DRN-4418615

The complaint

Mr A complains that Bank of Scotland plc trading as Halifax hasn't refunded him after he fell victim to a scam.

What happened

Mr A received a text message which said that there had been an attempted transaction on his account. It said to call the number given in the text message if the transaction wasn't recognised. Mr A knew he hadn't attempted the transaction and so called the number. He didn't realise at the time, but the message had been sent by fraudsters. And the call he made connected him to them.

The fraudsters claimed to be from Halifax and told Mr A his account was under threat. Fearful for the loss of his money, Mr A followed the fraudsters instructions and transferred £580.85 to an account in someone else's name and held at a different bank.

Mr A contacted Halifax once he realised he'd been scammed and asked that it refund his loss.

Halifax tried to recover Mr A's money from the bank he sent it to. But the fraudster had already moved the money on, and so nothing could be returned. Halifax went on to consider whether it should refund Mr A. In doing so, it considered the Contingent Reimbursement Model (CRM) Code, to which it is a signatory. But it said it wouldn't give a refund.

Halifax said it had done all it could to protect Mr A by giving him a written warning when he set up the scam payment. But it could see Mr A had selected 'family and friends' as the payment purpose – rather than 'move my money' – meaning the warning wasn't tailored to the type of scam Mr A fell victim to.

Halifax also said that Mr A hadn't held a reasonable basis for believing what he was told by the scammers. It noted that Mr A hadn't done anything to verify the message he'd received about the declined payment, despite it coming from an unverified mobile number. And he also hadn't checked the number he was told to call. From discussions with Mr A, it was also revealed that the scammers hadn't known any personal or account information about him. Mr A told Halifax he did have doubts at the time but proceeded to make the payment anyway.

Mr A was unhappy with Halifax's response and so brought his complaint to our service. One of our investigator's considered what had happened and found Halifax had acted fairly and reasonably in the circumstances. He could see that Halifax had attempted to recover Mr A's money in the way he'd expect. And he felt Halifax had fairly relied on exceptions to reimbursement set out in the CRM Code.

The complaint has been referred to me as Mr A didn't accept our investigator's findings.

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.

I know Mr A has been cruelly targeted by scammers and that he's an innocent victim here. I do sympathise with him. It must be difficult to accept that his money has been lost. But I'm not upholding his complaint and so won't be directing Halifax to refund him. I'll explain why.

Halifax is a signatory to the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. Broadly speaking, the Code is in place to see the victims of scams refunded. There are standards that signatory firms must adhere to. And there are also exceptions to reimbursement that a firm can rely on if it can be shown one or more fairly apply.

Halifax believes it met its own requirements – the standards for firms – and that an exception to reimbursement applies in Mr A's case. Halifax says Mr A didn't hold a reasonable basis for believing the text message he received and call with the fraudsters were legitimate.

Did Halifax do enough to protect Mr A?

A firm ought fairly and reasonably, as per the CRM Code, present a customer with an effective warning (as defined by the Code) when it identifies a scam risk. In Mr A's case it did present a warning. But I'm not going on to consider whether it meets the Code's definition of an effective warning. That's because I've found its intervention was enough here, given the payment made by Mr A didn't present as particularly risky.

It wasn't of particularly high value and was a lot less than Mr A had sent in the past. There was very little to mark the transaction out as unusual. So, even if Halifax hadn't presented a warning at all, I wouldn't make the finding that it hadn't met the requirements of the Code.

I've also noted that Halifax did present Mr A with *a* warning when he set up the new payment. But as he selected a payment purpose that differed from what he thought he was doing the information in the warning didn't really reflect the situation. And so Halifax was limited in how much relevant information could be given to try and protect Mr A.

Has Halifax fairly applied the 'reasonable basis for belief' exception to reimbursement?

I don't doubt that Mr A has acted honestly. And I'm sure, at the time, he believed he needed to act to protect his money. But I find Halifax has acted fairly in declining to refund him.

The text message Mr A received doesn't seem to have been disguised in any way. It came through from an unknown mobile number and only claimed to be from his bank. Mr A didn't check the sending number. Nor did he check the number he was told to call. Had he sought to verify either it's likely the scam would have been revealed, and I believe it's fair and reasonable to expect such checks in a scenario like this.

It's my understanding that the person Mr A spoke to didn't know anything about him or his account. And so there doesn't seem to have been the use of any detail that might have made the call more convincing.

Mr A was told to move his money to an account held at a different bank, and in someone else's name. But he doesn't seem to have questioned this, where I believe it presents as a worrying element of the scam.

Mr A has said he did have doubts at the time he was making the payment. But the action he took was to ask the scammer whether he was definitely from Halifax. It can't fairly and reasonably be said that any positive response from the scammer could provide assurance.

Mr A has said that he checked his account online before making the payment. And he's said he could see two declined transactions, which is what made him think his account was under attack.

I've looked at the electronic records for Mr A's account from the day he made the scam payment. I can't see any declined payments before the one he made to the scammer. There was a payment that Mr A attempted – but which was declined – after he made the scam payment. But there's nothing beforehand. I can't be sure what Mr A saw, but there's no evidence of the declined payments he's described that might have made the situation he

found himself in seem more genuine. Even if there were evidence of the declined payments Mr A has described, I don't believe it would change the outcome. There are too many other factors at play that I believe ought fairly and reasonably to have given Mr A significant cause for concern.

My finding is then that Halifax has fairly relied on the 'reasonable basis for belief' exception to reimbursement.

The attempted recovery of Mr A's funds

I can see Halifax contacted the bank that Mr A sent his money to in an attempt to recover it. Halifax did so quickly, right after the scam had been reported. There's nothing more Halifax could do here, and it had no control over what might or might not be returned.

Mr A's money had already been removed from the receiving account and so the receiving bank was unable to return anything.

My final decision

I don't uphold this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 19 December 2023.

Ben Murray
Ombudsman