DRN-3710123

The complaint

Mr H 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.

What happened

Mr H was a victim of an investment scam. A friend recommended an investment company I'll refer to as "C". The friend showed him C's website and explained he would first need to purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto his online wallet. Mr H was told the funds would show on the account he held with C and it would be very profitable.

Between 17 January 2022 and 4 February 2022, Mr H made eighteen payments using his Halifax Visa debit card. The payments, which totalled £31,045, were to a cryptocurrency exchange company who I'll refer to as "B". After making several payments to B, Mr H was able to withdraw a small sum of money from the account, but when he wanted to withdraw more, he was told he'd need to pay 28% of his balance. At this point he realised he'd been the victim of a scam.

Mr H contacted Halifax to ask it to refund the money he'd lost, but it said it couldn't raise a request under Visa's chargeback scheme because the cryptocurrency exchange had correctly provided the service it was supposed to provide. It also said that as the payments were made via debit card, they wouldn't be covered under the Contingent Reimbursement Model (CRM) code.

Halifax also said Mr H had made payments of both larger and similar amounts the previous year, so the disputed payments weren't unusual. And they had left the account with a healthy balance each time, so the payments weren't flagged for further checks.

Mr H wasn't satisfied and so, with the help of a representative, he complained to Halifax asking it to refund the payments. The representative said the payments were out of character and Halifax should have intervened.

Halifax explained it was difficult to evidence why a refund would be due under Visa's chargeback scheme and as the money from Mr H's account was paid to the exchange company and not the scammer's account, the chargeback would be against the exchange company. And as the exchange company had carried out the service they've been instructed to provide, it would be unable to ask them for a refund. It also said it didn't think the payments were unusual.

Mr H wasn't satisfied and so, with the help of his representative, he complained to this service. The representative argued the transactions were out of character and Halifax should have intervened to prevent the fraud. He argued that cryptocurrency scams have been prevalent since 2018 and Halifax would have been aware of how this type of scam operated and how common it was. He said the fact Mr H was sending money to a cryptocurrency

exchange company should have raised concerns and the fact B was very popular with scammers means Halifax should have identified the transactions as high risk.

The representative said that on 17 January 2022, Mr H had sent a payment which was larger than normal to a new payee which was also a very high-risk cryptocurrency exchange. Mr H had no history of sending large payments and had not previously sent money to a cryptocurrency exchange. The following day, he sent a large sum of money over multiple transactions, again, without any intervention from Halifax.

The representative argued that if Halifax had intervened with thorough questioning around the purpose of the payments and provided information about the risk of scams, the fraud would have been prevented. He explained Mr H had little to no knowledge of cryptocurrency or cryptocurrency wallets and simply followed instructions given to him.

Our investigator didn't think the complaint should be upheld. She agreed the activity on Mr H's account on 18 January was unusual and ought to have triggered an intervention from Halifax. But she didn't think this would've made a difference to his decision to go ahead with the payments because the investment opportunity had been recommended by a close family friend who seemed to be making a good profit.

Our investigator explained that on 18 January 2022, there wasn't enough evidence to say C was a scam as there were no regulatory warnings with either the Financial Conduct Authority ("FCA") or International Organization of Securities Commissions ("IOSCO") or negative comments or reviews online. So, all Halifax could've done would be to provide information about cryptocurrency scams and the relevant regulations needed to offer investment services to UK customers. She noted Mr H understood his friend was receiving returns and that he had started to receive return too, so she didn't think a warning would have outweighed the confidence this had given him.

Mr H's representative has asked for the complaint to be reviewed by an ombudsman and disputes our investigator's suggestion that Halifax couldn't have done anything apart from provide information. He's argued that thorough questioning would have uncovered the involvement of an unregulated third-party, the fact returns were presented in a portal and that Mr H had been told the more he invested, the higher the return. This information would have alerted Halifax to the fact this was probably a scam.

He believes Halifax would have told Mr H about the types of scams they see and warned him about the fact cryptocurrency investment scams often involve people being directed by a third party to invest via a cryptocurrency wallet.

The representative also pointed out Mr H only received £100 in returns and that this wouldn't have affected his decision to go ahead with the payments and that Halifax would have known that small early returns are common in this type of scam. The representative has also clarified that the family friend was the husband of a someone who lives down the street. The person wasn't a sophisticated investor who had only received fake returns, which, Halifax would have explained, wasn't a reliable source.

Finally, the representative argued that even if Mr H had chosen to go ahead with the payments, Halifax should have refused to remove the block.

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 H 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.

CRM Code

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

I'm also satisfied Mr H '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 H 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've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. But, although Mr H 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.

Chargeback

I've thought about whether Halifax could have done more to recover Mr H's payments 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 H).

Mr H's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers to C. It's only possible to process a chargeback claim against the merchant that received the disputed payments. It's most likely that B would have been able to evidence it had done what was asked of them. That is, in exchange for Mr H's payments, it 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 the cryptocurrency exchange company was fair.

Prevention

I've also 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've 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 need to consider whether it ought to have intervened to warn Mr H 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 H from financial harm due to fraud.

The payments didn't flag as suspicious on Halifax's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr H normally ran his account and I agree that they were.

On 17 January 2022 Mr H paid £3,000 to B and while I accept this is a lot of money, it's not so large that it should have triggered Halifax's fraud systems. This is because it's not unusual for people to make the odd larger payment, even if this isn't something they do regularly.

However, on 18 January 2022, Mr H made two payments to B for £2,500, followed by a further four payments of £2,445 each. These multiple payments totalled £14,780 and I'm satisfied that this, as a total daily spend, was unusual for Mr H's normal spending habits and should have triggered Halifax's fraud systems.

If Halifax had contacted Mr H on 18 January 2022, it should reasonably have asked several probing questions concerning the purpose of the payments and the circumstances of the investment. Mr H's representative has correctly pointed out that from 2018 onwards, we would expect banks to know there were several scams involving cryptocurrency and the common traits of such scams. Consequently, I would expect Halifax to have questioned Mr H about why he was investing in cryptocurrency, what he'd been told about possible returns on the investment, whether he was being assisted by a broker, who the broker worked for, whether the company was regulated in the UK and anything else he knew about how the investment actually worked. It should also have asked some questions around Mr H's investment experience.

I'm satisfied that if Mr H had been asked these questions, he'd have answered truthfully because there's no evidence of him having misled the bank before or that he was told to do so by the scammers. And, consequently, I'm satisfied that Halifax would likely have gathered enough information to suggest the investment could be a scam.

If this was the case, I would expect Halifax to have advised Mr H the investment could be a scam and the reasons why it had reached that conclusion. I would then expect it to advise Mr H to check the FCA register and to consider whether the returns he'd been promised were realistic.

Our investigator said that, even if Halifax had intervened, she doesn't think it would have made any difference to Mr H's decision to proceed with the payments because he knew someone who had used C and this had given him confidence that the company was genuine. The friend was positive about the returns he'd made, and the endorsement led Mr H to look into C himself. She also noted he said he felt confident because he was able to deposit, and then withdraw funds back into the account he held with B.

Mr H's representative has also downplayed the relationship Mr H had with the 'friend' and said he believes the friend had also received fake returns.

Based on the available evidence, I accept Mr H used C as it was recommended by someone he knew, and, regardless of the closeness of the relationship, he trusted the company was

genuine based on the fact someone he knew had invested with them and was making some money. I accept those returns are unquantified and that they were likely fake returns, but I am satisfied this legitimised C in Mr H's eyes. Similarly, the fact that Mr H had made some withdrawals by 18 January 2022 would have instilled yet more confidence in the fact the investment was genuine, albeit the returns were small.

The main crux of this complaint is whether Halifax could reasonably have said anything to Mr H to change his mind about going ahead with the payments. I think at that point, Halifax could have told Mr H that B was a company about which Action Fraud had concerns and that the investment shared some common traits with other cryptocurrency scams. But this was a sophisticated scam which had all the hallmarks of a genuine investment, and I don't think this information alone would have outweighed the confidence Mr H had that the investment was genuine.

Halifax could have told Mr H to do some more research, but there were no warnings about C on either the FCA or the IOSCO websites and at the time. And I haven't seen any evidence of negative information about C online. C wasn't regulated by the FCA and this is sometimes be an indication of a scam, but even if Mr H had seen C wasn't regulated, because there were no other obvious warnings this was a scam and they weren't based in the UK, I don't think there was anything Mr H could have done to confirm this was a scam. Consequently, while I accept Halifax failed to intervene on 18 January 2022, I don't think its failure to do so represented a missed opportunity to prevent Mr H's loss.

Mr H's representative has argued that, even if Mr H had gone ahead with the payments, Halifax ought to have refused to make the payment. But I disagree. While there were signs to indicate this was a scam, I don't think it was possible to say for certain, so I wouldn't expect Halifax to have refused to make the payments. B was a genuine cryptocurrency exchange company that many people used for genuine investments, so the involvement of B alone would not be confirm this was a scam.

Overall, while I think Halifax should have done more when Mr H tried to make the payments on 18 January 2022, I don't think it would have prevented Mr H's loss. I'm sorry to hear he's 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 H to accept or reject my decision before 22 March 2023.

Carolyn Bonnell
Ombudsman