DRN-4766736

The complaint

Mr C 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, 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.

In May 2022, Mr C received a WhatsApp message from some who I'll refer to as "the scammer" who said she'd contacted him by mistake. She said she worked in cryptocurrency and asked if he was interested in investing. Mr C said he wasn't interested, but they continued to communicate daily through WhatsApp. The scammer told Mr C he could earn an amazing income which banks didn't like because the returns were better than a savings account.

When Mr C eventually decided to invest, the scammer sent him a link to a scam platform which I'll refer to as "C" and advised him to use his email address and create an account. This required him to provide his contact information, ID, proof of address, and a picture of his bank card. Mr C noted the website included a 'contact us' section and a live chat, which reassured him it was genuine.

The scammer told Mr C to create an account with a cryptocurrency exchange company and that he could start with an initial investment of £250, which Mr C paid on 30 May 2022. She asked him to first purchase cryptocurrency through the cryptocurrency exchange company and then load it onto an online wallet. Between 30 May 2022 and 25 July 2022, he made a further nine payments to two cryptocurrency exchange companies totalling £18,415.71 using both faster payments and a debit card connected to his Halifax account.

After the first two payments, the scammer told Mr C the more he invested the more profit he'd make promising him he could double what he invested if not triple. In June 2022, Mr C withdrew £100, but when he tried to make a larger withdrawal on 25 July 2022, he was told his account had been frozen and he'd need to pay tax to make a withdrawal. As he had no money left to invest, the scammer told him to take out a loan or use a credit card, so he paid an additional £5,000 using a credit card. He realised he'd been scammed when the scammer said Mr C was being investigated for money laundering and that he would need to pay a further £15,000.

Mr C complained to Halifax stating he hadn't previously sent high value payments in such a short time frame, so the spending was unusual for the account. But Halifax reused to refund any of the money. It said the payments weren't covered by the Contingent Reimbursement Model ("CRM") code because Mr C had paid an account in his own name and the code didn't apply to debit card payments.

It said the payments weren't unusual because they were made using Mr C's online banking and debit card and he'd sent payments in the same way previously. Further, before the first

payment was set up, it said it couldn't confirm if the payee details matched. Mr C said he was paying an investment and he was shown the following warning: *"Make sure this investment is real. Deals that look too good can be scams. Do lots of research - good deals don't find you. See what your friends and family think. Use the FCA to check an advisor or company. Find out how to stay safe from scams on our Fraud Hub".* It also gave further warnings when he made the £5,000 and £10,000 payments, but he chose to continue.

Mr C wasn't satisfied and so he complained to this service with the assistance of a representative who argued Halifax should have intervened as he made nine payments to two new payees linked to cryptocurrency that totalled £18,415.71 within the space of 55 days. They said in the months prior to the scam, the highest payment on the account was for £1,900 and Halifax should have intervened because Mr C was making payments of large and unusual amounts to new payees which were linked to cryptocurrency. He made multiple payments to the same payee on the same day and there were large amounts of money coming into the account and quickly being transferred out.

The representative said Halifax should have contacted Mr C to ask him questions about the payment and as he wasn't coached to lie, it would have realised he was falling victim to a scam and provided a scam warning.

Our investigator felt the complaint should be upheld. He didn't think the first two payments were suspicious or out of the ordinary. But he thought Halifax ought to have been concerned about the payment of £10,000 on 6 June 2022 because the prior spending on the account was generally much lower value day to day spending, including purchases at supermarkets, council tax payments and direct debit bill payments.

He was satisfied that if Halifax had contacted Mr C and asked relevant questions about the payment including whether there was a third party involved and how he met them, it's likely he'd have explained that he'd been contacted out of the blue by someone who had persuaded him the invest in cryptocurrency and that he'd been advised to make an onwards payment from the cryptocurrency exchange. He also explained that Mr C would have heeded a meaningful scam warning and ceased sending payments. Because of this he recommended that Halifax should refund the money Mr C had lost from the third payment onwards.

He further explained he didn't think Mr C had acted unreasonably because even though he didn't conduct any due diligence, he hadn't seen any evidence that the scammer purported to be working for a particular company or that she was a professional broker. And there was no negative information online about C prior to the first disputed payment in May 2022. So, had he conducted due diligence at that point he wouldn't have found anything to indicate that the investment was a scam.

Finally, our investigator explained there would have been no prospect of a successful recovery as Mr C had transferred funds to legitimate cryptocurrency exchanges and the funds were moved on from there.

Halifax has asked for the complaint to be reviewed by an Ombudsman. It agrees it should have intervened when Mr C made the third payment, but it has argued there should be a deduction of 50% for contributary negligence because there were red flags present including the fact he'd received a message out of the blue via WhatsApp from someone he'd never met and didn't know, he'd been promised unrealistic returns, and he didn't receive any paperwork relating to the investment.

It has argued that Mr C should have taken steps to check the investment was genuine before going ahead such as checking which company the scammer worked for or asked for

some documents to review. It accepts there were no warnings about C, but he should have done some preliminary checks and had he done so he'd have seen the FCA warning about cryptocurrency dated in 2018.

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.

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 C 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 Mr C paid accounts in his own name and the code doesn't apply to debit card payments, and I'm satisfied that's fair.

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

Mr C'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 C'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.

I'm satisfied Mr C '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 C is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr C 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

Both parties agree that Halifax ought to have intervened when Mr C made the third payment and that it would likely have made a difference to the outcome, so Halifax should refund the money he lost from that point onwards. But Halifax has argued that the settlement should be reduced by 50% for contributory negligence, so I've gone on to consider that.

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mr C was to blame for the fact he didn't foresee the risk.

Having considered the circumstances of this scam, I'm satisfied it was sophisticated and I don't think it was unreasonable for Mr C to have thought it was genuine. Mr C has explained that over time he'd grown to trust the scammer, that he'd been impressed by C's professional-looking website, the fact he'd been required to provide ID when he created the trading account, and the fact he could see what he thought were his profits on the trading platform, so he believed this was a genuine investment opportunity.

I accept Mr C was shown some warnings when he made the payments, but these warnings weren't sufficiently tailored to the circumstances. And I've seen no evidence that he had any investment experience, so I wouldn't expect him to have known about the risks or that there were red flags present which meant he should have done more to check that what he was being asked to do by the scammer was legitimate. Consequently, I don't think he contributed to her own loss in failing to do so.

Halifax has argued that Mr C ought to have been concerned about the returns he was being promised. But in recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mr C to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

Halifax has suggested Mr C could have detected the scam if he'd done some due diligence, but there was no information online about C at the start of the scam (adverse or otherwise) and I don't think the FCA warning dated in 2018 would have made any difference because he believed the investment was genuine. So, I don't agree that basic research would have uncovered the scam.

Consequently, while there may be cases where a reduction for contributory negligence is appropriate, I don't think this is one of them.

Compensation

I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I don't think Halifax needs to pay any compensation given that I don't think they acted unreasonably when they were made aware of the scam. And he wasn't entitled to compensation for legal fees, as our service is free to access.

Recovery

Mr C has described that he paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I'm satisfied there was no prospect of a successful recovery.

My final decision

My final decision is that Bank of Scotland plc trading as Halifax should:

- refund the money Mr C lost from the third payment onwards.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Bank of Scotland plc trading as Halifax deducts tax in relation to the interest element of this award it should provide Mr C with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 4 July 2024.

Carolyn Bonnell
Ombudsman