DRN-4923337

Complaint

Mr A complained that Bank of Scotland (trading as Halifax) failed to prevent him from falling victim to an investment scam. He also complained about the way the bank handled things after he reported the scam.

Background

In early 2024, Mr A was contacted on a social media platform by someone who offered him an investment opportunity. She told him that the returns on offer were generous - a £1,000 investment would lead to a return of £10,000. Unfortunately, this person wasn't offering him a legitimate investment opportunity. They were a fraudster. She persuaded Mr A to invest a total of £7,209.40. He made those payments using his debit card connected to his account with Halifax. Those payments were made to a third-party cryptocurrency exchange. The money deposited was then converted into cryptocurrency and transferred into the control of the fraudster.

Once he realised he'd fallen victim to a scam, he notified the bank. It told him it couldn't help him and directed him to contact Action Fraud. He asked the bank to cancel the payments that were still showing as “pending” on his online banking. It said it couldn’t do so. Mr A then transferred funds into another Halifax account in his name. It seems he did this in the belief that, as the payments to the cryptocurrency exchange were still pending, emptying all the funds out of his account would cause those transactions to be declined. He says this was what he was told to do by employees of the bank. However, because those payments had been authorised, the merchant was able to collect them the following business day. This meant that Mr A's account went into an unarranged overdraft.

Mr A complained that the bank hadn't refunded his transactions. It didn't agree to uphold his complaint. He wasn't happy with that and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. Mr A disagreed with the Investigator's opinion. In addition to the arguments he had already made, his representatives argued on his behalf that:

- These payments ought to have been significant cause for concern for the bank. Mr A transferred a large amount of money in a short period of time to a cryptocurrency firm with all of the associated fraud risk.

- Mr A had significant vulnerabilities that affected his judgement in this case, including taking several forms of medication that are known to have cognitive impairment as a side effect.

Because Mr A disagreed with the Investigator's view, the complaint has been passed to me to consider and come to a final decision.

Findings

I’ve considered all the available evidence and arguments to decide what’s fair and

reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account. Mr A did authorise the payments in question and so he is presumed liable for them at first instance. Furthermore, these payments aren't covered by the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. That Code only applies to payments that meet its definition of an authorised push payment (APP) scam and that requires that Mr A have transferred funds *"to another person."* Mr A was paying his own account with the third-party firm and so he doesn't benefit from any protection the CRM Code might otherwise offer him.

However, that isn't the end of the story. Good industry practice required that Halifax be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to protect the customer. That might be as simple as providing a written warning as part of the payment process or it might extend to making contact with the customer to establish the circumstances surrounding the payment.

We now know with the benefit of hindsight that Mr A was falling victim to a scam. The question I must consider is whether that ought to have been apparent to the bank at the time. I've looked at his transaction history and I'm not persuaded that these payments would've appeared particularly out of character to Halifax. He'd used this account for some time and had made payments of similar values in the past. I accept that he transferred a significant sum in a relatively short period of time – but the individual payments weren't made in quick succession, and they were being made to an account he'd paid before, dating back to 10 January 2024. The account had sufficient funds at the time of the transactions, and only went overdrawn after Mr A transferred funds out on 6 February 2024. Overall, I don't think it was unreasonable for Halifax to have processed these payments without intervening.

Mr A's representatives have given me a great deal of information regarding Mr A's vulnerabilities. There's a strong possibility that his medical history and the medication he was taking affected his judgement here and led to him falling victim to this scam. However, the evidence I've seen shows that Halifax only became aware of those vulnerabilities after the scam took place. I don't think I can fairly conclude that it ought to have taken those vulnerabilities into account when deciding whether it needed to do more to protect him from financial harm in the circumstances of this case.

Mr A has also raised concerns about the advice he was given by the bank. He says that an employee of the bank told him that his money wouldn't be taken from the account. However, I've listened to the telephone conversations he had with several Halifax employees and they were clear that the bank had declined his fraud claim, the transactions that appeared to be pending could still be collected by the merchant and the bank didn't have the option of cancelling them.

On a subsequent call, Mr A asked if he could withdraw his funds. He was advised that he could either withdraw the money by cheque or open a new account and transfer the funds to it. Although the adviser did not reiterate that the scam payments might still be collected, I think this information had already been communicated to him. The idea that the payments might be more likely to be declined if the account was empty seems to have been something Mr A conceived of himself. Given the obvious urgency of the situation, I can understand why he might have been willing to try something like that – but I've not seen any evidence to suggest that the bank recommended he do so. The Investigator said Halifax should pay Mr A

£50 in recognition of the way these calls were handled. It has agreed to do so, and Mr A is free to accept that offer.

Mr A also questioned why the bank allowed his account to go so far beyond its arranged overdraft limit. However, I've reviewed the account statements, and I can see that the debit card payments were authorised while Mr A had sufficient funds in his account. He then transferred a large sum out before the merchant collected the earlier card payments, which resulted in the account becoming overdrawn.

Finally, I have considered whether Halifax could have attempted a chargeback on Mr A's behalf. The payments were made to a legitimate cryptocurrency exchange, which provided a service by exchanging his money for cryptocurrency. In view of that, there was never any realistic prospect of a successful chargeback, so I don't think the bank did anything wrong in deciding not to pursue one.

I don't say any of this to downplay the fact that Mr A has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for him and the position he's found himself in. However, my role is to look at the actions and inactions of the bank and, in the circumstances of this case, I'm not persuaded it did anything wrong.

Final decision

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 22 April 2025.

James Kimmitt
Ombudsman