DRN-4262386

The complaint

Mr R 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 2020, Mr R saw some adverts on TV about the benefits of investing in cryptocurrency and so he looked online for investment opportunities. He came across various companies and left his contact details via an online contact form.

Shortly afterwards, he was contacted by someone I'll refer to as "the scammer" who claimed to work for an investment company I'll refer to as "B". The scammer said would advise him how to invest in cryptocurrency and the more money he invested, the more money he would make.

Mr R checked B's website which looked extremely professional as did the documents he was given. He was also reassured because the scammer told him he could make withdrawals whenever he wished.

He created an account with B, which required him to send a copy of his ID to verify the account. He also downloaded remote access software so the scammer could give him the details of each payee before he made the payments. The scammer asked him to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Between 22 May 2020 and 17 November 2021, he made 25 payments totalling £163,028.28 from his Halifax account. This included four debit card payments, one international money transfer and twenty faster payments. He also received credits during the scam period.

Following each payment Mr R saw funds enter his trading account and his account balance increase. He funded the payments with his savings and on the advice of the scammer he took out a loan from Halifax, used credit cards and borrowed money from family. He was also forced to sell his home to pay off the debt.

Unfortunately, following the sale of his home in February 2021, the scammer got in touch and told Mr R to send more funds, but in November 2021 he ran out of money and stopped sending funds. When he later discussed the investment with his brother-in-law, he realised he'd been scammed.

Mr R complained to this service with the assistance of a representative who said Halifax didn't block any of the payments or provide scam advice and if it had warned him about the risks, his loss could have been prevented. He said it had many opportunities to intervene despite red flags which included multiple unusual payments to new payees linked to

cryptocurrency, a sudden change to the operation of the account, ten new payees in six months and multiple payments on the same day to the same payee.

The representative explained that in the three months before the scam, Mr R used the account for low-value day-to-day spending and the highest payment was only £500. Furthermore, the scam payments took the account into overdraft which was a change in spending habits and should have indicated that he was at risk of fraud, as should the rapid movement of funds into the account including £165,243.60 in February 2021 following the sale of his home.

They said the Financial Conduct Authority ("FCA") have now banned one of the cryptocurrency exchanges from carrying out financial activities in the UK and there are a lot of banks blocking transactions made to cryptocurrency exchanges due to investment fraud, so it should have been immediately alerted to the very real possibility of fraud on the account.

The representative said Halifax should have contacted Mr R and asked why he was making the payments, who he was trading with, how he found out about the company, what research he'd done, whether he'd checked the FCA register and what returns he'd been predicted. And as the answers he provided didn't match the payment activity, it would have realised he wasn't being honest and identified he'd been scammed.

Halifax said Mr R should have done more checks to make sure the scammer was genuine and when it spoke to him, it told him the investment was high risk and he wouldn't be able to get his money back, but he still sent the money. However, it accepted it should have contacted him and tried to warn him sooner and that when it did speak to him it should have had more doubts and probed further or asked him to pop into a branch.

It agreed to refund the loss in full from 3 November 2021 because it accepted it had missed an opportunity at that point to provide tailored warnings and invoke Banking Protocol. And it said it would share liability for his loss and pay him 50% of the payments he made from 29 June 2020 to 21 October 2021. It also paid him £200 compensation to make up for the things it could've done differently.

Our investigator was satisfied Halifax's offer was fair. She agreed there would have been no concerns around the first six payments but she felt payment seven was unusual when compared to the previous activity on the account, so she agreed it missed an opportunity to intervene from that point.

She noted Halifax spoke to Mr R on a number of occasions and he was asked if anyone else was involved, which he denied. On 3 March 2021, the call handler said he should contact the merchant if he had concerns and he said he wanted to think before he made the payment. He was directed to check Trustpilot for reviews and she was satisfied that if he'd done so, he'd have seen negative reviews about B. In a further call on 3 November 2021, Mr R said he paying for a holiday and on 16 November 2021, he said the payment was for web development service. So she was satisfied Halifax's decision to reduce the first part of the settlement for contributory negligence was fair.

She also explained that by the time Mr R reported the scam, the timeframe to raise a chargeback on the card payments had passed. And in any event, the merchants would probably have they transferred the funds as directed. She explained that as the faster payments were to accounts in his own name, the CRM Code wasn't applicable. And its unlikely funds could've been recovered as they were sent from accounts in Mr R's name to the scammer. Finally, she was satisfied the compensation Halifax had awarded was fair and

she explained our service is free for consumer to use, so she wouldn't be asking it to pay any of Mr R's legal costs.

Mr R's representative has argued that the settlement should only be reduced by 25% because his behaviour during the phone calls should have raised concerns and Halifax should have invoked Banking Protocol. They've argued that the call on 3 March 2021 put Halifax on notice that the payments related to cryptocurrency, his comments on 3 November 2021 should have raised concerns and it wasn't appropriate to tell him to check Trustpilot.

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 R 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.

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 R says he's fallen victim to, in all but a limited number of circumstances. But the CRM code didn't apply to these payments because Mr R was paying accounts in his own name.

I've thought about whether Halifax could have done more to recover the debit card 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 R).

Mr R'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 R'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.

Further, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mr R's case, the claim was referred to Halifax after this time, so this wasn't an option.

I'm satisfied Mr R '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, he is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr R 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've 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 genuine cryptocurrency exchange companies. However, 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 ought to have intervened to warn Mr R 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 R from financial harm due to fraud.

The payments did flag as suspicious on Halifax's systems so I've considered the nature of those interventions in the context of the whether Halifax did enough when it did intervene. The first six payments were relatively low value and Mr R was paying legitimate cryptocurrency exchanges, so Halifax didn't need to intervene. However, I agree it ought to have intervened from the seventh payment on 29 June 2020, so I think the offer to refund the payments from that point onwards is fair.

Halifax has offered to refund 100% of the payments from 3 November 2021 on the basis that it missed an opportunity to provide tailored warnings and invoke Banking Protocol during the call that took place on that date. I'm satisfied that's fair and reasonable in the circumstances. However, it has only offered to refund 50% of the payments Mr R made from 29 June 2020 to 21 October 2021 because even though it accepts it missed an opportunity to intervene on 29 June 2021, it has argued that Mr R had contributed to this own loss, so the settlement should be reduced accordingly. Mr R doesn't agree with this and so I've considered whether a reduction for contributory negligence is fair.

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence. This was a sophisticated scam and B's website had several features which resonated with a genuine companies website. He was also required to provide ID which gave Mr R the impression B was genuine as did the fact the scammer seemed extremely professional.

Mr R could see his account balance increase throughout the scam and 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 him to have believed what he was told by the scammer in terms of the returns he was told were possible, especially as he hadn't invested in crypto before.

However, I note Mr R was funding the investment with loans and credit cards and I haven't seen any evidence that he did reasonable due diligence or that he followed Halifax's advice to check for negative reviews on Trust Pilot, even though it's clear he understood why he'd been advised to do more checks. It's clear he ignored the warnings he was given when Halifax did intervene and that he wasn't honest when said he was paying for a holiday/rental and paying for web development. I accept it's well known that scammer's coach their victims to lie and I agree Halifax ought to have questioned Mr R's explanation for making the payments but in the circumstances I'm satisfied he could have done to protect himself and so I'm satisfied that Halifax's decision to reduce part of the settlement by 50% is fair.

Mr R's representative has argued that he should be refunded in full from an earlier point, but while there's no dispute that Halifax could to have taken more positive steps to stop the scam from 3 November 2021, I don't think it missed an opportunity to detect the scam any

sooner than that. And even if it did, I'm satisfied Mr R did contribute to his own loss and that the reduction for contributory negligence is fair.

Compensation

I'm satisfied £200 is fair and I don't think Mr R is entitled to any legal costs.

Recovery

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

Overall, I'm satisfied Halifax's offer is fair. I'm sorry to hear Mr R has lost money and the effect this has had on him. But for the reasons I've explained, 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 R to accept or reject my decision before 30 April 2024.

Carolyn Bonnell
Ombudsman