DRN-4450218

## The complaint

Mr L complains that Bank of Scotland plc trading as Halifax ("Halifax") won't refund the money he lost, after he fell victim to a cryptocurrency investment scam.

## What happened

The background to this complaint is well-known to both parties, so I won't repeat it in detail here. But, in summary, I understand it to be as follows.

In or around April 2023, Mr L was looking for different investment opportunities and came across one that interested him. He expressed an interest and was told that the opportunity offered a faster method of investment with guaranteed high returns. Believing everything to be genuine Mr L decided to invest. But unknown to him at the time, he was dealing with fraudsters.

Between 26 April 2023 and 22 May 2023, Mr L made a number of payments totalling £14,037 from his Halifax account. The payments were made by Open Banking to an account Mr L held with a cryptocurrency company and from there Mr L sent the money onto accounts that were controlled by the fraudsters.

On realising he'd fallen victim to a scam Mr L raised the matter with Halifax, but it didn't uphold his complaint. In summary, it said there were various stages where Mr L could've protected himself. It also considered the payments Mr L made were within his normal spending pattern, so didn't think it had any reason to be concerned.

Unhappy with Halifax's response, Mr L referred his complaint to this service. One of our Investigator's looked into things and concluded there was no basis on which he could fairly and reasonably ask Halifax to refund Mr L the money he had lost. In summary he didn't consider the payments Mr L made would have appeared as particularly unusual or suspicious in appearance to Halifax, when considering his normal account and payment activity. So he didn't think Halifax should have realised Mr L was at risk of financial harm and being scammed.

Our Investigator also thought about whether Mr L was vulnerable to this scam, but he didn't think there was any indication that Halifax had been made aware of any vulnerabilities.

Through his representatives, Mr L didn't agree with our Investigator's view. In summary, he maintained that the transactions were highly unusual and that he hadn't previously transacted to a cryptocurrency exchange. Mr L also shared details of his personal circumstances at the time, which he says enabled the fraudsters to perpetrate the scam.

As agreement hasn't been reached, the complaint has been passed to me for a final decision.

## 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.

Having done so, I have reached the same conclusions as those of the Investigator. I'm extremely sorry to hear about what happened to Mr L. I can understand entirely why he feels so strongly that his money should be returned to him. It's important to clearly acknowledge that Mr L has been the victim of a crime here. Mr L has shared with us details of his circumstances at the time of the scam and has explained about the impact this has had on him. I can understand how losing this money has impacted him and I'm sorry to hear of the difficult time he's been going through.

But I can only compel Halifax to refund Mr L if it is responsible for the loss incurred. Having carefully considered the circumstances of this complaint, I can see no basis on which I can fairly say that Halifax should be held liable for some or all of Mr L's loss. I will explain why.

The starting position at law is that banks and building societies are expected to process payments and withdrawals that their customers authorise them to make. Mr L made the payments himself. He initiated the payments to the cryptocurrency company he held an account with and agreed that faster payments should be made from his Halifax account via Open Banking. This means that it was an authorised payment, even though Mr L did not intend for this money to go to fraudsters.

But, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider 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 (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks and building societies 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.

This means that Halifax should be on the lookout for unusual and out of character situations which can indicate that a transaction could involve fraud or be the result of a scam. So I've also considered whether Halifax should have identified that Mr L was potentially at risk of falling victim to fraud as a result of the payments, or otherwise done more to protect him.

Halifax did not identify the payments Mr L made as being out of character or suspicious at the time. When considering what payments should be considered significantly out of character, it's often a finely balanced matter – and firms have a difficult balance to strike between identifying transactions where there are indications of higher fraud risks, and

allowing customers to utilise their accounts as they want to with minimal unnecessary disruptions.

On balance, I can't fairly say that the transactions in this case were so unusual or suspicious, that they ought to have alerted Halifax that Mr L was at risk of financial harm. I say this as, having looked through the activity on Mr L's account, for the twelve months leading up to the scam, I can see there are numerous other transactions for similar/or higher amounts and it isn't uncommon for Mr L to make multiple payments on the same or consecutive days. I'm also mindful, in the circumstances of this case, Mr L had previously sent payments to this cryptocurrency platform. So, by the time he came to make these payments, the platform was already established on his account as an existing payee, which was also a legitimate cryptocurrency exchange platform.

So having considered the payments Mr L made, I'm not persuaded there was anything so unusual or untypical about them, that they ought fairly and reasonably to have given Halifax cause for concern that Mr L may have been at risk of financial harm. With the benefit of hindsight, we now know that the payments Mr L made were going to be lost to fraud. But when Mr L sent the money, this wouldn't have been obvious to Halifax.

I don't consider it reasonable to have expected Halifax to ask questions about payments that aren't unusual or out of character. This means that I do not need to go on to consider whether anything Halifax could reasonably have been expected to do would have stopped Mr L from making the payments.

I've also thought about whether Halifax ought to have refunded the loss for any other reason, and in particular, whether Halifax ought to have reimbursed Mr L under the provisions of the Lending Standards Board's voluntary Contingent Reimbursement Model Code, which Halifax has signed up to and was in force at the time Mr L sent the money. But the CRM Code is quite explicit that it doesn't apply to all push payments. The CRM Code only covers scam payments when the funds are being transferred to another person and not to a consumer's own account. In this case, Mr L sent the money to his own account held with a cryptocurrency exchange. This means I don't think Halifax is responsible for reimbursing him because of any obligation under the CRM Code.

Mr L has been brave enough to tell us something of his background. Which I imagine was hard to do, I thank him for this and can understand why he believes this would make him more susceptible to becoming a victim of this type of scam. I don't mean to in any way diminish the difficult personal circumstances Mr L has been faced with, but I can't see that the bank would have been aware of any vulnerabilities he had prior to the scam, so there was no reason for it to think he might be at higher risk of financial harm from fraud.

I've also considered what attempts Halifax made to recover the funds from the fraudsters. Unfortunately, as the payments went to a cryptocurrency account in Mr L's name before being sent on to accounts the fraudsters controlled, Halifax would not have had the option to recover the payments.

I have a great deal of sympathy with Mr L being the victim of what was clearly a cruel scam that has had a significant impact on him. But it would only be fair for me to direct Halifax to refund his loss if I thought it was responsible for the failure that caused it. And for the reasons I've explained, I'm not persuaded that it would've been able to prevent Mr L's loss.

**My final decision**

My final decision is that 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 L to accept or reject my decision before 28 December 2023.

Stephen Wise
**Ombudsman**