DRN-3870332

The complaint

Mr A complains that Bank of Scotland plc trading as Halifax didn't do enough to protect him from the financial harm caused by an investment scam company, 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.

Mr A was added to a telegram group for professional marketing investors who used the group to discuss their investment strategy and opportunities with a company I'll refer to as "B". The investors were complimentary towards the analysts who were offering 'signals' on cryptocurrency trading, which attempted to predict the cryptocurrency market to achieve a profit.

Mr A researched B and found positive reviews online. He also reviewed the trading platform and reached out to other members of the telegram group, asking for their opinion of the analysts. He was told the analysts were highly professional and competent and although they'd lost some money, they had eventually made a significant profit.

Mr A was contacted by someone claiming to be an analyst working for B, who told him to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. Mr A opened an account with a cryptocurrency exchange company I'll refer to as "K", and a trading account with "N". And between 6 June 2022 and 24 June 2022, he made five payments to K totalling £52,363.79. Four of the payments were transfers from his Halifax account and one was made using a debit card.

On 6 June 2022 Mr A £3,863.79 using his debit card, with no intervention from Halifax. Later the same day he attempted to transfer £15,000, but Halifax blocked the payment. During the subsequent call, Mr A was asked basic questions, such as whether anyone was forcing him to make the payment. The call handler also told him cryptocurrency was high risk, before releasing the payment.

When Mr A decided he wanted to make a withdrawal, he was told he needed to pay 15% commission, which he paid. He was then told he needed to pay capital gains tax on the profits, at which point he realised he'd been scammed. Mr A complained to Halifax arguing it should've stopped the payments. But Halifax refused to refund the money he'd lost. It said he'd failed to research the investment, stating he should have checked B was regulated by the Financial Conduct Authority ("FCA") and looked for independent reviews.

It said stopped the first debit card payment so it could check it was really him making the payment by sending a one-time passcode. It also stopped the second payment and he said he was sending money to his own cryptocurrency account and that no one else was involved. It also stopped payments on 9 June 2022 and 24 June 2022 and, based on what he told it, it couldn't have known he was being scammed.

Halifax stated it was signed up to the Contingent Reimbursement Model ("CRM") code, but as he'd sent funds to an account in his own name and it was lost from there to the fraudsters, he should complain to the provider from which he lost the funds.

Mr A complained to this service with the help of a representative. The representative explained Mr A had little to no knowledge of investing in cryptocurrency and had simply followed the instructions given to him. They argued Halifax would have known this type of scam often involves the use of a cryptocurrency wallet set up in the customer's own name. They said the transactions were out of character, so Halifax should have intervened.

Specifically, Mr A had previously only made small transactions for everyday spending, and he had never made large payments to cryptocurrency exchanges. Further, he sent his entire account balance to the cryptocurrency exchange company having transferred funds from other account, which should have raised concerns. He also made multiple large payments on the same day, all of which constituted a sudden and drastic change in the operation of the account.

The representative further argued that appropriately trained staff would easily have been able to identify this as a scam, but it failed to ask proper questions to understand what Mr A was doing and what the risk was. They argued the questions Halifax asked during the first call weren't appropriate, for example it should have asked whether there was a third party involved and how he met the third party. And had it done so, Mr A would have said he was sending funds to N and that he'd been contacted on a telegram group.

The representative said Halifax ought to have checked the FCA register and would have seen B was unregulated and it would have recognised that the story of how Mr A was groomed.

Responding to the complaint, Halifax said the circumstances in which Mr A was added to the telegram group and the fact he was told the investments could go from £32,000 to £38,000 or even £50,000 within three or four weeks should have raised concerns.

It also said that when Mr A made the first payment, he was presented with a payment categorisation warning and selected Investment and funds. It also payments 1, 2 and 4 were stopped and referred for checks, and each time Mr A confirmed he was paying his own account. He was advised the payments were high risk and he said he was aware of the risks involved and the possibility of losing his money. He also said there were no third parties involved and no one had contacted him with an offer to make money.

My provisional findings

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr A says he's fallen victim to, in all but a limited number of circumstances. Halifax had said the CRM code didn't apply in this case because the payments were to an account in Mr A's own name, and I was satisfied that is fair.

I was also satisfied Mr A '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 A is presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods

that were arguably unethical and/or misleading. However, while customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I carefully considered the circumstances, and I was persuaded this was a scam. But I explained that although Mr A didn't intend his 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 thought about whether Halifax could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I had seen, the payments were made to a genuine cryptocurrency exchange company. However, Halifax had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have intervened to warn Mr A 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 A from financial harm due to fraud.

The first payment for £15,000 on 5 June 2022 flagged for checks. I listened to the call Mr A had with the specialist fraud team, and I noted he was given a scam warning in that the call handler told him that people are sharing login details with third parties to gain maximum profits, and their accounts are being cleared out. But I noted he wasn't asked any questions around whether there was a third party involved or around the nature of the checks he'd completed.

The next intervention took place on 9 June 2022 when Mr A tried to pay £16,800 to K. I listened to this and noted that, this time the call handler did ask whether there was a third party involved and they also checked Mr A had received the funds into the account he held with K and warned him that cryptocurrency investments were high risk. Mr A didn't mention the fact he was following instructions from a third party and, based on the fact he wasn't open when he was asked whether there was a third party involved, I didn't think Halifax missed an opportunity to identify that he was the victim of a scam.

The final call took place on 24 June 2022, when Mr A tried to pay £8,300 to K. During this call, Mr A was given a very detailed and robust scam warning, whereby the call handler described in detail the methods used by the scammers, including the fact they contact people on social media and encourage victims to open accounts on trading platforms where they think they can see their funds.

I thought carefully about what took place during the three interventions and I was satisfied Halifax intervened at the points I would expect it to. I was also satisfied that, overall, it did enough across the three calls. I thought the call handler could have done more during the call on 5 June 2022 because they ought to have asked Mr A some detailed questions around how he learned about the investment opportunity, whether there was a third party involved and if so, how he met them, and whether he'd been promised unrealistic returns. I explained they should also have asked whether he'd checked the FCA website and more generally about the nature of the checks he'd undertaken.

Based on the fact Mr A denied the existence of a third party during the call on 9 June 2022, I had some concerns as to whether he would have been open in his responses if he'd been

had asked these questions during the first call. But considering he was paying £15,000 to a new payee which was associated with cryptocurrency, I said I would expect the call handler to have provided a similar scam warning to the one given on 24 June 2022.

However, as he went ahead with the payments having received a very thorough and effective scam warning on 24 June 2022, I didn't think the same warning on an earlier occasion would have made a difference to his decision to go ahead with the payments. Mr A's representative had said the questions around whether he'd given anyone access to his wallet weren't relevant, and I agreed with that. But I was satisfied the scam warning he received on 24 June 2022 was relevant, yet it didn't make a difference to his decision to go ahead with the payment.

Further, I explained there were no regulatory warnings with either the Financial Conduct Authority ("FCA") or International Organization of Securities Commissions ("IOSCO") websites to which Halifax could have drawn his attention, and it was clear Mr A believed B was genuine and that he considered he understood the investment based on the research he'd done into cryptocurrency over the previous two or three years. And he'd done some due diligence, including reaching out to other investors who he believed were genuine investors who were endorsing the investment. So, even if Halifax had done more during the call on 5 June 2022, I didn't think it would have made a difference to the outcome.

Overall, I was sorry to hear Mr A has lost money and the effect this had had on him. But for the reasons I explained, I didn't think Halifax could have prevented it so I couldn't fairly tell it to do anything further to resolve this complaint.

Developments

Neither party has made any further comments.

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.

Because neither party has added anything further for me to consider, my findings will be the same the findings in my provisional decision.

My final decision

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 A to accept or reject my decision before 30 November 2023.

Carolyn Bonnell
Ombudsman