DRN-4483773

The complaint

Mr and Mrs H complain that HSBC UK Bank Plc didn't do enough to protect them from the financial harm caused by an investment scam company, or to help them recover the money once they'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 H came across an online advertisement for an investment company I'll refer to as "C" which was endorsed by a well-known celebrity. He completed an enquiry form and made a payment of £250, after which he was contacted by someone claiming to be a broker working for C. The broker told Mr H he could help him to invest in cryptocurrency and that he should earn enough to help fund his mortgage repayments.

The broker told Mr H to download AnyDesk remote access software to his device and to open a trading account with C and an account with a cryptocurrency exchange company I'll refer to as "F".

Mr H visited C's website and believed that it looked professional and he was reassured because he was able to start with a small investment. The broker asked him to first purchase cryptocurrency through a F and then load the cryptocurrency onto an online wallet. Between 4 August 2022 and 19 June 2023, he transferred 22 payments to F totalling £95,118.

Mr H made a test payment to F for £1 on 4 August 2022 and on 14 September 2022, the broker showed him how to make a withdrawal and £81 was credited to his account from F. He was the encouraged to invest further funds, which he did up to February 2023. And from 8 June 2023, Mr H made what he believed were payments to Blockchain for the release of his funds. During the scam period, he took out loans for £19,000 and £25,000, which have since been paid off.

Mr H contacted HSBC when he realised he'd been scammed, arguing that the payments should have been flagged for further checks. But HSBC refused to refund any of the money he'd lost. It said the Contingent Reimbursement Model ("CRM") code wouldn't apply to the payments because Mr H paid an account in his own name and control. It also explained fraudulent transactions can be authorised on a customers' account without being picked up by the Fraud Detection System.

Mr and Mrs H weren't satisfied and so they complained to this service with the assistance of a representative. The representative said HSBC should have intervened and asked questions about the purpose of the payments. They argued the payments were unusual for the account as Mr H had never purchased cryptocurrency before and was making large transfers into the account from his other accounts before sending the funds straight out again to a cryptocurrency merchant. He had also taken out two loans to fund the investment.

The said HSBC should have asked Mr H about the purpose of the payments and he would have explained he was being advised by a broker to invest in cryptocurrency. HSBC would have known to check the Financial Conduct Authority ("FCA") register and it would have identified other red flags including the use of AnyDesk, the fact C was endorsed by a celebrity, and the fact Mr H had been advised to send money to a cryptocurrency wallet held by an unregulated third-party. And with this information it would have been able to warn Mr H about the risk of scams and provide advice on how to protect himself.

Our investigator didn't think the complaint should be upheld. She confirmed the payments weren't covered under the CRM code because they were to an account in Mr H's own name. And she didn't think Payments 1 to 3 were unusual because the account had a history of making payments of similar value. She accepted the historic payments were to existing beneficiaries, but by the time Mr H made the slightly larger payment of £7,580 on 30 September 2022, F was no longer a new payee.

Our investigator went on to explained that she thought HSBC ought to have intervened when Mr H made the fourth payment because it was a larger payment and the account didn't have a history of similar payments. She also thought that as he was making further large payments in quick succession to a high risk merchant having had loans credited to the account, HSBC missed other opportunities to intervene on 6 June 2023, 8 June 2023, 9 June 2023, 12 June 2023 and 19 June 2023.

However, she didn't think an intervention at any of those points would have made a difference because she thought Mr H would have gone ahead with the payments even if he was warned of the potential for a scam. She accepted that if HSBC had contacted Mr H, based on what he said to his other bank ("Bank R") when it questioned him about payments from that account, he would probably have said that he was investing in cryptocurrency with the help of a broker he'd found online. And she was satisfied that this would have been enough for HSBC to have identified that he was making payments to a scam.

However, she didn't think an intervention or warnings from HSBC would have made any difference to Mr H's decision to go ahead with the payments because he was taking advice from the broker and had already ignored a warning from Bank R.

She explained that on 3 May 2023, Mr H had told the broker about a call he'd received from someone stating his dealings with C were fraudulent and that he'd hung up the phone because the broker had cautioned him about scams. The broker told Mr H he should talk to him immediately whenever he gets a question. On 6 June 2023, Mr H told the broker that Bank R had told him the investment was a scam, and on 7 June 2023 he told him someone else had called asking to connect to his phone through AnyDesk but he'd refused because he recalled the broker cautioning him. Finally, on 9 June 2023, he told the broker that Bank R had agreed for him to trade because he had accepted its scam conditions.

Our investigator also explained that Bank R had warned Mr H the investment was a scam. It also told him the email address he'd received from Blockchain wasn't a legitimate contact. He was asked to confirm that he acknowledged the warnings and that he didn't intend to continue with the investment which he responded to by saying he wanted his funds returned and his account closed.

Our investigator noted Mr H told the broker on 6 June 2023 that Bank R had told him the investment was a scam, yet he continued to make payments. And when he was unable to make payments from the account he held with Bank R, he proceeded to use other accounts to make further payments. This showed he was clearly under the spell of the scammer to the extent that he trusted what he was told by the broker over the advice he was given by Bank

R. Because of this, she concluded that, even if HSBC had intervened and provided a scam warning, she didn't think it would have prevented Mr H from making further payments.

Mr and Mrs H have asked for the complaint to be reviewed by an Ombudsman. The representative has argued that Mr H had told the truth to Bank R, so the only reasonable conclusion is that an intervention from HSBC would have exposed the scam. The red flags included the fact Mr H discovered C on social media and it was endorsed by a celebrity, it was an unregulated investment company, he was told to use AnyDesk, and he'd been asked to send money via a cryptocurrency exchange to a third-party wallet.

The representative has argued that Bank R didn't stop Mr H from making payments despite knowing it was as scam and that it didn't say for certain that it was a scam when he asked how it knew the investment was a scam, which left open the possibility that it wasn't. They don't accept he ignored Bank R's advice or that he was under the spell of the scammer because he asked it to explain why the investment was scam. Finally, they've argued that Bank R's intervention was poor and shouldn't be used against Mr H as evidence of how Mr H would have responded to a warning from HSBC.

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 and Mrs H have been the victims of a cruel scam. I know they feel strongly about this complaint and this will come as a disappointment to them, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr and Mrs H says they've fallen victim to, in all but a limited number of circumstances. HSBC has said the CRM code didn't apply in this case because Mr H was paying an account in his own name, and 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.

There's no dispute that this was a cam, but although Mr H didn't intend the money to go to scammers, he did authorise the disputed payments. HSBC 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 HSBC 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, HSBC 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 H when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect HSBC to intervene with a view to protecting Mr H from financial harm due to fraud.

The payments didn't flag as suspicious on HSBC's systems. I agree with our investigator that even though Mr H was paying a cryptocurrency merchant, the first three payments weren't unusual when compared to the normal spending on the account, so I don't think HSBC needed to intervene when he made those payments. I also agree that, by the time Mr H made the fourth payment of £10,037 on 24 November 2022, the spending was unusual when compared to the historic payments on the account, so HSBC should have intervened.

It should have contacted Mr H and asked him why he was making the payments, whether there was a third party involved and if so how he learned about the third party, whether he'd been promised unrealistic returns, whether he'd been allowed to make any withdrawals, whether he'd been told to download AnyDesk and whether he'd been advised to make an onwards payment from the cryptocurrency exchange. And as Mr H was open in his responses when he was questioned by Bank R, I'm satisfied he'd have told HSBC that he'd been advised to invest in cryptocurrency a broker who worked for a company that had been endorsed by a well-known celebrity and that he'd been told to download AnyDesk to his device.

With this information, I'm satisfied that HSBC would have identified that the payments were being made to a scam and so it have told him there were red flags present and provided a tailored scam warning, including advice on additional due diligence.

However, I agree with our investigator that an intervention from Halifax on 24 November 2022 or at any other point in the scam period wouldn't have made any difference to Mr H's decision to go ahead with the payments. This is because, while I accept there were red flags present which HSBC could have brought to Mr H's attention, I agree with our investigator that Mr H's conduct after the intervention from Bank R means it's unlikely that a warning from HSBC would have made any difference.

Bank R warned Mr H that the investment was a scam and that the email address from Blockchain wasn't legitimate. His representative has argued that it didn't confirm that the investment was a scam, despite Mr H having asked it to do so. But I'm satisfied Bank R gave a very clear warning that he was making payments to a scam and that it did all it reasonably could to highlight the risk to Mr H and in the circumstances I don't think it could reasonably have done anything more.

After the interaction with Bank H, instead of doing further due diligence, Mr H engaged in communications with the broker which demonstrate that he was more inclined to listen to the broker's advice than the advice given Bank R and I'm satisfied he'd have done the scam if HSBC had intervened.

Further, having being told by Bank R that C was operating a scam, Mr H took out two loans on the advice of the broker and there is evidence that other loan applications were rejected. He also made 17 further payments to the scam. This tells me that if HSBC had intervened and told Mr H that he was making payments to a scam, it wouldn't have made any difference. His representative has said HSBC should have gone further and explained why the investment was a scam and this would have stopped Mr H from making the payments. But I don't think HSBC could reasonably be expected to have done anything more than Bank R did in the circumstances.

So, while I accept that HSBC missed opportunities to intervene, I don't think this represented a missed opportunity to prevent Mr and Mrs H's loss and so I can't fairly ask it to do anything further to resolve this complaint.

Compensation

Mr and Mrs H aren't entitled to any compensation of legal fees from HSBC.

Recovery

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

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 and X to accept or reject my decision before 25 January 2024.

Carolyn Bonnell
Ombudsman