

The complaint

Mr R complains that Bank of Scotland plc trading as Halifax ('Halifax') hasn't written off a loan he took out during a scam.

What happened

Mr R says that on 17 March 2022 he received a call from someone who said they were from Halifax's fraud department. Although he didn't know this at the time, the caller was a fraudster. He was asked to search the number he had been called from and found that it was a Halifax number. The caller told Mr R that they could see that his card was being used in branch to withdraw cash and that the person doing this had then joined the back of the queue and was trying to take out a loan in his name. In order to catch the criminal involved, Mr R was told he needed to apply for a loan himself.

Mr R went through the loan application with the fraudster and on his advice recorded that the loan was for home improvements. He was then told to transfer the majority of the funds (£24,468.39) to an account that was computer generated and that they would be returned to him within two hours.

Mr R tried to make a payment of £24,468.39 and chose the HMRC payment reason. The payment was flagged by Halifax's security systems and he was asked to call Halifax. Mr R had three calls with Halifax's fraud department about the payment. In each call Mr R was told to lie about the payment purpose and say that the payment was for a loft conversion. I have set out below what was discussed in each call.

Call 1 – 14:04 on 17/03/22

Mr R explained that he'd tried to make a payment and been asked to call. The agent discussed the amount of the payment and the reason for it. Mr R explained that he was paying the final amount for a loft conversion that he was happy with. The agent raised concerns because the payee name and account details didn't match and asked Mr R for the name of the business that completed the work, but Mr R didn't have it.

The advisor said that he didn't think there was a problem in terms of scams as the work had been completed but he wasn't comfortable to release the payment until Mr R had double-checked he had the correct details given the amount involved.

Call 2 – 14:22 on 17/03/22

The advisor asked questions about the amount, the payee and the reason for the payment. Mr R was then advised that Halifax felt his payment carried a higher than normal risk that he was the victim of fraud or a scam and that once the payment left his account Halifax would be unlikely to recover it.

The advisor went on to say,

"We want to make sure with you today that no-one contacted you and you're not following anyone's instructions because fraudsters and scammers have been contacting our customers and maybe claiming to be [financial advisors and investments]. Also they can claim to be the fraud team or they will tell you there is a fraud happening inside the bank and they have a private investigation team that is trying to track this fraud down and they will ask you to make some payments with promises that you'll get the money back."

Mr R confirmed he hadn't had any calls and that he wanted to make the payment because the work had been done. But the advisor asked Mr R further questions in relation to whether the individual he was paying had a company, how he knew the builder and whether he had an invoice. The advisor clearly had concerns about the fact major works had been completed but Mr R didn't have an invoice. Mr R then said he had a bill and was asked for the name on it. He gave the name of an individual and was told that it was the name of a professional footballer not a builder. The advisor expressed concern about the payment and went on to explain Halifax's duty to protect Mr R. He noted that Mr R stated the work had been completed but that some customers will say that when it's not the case. The advisor discussed the loan Mr R had taken out and established that no-one talked to Mr R about taking out a loan or suggested that he do so. He also asked Mr R to confirm he hadn't paid a deposit. Ultimately, the advisor said he'd made notes and Mr R should call back with further information.

Call 3 – 14:47 on 17/03/22

During this call the advisor went over many of the issues discussed in the previous call. Mr R explained that he was paying the builder's personal account and confirmed that he hadn't established why the details didn't match or the name of the company that completed the work. Mr R explained that the builder told him he'd had the same problem before. The advisor satisfied herself that Mr R was aware of the loan.

The advisor discussed with Mr R the prevalence of scams and said she wasn't providing advice for the payment Mr R was making but for future payments and said it was advice given in every call at the time. She went on to say,

"There is one [scam] in particular that we're seeing quite a lot at the moment so we call it the safe account scam. So customers have been getting calls saying they're from the bank or the fraud team and they're being told that someone's tried to either access their account or move money from their account and that it's no longer safe, erm, so they're being told they need to move their money to a safe account and of course these calls aren't genuine and so if the customer moves their money then it's gone and that's when we have to try and get it back for them. So it's just to let you know that the bank would never phone you and ask you to move any money or tell you that your account's unsafe at all. So if you do receive anything similar then please just ignore it, it's not us."

Before making the payment for Mr R the advisor checked that Mr R hadn't received any unusual contact recently, that no-one had asked him to move his money or said his account was unsafe, whether he'd been asked to download software or to lie to the bank. Mr R said none of these scenarios had occurred.

Mr R says he spoke to the scammer between calls and was told the police wouldn't get involved if the payment wasn't made. When Mr R was later told to delete the Halifax app, he became concerned and called Halifax and the scam was uncovered.

Mr R says that he was tricked into taking out the loan and will struggle to make repayments so Halifax should write it off.

Halifax has referred to the three calls with Mr R before the payment was made and says it did everything it could to prevent the scam. It contacted the bank that received the funds Mr R sent within two hours of the scam being reported but was only able to recover £3.46 which has been returned to Mr R.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in part. She said this because she felt Mr R didn't do enough to satisfy himself he was contacted by his genuine bank. But as Halifax didn't provide Mr R with an effective warning it should share responsibility for his loss. The investigator also said that Halifax didn't go far enough when it spoke to Mr R before he made the payment. As a result, she recommended that Halifax

restructure the loan, remove 50% of the capital and take into account any payments Mr R has already made.

Halifax responded and said that whilst it didn't agree with all the points raised it was prepared to accept the investigator's recommendations in an effort to resolve the complaint. But Halifax said it was unable to reconstruct the loan and so the loan repayments would need to stay the same.

Mr R accepted that he should take some liability. But he referred to the huge impact of the scam on his mental health and finances as he is in arrears on the loan taken out in the scam. Mr R asked for a final decision, so his complaint has been passed to me to consider.

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 in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Mr R has raised some points about the service he has received after Halifax made its decision not to reimburse him and in respect of loan repayments. These points didn't form part of Mr R's initial complaint to this service, so I won't consider them in this decision. Mr R may choose to raise a separate complaint about these issues.

The starting point for my considerations is that, under the Payment Services Regulations 2017 and the terms of his account, Mr R is liable for transactions he's carried out himself. But Halifax are signatories to the CRM Code and also have a longstanding obligation to be on the lookout for unusual and out of character transactions which might indicate their customer is at risk of financial harm from fraud.

There's no dispute here that Mr R was tricked into taking out a loan and making the payment. But this isn't enough, in and of itself, for Mr R to receive a refund under the CRM Code. The Code places a level of care on Mr R too.

Halifax is a signatory of the CRM Code which requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances and it is for Halifax to establish that Mr R failed to meet his requisite level of care under one of the listed exceptions set out in the CRM Code.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning
- The customer made payments without having a reasonable basis for believing that: the payee was the person the Customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

There are other exceptions that do not apply to this case.

Did Mr R have a reasonable basis for belief when he made the payment?

Taking into account all of the circumstances of this case, I think the concerns Halifax has raised about the legitimacy of the transaction Mr R made, are enough to support its position that he failed to meet his requisite level of care under the CRM Code for the payment he made. I don't think Mr R had a reasonable basis for believing the person he transacted with was legitimate. I'll explain why.

I understand the call Mr R received was made from a 'spoofed' telephone number and I don't underestimate the impact this must have had in reassuring him that this was a genuine call from Halifax. But I still need to consider whether, after this initial reassurance, Mr R ought reasonably to have had doubts and conducted some checks before proceeding.

Mr R was initially told by the scammer that someone had made cash withdrawals from his account and then that they were applying for a loan. He said that he didn't see any pending transactions. In the circumstances, I consider that Mr R should have been concerned about what he was being told by the scammer.

I'm also not persuaded the premise of the scam was very plausible and so I think Mr R should have completed some checks. I can't see how Mr R taking out a loan and transferring the loan funds to what he thought was a computer-generated account would help a fraud department to catch a criminal. When he completed the loan application Mr R was told he was doing this to verify the fraudster's application. But the scammer gave Mr R the details to input so I find it hard to understand how the verification process worked too.

I've also thought about the fact that the genuine fraud department of Halifax blocked Mr R's account and didn't allow him to make the payment. Mr R then had three telephone conversations with the genuine fraud department of Halifax before the payment was released. I find it hard to understand why, if Mr R thought the original call was from Halifax's fraud department, there was a need for three further calls with the same department before the payment was released. And Mr R was told to lie to the advisors he spoke to from the Halifax fraud department. I think this ought reasonably to have caused Mr R to be very concerned and to have taken additional steps to satisfy himself the scammer was who he said he was.

During his calls with Halifax's genuine fraud department Mr R was told of numerous concerns about the payment. For example, he was told that the name and account details of the account he was paying didn't match and that the account was in the name of a professional football player. Given these points I don't consider Mr R acted reasonably in placing his faith in the caller and following their instructions without question.

Halifax also provided Mr R with a number of warnings that should have resonated with him and led him to take steps to verify what he was being told. In the second call Mr R was told that the payment carried a higher than normal risk of fraud. Bearing in mind this information I consider Mr R's suspicions should have been raised. In the third call, and before the payment was made, Mr R was given information for the future that directly applied to his circumstances. He was told that Halifax were seeing a lot of scams where customers were told someone had tried to access their account or move funds. The advisor went on to say that the calls weren't genuine, and that Halifax would never phone and ask a customer to move money or say an account wasn't safe. In light of this advice, I consider Mr R didn't have a reasonable basis for believing the caller was a genuine Halifax employee or that the reason for the payment was genuine.

Overall, while I don't dispute the power a spoofed number would have had on Mr R's decision making, I think the red flags that followed this were enough that Mr R ought reasonably to have made further enquiries before making the payment. I fully accept that Mr R was the innocent victim of a crime but that doesn't mean Halifax is responsible for returning him to the position he was in before the crime.

I've also thought about Halifax's obligations under the CRM Code, what I consider to be good industry practice, as well as what's fair and reasonable in the circumstances of this complaint. The CRM Code requires Halifax to provide an 'Effective Warning' (that is a warning that meets certain criteria set out in the CRM Code). More generally, Halifax had an obligation to be on the lookout for unusual and out of character transactions in order (among other reasons) to try and protect its customer from financial harm from fraud.

In this case, Halifax's fraud prevention systems flagged the payment Mr R sought to make and so he was asked to contact Halifax to discuss it. There's no dispute that Mr R misled Halifax about the purpose of the payment. I recognise that Mr R did so because he'd been told to do so by the scammer and that he believed he was acting on the instructions of his bank. Undoubtedly this made it much more difficult for Halifax to provide an 'Effective Warning' – as required under the CRM Code. But even though Mr R told Halifax the payment was for home improvements Halifax did provide warnings in respect of safe account scams. The warning provided in the second call explained what safe account scams can look like and the fact that once the payment had been made it was unlikely the funds could be recovered. But the warning didn't go far enough and say that the bank will never ask a customer to help with a fraud investigation or to move money and that if a customer is asked to do so it's a scam. The impact of the warning in the third call is lost because the advisor says it relates to future payments rather than the one Mr R was making.

In considering this case, I haven't just considered the provisions of the CRM Code though. Overall, I don't consider it was fair and reasonable of Halifax to have accepted Mr R's responses to the questions asked at face value and to allow the payment to be processed. I'm satisfied that there ought to have been sufficient concern to override any reasonable reassurance Halifax could have taken from Mr R's responses to the questions it asked in all the calls it had with him.

Halifax knew that the name and account details of the payee didn't match and that the account appeared to be in the name of a professional footballer. Mr R explained this by saying that he was paying a personal account. I don't consider Halifax should have been satisfied with this explanation and I note that in the third call the Halifax advisor asked Mr R if he'd established why the details didn't match and he said he hadn't. If work costing nearly £25,000 had been completed by a company, Mr R should have paid that company and not an individual, and particularly not an individual whose name didn't match the account details.

Halifax will be aware that scam victims are often given cover stories to hide the real reason for a payment request. In this case a lot of red flags were raised but the Halifax advisors didn't go far enough and often asked closed questions. Two of the Halifax advisors established that Mr R didn't pay any form of deposit and was paying the entire bill on completion, which is unusual, but didn't go any further. And Mr R wasn't asked to provide a breakdown of the total cost of the work.

Halifax also knew that when Mr R initially tried to make the payment himself, he said he was paying HMRC but that when asked in calls he said he was paying for a loft conversion.

I think that had Halifax probed further about the work that was being done and the breakdown of the invoice, it would have been clear that Mr R was falling victim to a scam and the true circumstances surrounding the payments may have been revealed. Even if they were not, I think there ought to have been sufficient concern here for Halifax to refuse to make the payment until it was satisfied of the circumstances. Halifax could, for example, have asked Mr R to provide a copy of the invoice. In either case, I think it's more likely than not that Mr R's loss could have been prevented. But, as I've already concluded that Mr R didn't have a reasonable basis for belief in making the payments, it's clear he had a role to play in what happened. In the circumstances, I think there should be a 50% deduction from the amount Halifax pays him.

Overall

Whilst I sympathise with Mr R as he's clearly been the victim of a cruel scam, I consider that he should share responsibility for his loss with Halifax. Halifax has said that it can't reconstruct or cancel the loan but can apply a credit of 50% of the remaining capital balance. Mr R would then be responsible for arranging a payment plan to pay the remaining 50% of the loan balance. No interest is being applied to the account now, but interest already

charged should be refunded and Mr R should receive 50% of the payment he made towards the loan in April 2022.

My final decision

My final decision is that Bank of Scotland plc trading as Halifax should:

- Apply a credit of 50% of the remaining loan capital balance;
- Refund 50% of the payment Mr R made towards the loan;
- Refund all interest charged on the loan account (if any);
- Amend Mr R's credit file to reflect the above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 20 December 2022.

Jay Hadfield
Ombudsman