payments Mr C made in the first place – therefore preventing the loss before it happened.

Mr C authorised the scam payments in question here – so as I've explained above, he is presumed liable for the loss in the first instance.

That said, as a matter of good industry practice, Bank of Scotland should have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions – that could involve fraud or be the result of a scam. However, there is a balance to be struck: banks had (and have) obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't reasonably be involved in every transaction.

Taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider having been good industry practice at the time, I consider Bank of Scotland should fairly and reasonably:

- Been monitoring accounts – including payments made and received – to counter various risks including anti-money laundering, countering the financing of terrorism and preventing fraud and scams;
- Had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst 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; and
- 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.

So, I've carefully considered what this means for Mr C and the payments in question here.

The first six payments made were all £100 or less – so I wouldn't expect Bank of Scotland to have made any interventions here, or been obliged to contact Mr C.

However, I can see Bank of Scotland did intervene when Mr C attempted to make a payment of £4,550 to B. Mr C's internet banking was blocked – and he had to confirm the transaction over the phone.

I've listened to the call, and Bank of Scotland warned Mr C about investment scams – it also asked him if there was any third party involved to which Mr C answered 'no' – although this wasn't the case. Bank of Scotland also said the business 'B', Mr C was attempting to pay didn't have good reviews online – and it seemed scammers were using B as a means to defraud customers. Mr C said he would cancel the payment and make the payment through a different business – but he then went on to pay B anyway.

I do think perhaps Bank of Scotland could have asked more questions than it did, but I don't think this would have stopped Mr C from making the payments. I also don't think that asking Mr C to come into branch at this point would be proportionate to ask Mr C to visit the branch or inform the police as many customers use B and other crypto providers to make genuine crypto investments. Also, by this stage Mr C believed that he was making payments towards a genuine investment and was taken in by the scammers – and his later behaviour also gives me doubts that he would have listened to a clearer warning even if it was given. I'll explain why.

When Mr C attempted to make the next payment of £7,500 this was again blocked by Bank of Scotland. Mr C says that he explained the situation and was told that there was a risk he was being scammed – but he believed that his 'account' (with the scammer) was collapsing and that he had no choice but to make the payment, so he told Bank of Scotland it was genuine, and to authorise it. Mr C says he was very open during this call – and so Bank of Scotland should have done more to stop him – but I don't think he told it everything that had happened so far, and again, his later behaviour leads me to doubt that he wouldn't have made this payment.

Finally, when Mr C was told by the scammer that he needed to pay commission in order to access the supposed profits he had made, a further payment of £2000 was again blocked. I've listened to the call between Mr C and Bank of Scotland – and Mr C was clearly told that everything he had said had the hallmarks of a scam – and Bank of Scotland refused to make the payment or remove the block until he visited a branch.

On visiting the branch, Mr C initially told branch staff he wanted to withdraw £2000 in cash to pay his son – but this wasn't true. He had been told by the scammer to deposit the cash into another account in order to make the payment. The branch staff then called the fraud department of Bank of Scotland for advice.

While on the call, Branch staff voiced their concerns that Mr C was not being truthful. Mr C then explained what he had been told to do – and he still wanted to make the payment, even given all the information he had been told, including that this was another way in which the scammer was trying to get more money and it would almost certainly be a further loss. It wasn't until Bank of Scotland involved the police who visited Mr C at home as he didn't want to speak with them in branch, he finally accepted he had been the victim of a scam.

I don't blame Mr C for what happened here – the scammer had obviously utterly convinced Mr C of their legitimacy, and I can understand Mr C was desperate to not lose the money he

had already paid. But it seems to me that no matter what Bank of Scotland said to him, he was determined to continue with what he was doing until the most extreme measure of involving the police was taken.

I do have a great deal of sympathy for Mr C and the situation he now finds himself in. He has been the victim of a wicked and cruel scam.

However, the loss suffered is ultimately caused by the scammers themselves – not Bank of Scotland. And I can't ask Bank of Scotland to refund this loss when I think Mr C would have made the payments regardless of the warnings given.

My final decision

For the reasons set out above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 14 April 2023.

Claire Pugh
Ombudsman