DRN-4426025

The complaint

Mr A complains that Bank of Scotland plc, trading as Halifax, will not refund the money he lost as a result of an authorised push payment (APP) scam.

Mr A brought his complaint to this service through a representative. For ease I will refer solely to Mr A in this decision.

What happened

As both parties are familiar with the details of the scam I will not repeat them in full here. In summary, Mr A made four payments between 13 April 2021 and 21 April 2021 to his cryptocurrency account. From there he moved the money to an online trading platform. He had responded to an advert about financial investments on an online video sharing platform and was then contacted by the scammer. The payments totalled £3,900 and the highest was for £2,000. The first was made by debit card and the subsequent ones were all faster payments. Mr A realised he had been scammed when he was unable to access his funds and the scammer blocked him when he tried to make contact. It is not clear when this was; he complained to the bank on 27 October 2022.

Mr A says Halifax did not do enough to protect him and must refund the payments. Halifax says the payments were not high value or out of character enough such that it should have flagged them as suspicious and intervened. It also said there were red flags that ought to have prompted Mr A to complete further checks before proceeding.

Our investigator did not uphold Mr A's complaint. He said Halifax acted fairly and reasonably as the payments were not so out of character that there was reason for it to intervene. And as Mr A had moved the money onwards from his cryptocurrency account, Halifax could not reasonably have been expected to successfully recover the funds.

Mr A disagreed with this assessment and asked for an ombudsman's review. He said, in summary, these were the only transactions in excess of £1,000 in the 12 months prior and they were to a new payee that was a cryptocurrency exchange – this should have triggered a warning or intervention; Halifax failed to exercise its right to prevent this fraud; and the Contingent Reimbursement Model (CRM) code places obligations on Halifax that it has not met. He thinks these payments should fall under the code regardless of the fact they went to an account in his name.

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.

Having done so I am not upholding Mr A's complaint.

There's no dispute that Mr A made and authorised the payments. Mr A understood why he was making the payments and who he was sending the money to. At the stage he was making these payments, he believed he was firstly transferring money to a cryptocurrency

account in his name in order to move on and invest. I don't dispute Mr A was scammed and he wasn't making the transfers for the reasons he thought he was, but I remain satisfied the transactions were authorised under the Payment Services Regulations 2017.

It's also accepted that Halifax has an obligation to follow Mr A's instructions. So in the first instance Mr A is presumed liable for his losses. But there are other factors to take into account.

I have considered the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time. To note, as the payments were to an account in Mr A's name the principles of the CRM code do not apply in this case.

So, overall, I think that Halifax should have:

- been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.
- 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 financial institutions are generally more familiar with than the average customer.
- in some circumstances, irrespective of the payment channel used, taken additional steps or made additional checks before processing a payment, or in some cases declined to make a payment altogether, to help protect its customers from the possibility of financial harm.

In this case I don't think Halifax ought to be held liable for the transactions. I'll explain why.

I don't think the payments ought to have triggered an intervention from Halifax. I accept they were to a new payee that was at cryptocurrency exchange, but it was a legitimate platform and Mr A had made transfers of £4,200 (so in excess of the total value here) to another account in his name in February and March 2021. There was a payment of £2,200 and two of £1,000 which I would say were very similar to these transactions making them not out of character. So in the round, I don't think Halifax acted unfairly when it did not identify the payments as suspicious and intervene.

Mr A argues these payments should fall under the CRM code but for the code to apply the payment has to be made to an account held by another person. This service does not have the power to select the circumstances under which the guidance in the code applies.

Mr A also says Halifax ought to have intervened as he has difficulties reading and writing in English and the bank should have been aware of this. Mr A recalls that he told the bank this when he opened the account. He cannot provide any supporting evidence. However, Halifax has confirmed it was not on notice of Mr A's difficulties with English.

As the evidence here is contradictory, I have to make a finding on this point based on the balance of probabilities – in other words, what I think is most likely given the available evidence and the wider circumstances. And on balance, I cannot conclude with certainty that Halifax was on notice about Mr A's difficulties. I don't doubt that Mr A's testimony is his honest recollection, but I think the bank would have recorded his difficulties with reading and writing in English had it been told. It has a process to do so, and it would have anticipated this would be important information to capture. So I don't think Halifax was most likely aware of Mr A's vulnerabilities until this complaint investigation. I trust it will now record them and find out what reasonable adjustments Mr A requires.

I have also considered if Halifax did enough to try to recover Mr A's money once he reported the scam. It seems this was many months after the payments were made and not until the point of complaint. Mr A knew he had allowed the scammer access to the cryptocurrency account in his name to move the money on. So I don't think Halifax could reasonably have done anything to recover the money in the circumstances. I can see that Halifax didn't attempt a chargeback claim for the debit card payment. I think that decision was reasonable as it would have been out of time under the rules of the chargeback scheme - plus the cryptocurrency exchange had provided a service to Mr A as he expected.

It follows I am not instructing Halifax to refund any money to Mr A. This is a difficult decision to make, I'm sorry Mr A has lost a considerable amount of money and I can understand why he would like to be compensated for his losses. I do accept he has fallen victim to a sophisticated scam. But I can only consider whether the bank, which had no involvement in the scam itself, should be held responsible for what happened. For the reasons set out above I do not find Halifax can be held liable in the circumstances of this case.

My final decision

I am not upholding Mr A's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 13 December 2023.

Rebecca Connelley
Ombudsman