DRN-4261971

The complaint

Mr H complains that Bank of Scotland plc (trading as Halifax) won't refund the money he lost when he tried to buy a new phone and it turned out to have been a scam.

What happened

In October 2022, Mr H saw a brand-new iPhone 13 Pro Max phone advertised for sale at a low price on a well-known social media marketplace.

He messaged the seller to find out more, and then he and the seller got in contact using a separate messaging app.

The seller sent Mr H screenshots appearing to show purchases made from a major retailer, which the seller said were orders for other customers. Mr H said he was interested and asked how to pay. The seller gave him payment details to pay by bank transfer.

The seller said Mr H could collect the phone in person. But it was slightly too far for Mr H to travel. The seller then said they would arrange next day delivery.

Mr H then sent the £500 payment for the phone by Faster Payments transfer from his Halifax current account. The seller sent Mr H a screenshot appearing to show an order being placed.

However, the seller said he'd used the incorrect payment reference. Mr H was asked to send the payment again. Mr H knew this wasn't legitimate. He says the seller insisted and threatened him if he didn't make payment.

Mr H refused, and he reported the matter as a scam to Halifax within two hours of the payment being made. But unfortunately, the scammer had already moved the money on from the bank account Mr H had paid. So, there was nothing left to be recovered.

Halifax is a signatory of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) which can offer additional protection from Authorised Push Payment scams (APP scams) such as this one. But Halifax didn't refund Mr H's loss under the CRM Code. It said he'd not done enough to check who he was paying, or to check the seller had the item they were offering for sale.

Halifax also said Mr H had awareness of the risks of the transaction he was making. He'd fallen victim to a similar goods purchase scam on social media about 12 months earlier and Halifax had given him relevant scam information, including how to protect himself in future.

Mr H complained to Halifax. He said he'd been unable to protect himself from this scam because English wasn't his first language, and he wasn't digitally literate. He said he desperately needed the money back.

Our Investigator looked into what had happened, but didn't think Halifax needed to refund Mr H. He noted that the price was well below what would be expected for this item. He

thought the deal being offered was simply too good to be true. Mr H had asked sensible questions about the seller, asking for the seller's website, and asking why the seller's name didn't match the bank account name or the name of the social media profile (all were different). But he'd only asked this after having sent the payment.

Mr H didn't accept the Investigator's view, so I have been asked to make a final decision on his complaint.

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'm sorry to disappoint Mr H and I know how much this complaint means to him, but I've decided I can't fairly require Halifax to pay him what he lost.

Mr H was the victim of a scam, and I am sorry to hear about the situation he now finds himself in. However, even though this was a scam, that doesn't mean Halifax must refund what was lost. The cause of the loss was really the scammer who tricked Mr H.

As a starting point, because Mr H authorised the relevant payment, he is presumed liable for it.

However, the CRM Code can provide additional protection from APP scams. I'm satisfied this payment was the result of an APP scam and is one that falls within the scope of the CRM Code.

Even though it gives additional protection, the CRM Code won't always require a bank to refund its customer. Halifax points out that the CRM Code allows a bank not to refund a customer in some situations and says one of those situations applies here. Halifax says that Mr H didn't have a reasonable basis for believing that he was paying a genuine seller for genuine goods, or that he was paying who he expected to pay.

So I've first thought about whether Halifax can fairly rely on this when it says it won't refund Mr H.

Mr H explains he'd used social media to buy items before. One of those times was unfortunately a similar scam, and that time Halifax refunded him in full. Having had that experience, Mr H would likely have gained some knowledge of the risks of paying by bank transfer for something advertised on social media.

This later scam had some features that made it seem more genuine. The seller showed a photo of the phone with its box and a receipt. They also provided screenshots appearing to show other customer's orders being placed.

But there were factors I think should have caused Mr H to have significant doubts about what was happening.

The price advertised was far lower than the usual selling price for this model of phone, and for one that was essentially brand new. Mr H says he'd only been looking for a refurbished phone, which would normally be cheaper than a new phone. The price of this one was nearly half the typical new price at the time and was sold including next day delivery. I think the deal he was being offered was too good to be true.

The seller told Mr H he had a business discount code but that isn't a plausible explanation as to how (or why) the phones were supposedly being sold at such a low price compared to the normal price.

The screenshots provided by the seller aren't good evidence that the orders were actually made or successfully received by the supposed customers. And there was nothing to show the seller actually had the item for sale rather than just having access to a photo of it. I don't think the advert or screenshots should have given Mr H reassurance that what he was being promised was true – especially given how exceptionally cheap the price being quoted was.

Mr H later questioned the seller about the mismatch between the name of the seller, the name on the social media profile, and the name on the bank account he was being asked to pay. He was right to have these concerns, these were all further signs that something probably wasn't right. Asking these questions helped him to uncover the scam.

Unfortunately, he says he didn't ask the seller about this until shortly after he'd made his payment. Taking everything into account, I think Mr H did know what steps to take to protect himself from this scam (such as asking these questions). Had he asked questions such as these before sending the payment I think he'd probably have realised sooner what was happening and so would have not gone ahead. But with all of this in mind, I don't think I can fairly and reasonably find Mr H would have been unable to protect himself from this scam.

In short then, at the point he made the payment I don't think Mr H had seen enough to have reasonable confidence that the seller would provide the phone as promised – or that the seller was legitimate or genuine. That means I find Mr H made these payments without a reasonable basis for believing the seller was legitimate or knowing who he was paying - so Halifax is entitled to rely on that reason not to refund him.

Mr H has explained that he thinks Halifax should have blocked the payment from being made, at least until it could have spoken to him about it. I think it is fair to expect a bank to intervene when a payment is requested which is significantly out of character or unusual. But here the payment wasn't for a remarkable amount compared to many of Mr H's usual transactions. He often makes payments for similar or larger sums. I don't think there was enough here that Halifax should have been concerned that the payment might be linked to fraud or a scam. So, I don't think it was at fault for not blocking the payment, or otherwise intervening to warn Mr H.

While Mr H reported the scam very quickly, the scammer had already removed his money from the account he'd sent it to. So, it wasn't possible for any of the funds to be recovered. Unfortunately, scammers often move money on very rapidly before it can be reclaimed – and this is what happened here.

Overall, I'm sorry to hear of what's happened to Mr H. I can understand why he wants to do all that he can to try and recover the money he lost through this scam. He sent the payment in good faith and did not receive anything in return for it. He's explained how in his circumstances money is already tight, and he's been left in a difficult financial position.

But I can't fairly hold Halifax responsible for the actions of a scammer. I can only look at the bank's position on Mr H's fraud claim and its assessment under the CRM Code. I'm satisfied the bank processed Mr H's payment correctly in line with his instructions. It then tried to recover his money once it knew what had happened. Halifax has established it can choose not to refund Mr H under the CRM Code and I can't fairly ask Halifax to do more than it has done. So, Halifax isn't required to refund Mr H for what he lost to the scammer – either under the CRM Code or for any other reason.

My final decision

For the reasons given above, my final decision is that I don't uphold Mr H's complaint about Bank of Scotland plc (trading as Halifax).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 28 September 2023.

Stephen Dickie
Ombudsman