DRN-5138571

The complaint

Mr S complains that Bank of Scotland plc trading as Halifax didn't do enough to protect him from the financial harm caused by a job scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On 1 September 2023, Mr S was contacted by someone I'll refer to as "the scammer" who claimed to work for a recruitment company which I'll refer to as "T". The scammer told Mr S about an opportunity to earn commission by completing tasks. The scammer explained he'd be able to work part-time from home and that the job required him to purchase the tasks by sending cryptocurrency to an online wallet. He would earn commission for each task, but he wouldn't be able to withdraw any money until the tasks were complete. Unfortunately, T was a clone of a genuine company.

The broker asked him to first purchase cryptocurrency through cryptocurrency exchange companies I'll refer to as "B" and "C", and then load it onto an online wallet. Between 31 August 2023 and 4 September 2023, he made one debit card payment and five faster payments to two cryptocurrency exchanges totalling £25,228.49. He also made several cryptocurrency transactions using an account he held with an EMI I'll refer to as "R", and payments totalling £8,450. On 1 September 2023, he received a credit of £1471.51 from B.

Mr S realised he'd been scammed when the scammer kept asking him to pay higher amounts and he was prevented from making a withdrawal. He complained to Halifax stating it should have flagged the payments as suspicious, but Halifax refused to refund any of the money he'd lost.

It said the payments weren't covered under the Contingent Reimbursement Model (CRM) Code because they were to accounts in his own name, and the Code doesn't apply to debit card payments. It also said it was unable to raise a dispute under Visa's Chargeback scheme because the merchants had provided the service they'd offered.

It said the first three payments were in line with the previous account activity, so there was no cause for concern. It contacted him on 1 September 2023 and 2 September 2023 and during the calls, Mr S said there were no third parties involved, he'd been dealing with cryptocurrency for three years, and there was no one assisting or helping him with the payments. It said there was nothing further it could do to protect him because it didn't know what he was planning to do with the money after it reached the cryptocurrency exchanges, and he didn't disclose the real reason for the payments.

Mr S wasn't satisfied and so he complained to this service. He explained he didn't tell Halifax about the scammer because he was so desperate to get his money back.

Halifax explained that it provided warnings relevant to cryptocurrency trading on 1 September 2023 and 2 September 2023 and Mr S had opportunities to tell it he was making the payments as part of a job opportunity, but he said there were no third parties involved and he'd been dealing with cryptocurrency three years, so it was prevented from detecting the scam. It explained that after the calls, it marked the activity as genuine, so even though there were three high value payments the next day, it didn't intervene.

Our investigator didn't think the complaint should be upheld. He noted Halifax had discussed the attempted faster payment of £8,500 on 2 September 2023 and Mr S still wanted to go ahead despite appropriate warnings and questioning. Further, he told Halifax there was no third-party involvement, he had several years of experience in cryptocurrency, and he knew what he was doing. He accepted Mr S had been desperate not to lose his money, but he was satisfied that this had prevented Halifax from detecting the scam and that he'd have given the same answers if Halifax had intervened again. So, there was nothing it could have done to prevent the scam.

Our investigator explained the CRM Code doesn't cover faster payments to accounts in the consumer's own name or debit card payments. And Mr S had transferred funds to legitimate cryptocurrency exchanges in his name before moving the funds to an online wallet, so there would have been no chance of a successful recovery.

Finally, he explained that there was no prospect of a successful chargeback because Mr S had received a service from the cryptocurrency exchanges, so Halifax didn't act unfairly when it considered Mr S's chargeback claim.

Mr S has asked for his complaint to be reviewed by an Ombudsman, stating that Halifax could have implemented better fraud prevention systems. He's argued that it should have asked probing questions and had it done so it would have recognised that he was being influenced by a third party.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr S has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr S 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr S didn't intend him money to go to scammers, he did authorise the disputed payments. Halifax is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether Halifax could have done more to prevent the scam from occurring altogether. Halifax ought to fairly and reasonably be alert to fraud and scams and these

payments were part of a wider scam, so I need to consider whether it did enough when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Halifax to intervene with a view to protecting Mr S from financial harm due to fraud.

Halifax's blocked payments four and five. In considering whether it should have intervened sooner, I've noted that the first payment was a low value card payment to a legitimate cryptocurrency merchant, so there would have been no reason to intervene. Payments two and three happened within two hours of each other on 1 September and the cumulative total was £4,000 and as Mr S was paying a high-risk cryptocurrency merchant, I think Halifax should have intervened.

However, it blocked payment four, which was £1,500 to C on 1 September 2023. During the call, Mr S was questioned about the payment, and he said there was no third party involved and he'd been trading in cryptocurrency for two to three years. He was then given some information about cryptocurrency scams and the payment was resubmitted. I've considered what took place during the call and I'm satisfied it was a proportionate response to the risk presented by the payments, the questions were sufficiently probing, and the warning was relevant based on the information Halifax had. Significantly, it was prevented from detecting the scam or giving a more appropriate warning because Mr S didn't answer the questions honestly and, in those circumstances, I'm satisfied there was nothing else Halifax could have done to prevent Mr S's loss.

There was then another call when Mr S tried to pay £8,500 to C. During this call Mr S was asked similar questions and again he denied the involvement of a third party and confirmed he'd been investing for three years. Again, I'm satisfied that he was asked sufficiently probing questions and that Halifax was unable to detect the scam because he wasn't open about the fact he was making payments to buy tasks for a job in return for which he was expecting to be paid.

Based on what happened when Halifax did intervene, I agree with our investigator that it wouldn't have made any difference if it had intervened in any of the other payments because its likely Mr S would have answered the questions in the same way and Halifax wouldn't have been in a position to give a more tailored warning.

The final payment for £9,500 was made without any further intervention. Halifax has said that by this point C was a trusted beneficiary and I'm satisfied there would have been no reason to intervene again, particularly as the amount was only slightly more than the previous payment. And even if it had intervened, I don't think the outcome would have been any different, so I don't think there was anything else it could have done to stop the scam.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr S paid an account in his own name and moved the funds onwards from there.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S says he's fallen victim to, in all but a limited number of circumstances. Halifax has said the CRM code didn't apply in this case because it doesn't apply to payments to an account in the consumer's own name or to debit card payments, and I'm satisfied that's fair.

I've thought about whether Halifax could have done more to recover the card payment when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme

— so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Halifax) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr S).

Mr S's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr S's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Halifax's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr S to part with his funds. I haven't found any errors or delays to Halifax's investigation, so I don't think he is entitled to any compensation.

Overall, I'm satisfied Halifax took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Mr S has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Halifax is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 30 December 2024.

Carolyn Bonnell
Ombudsman