DRN-4406619

The complaint

Mr R complains that HSBC Bank UK Plc 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.

In November 2021 Mr R received a friend request on social media from someone I’ll refer to as “the scammer”. He checked her profile and could see she had a lot of photographs and posts with comments and interactions, so he accepted the request and began exchanging messages. The scammer told Mr R that he’d appeared as a suggested friend and after a few weeks, they began to communicate on Telegram.

She eventually told him that in addition to her job, she also invested in cryptocurrency. She didn’t push him to invest but she occasionally mentioned how her investments were performing. She told him she used a trading platform I’ll refer to as “P”, which Mr R researched, noting the website seemed professional and included information indicating it was a genuine company. He also discovered it had a social media page which included videos about trading. He checked the reviews on Trustpilot, which were positive, and he noted it was registered on Companies House with a registered office in London.

The scammer told Mr R to open an account with P, which required him to upload personal information and a copy of his ID as part of the KYC and Anti-Money Laundering (AML) checks. He received an email confirming the account had been verified and the scammer told him the minimum investment for a beginner would be £1,000, and the deluxe option would require £5,000.

Mr R was assigned a broker who explained the scammer would receive a bonus for the referral. The returns would be dependent on what he invested but the returns would be positive. He said he would guide Mr R on which trades to place and advised him to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Between 12 May 2022 and 12 December 2022, he made 26 payments to two cryptocurrency exchange companies totalling £75,215.41 using a Visa debit card connected to his HSBC account. This included transaction fees totalling £1,418.18.

On 12 May 2022 Mr R made an initial payment of £817.39. Then on 6 September 2022, he paid £4,370.25 for a deluxe account. In October 2022, he made further payments totalling £13,244.28, and in November and December 2022 he paid £16,528.47 and £38,453.44.
At the end of December 2022 Mr R was told he needed to pay the annual account fee of £20,000, so he asked his brother to lend him the money and he was subsequently alerted to the fact he’d been scammed.

Mr R complained to HSBC, but it refused to refund any of the money he’d lost. It advised him to contact the cryptocurrency exchange and provided advice on how to avoid scams in the future. It explained he wasn't entitled to a refund as the payments were made to an external account in his name and as he'd authenticated and authorised the payments, they were authorised card scam transactions.

It said its fraud detection systems highlighted the first payment, which Mr R confirmed was genuine, and this negated the need to follow up on further individual transactions. It also said the Contingent Reimbursement Model ("CRM") code didn't apply to card payments and he wasn't entitled to a refund under the Payment Service Regulations 2017 as he had authenticated and authorised the payments.

Mr R complained to this service with the assistance of a representative. He explained he wasn't an experienced investor and had believed the investment was genuine because he was asked to send ID, he had access to the trading portal and had carried out extensive research. He argued that HSBC failed to recognise the unusual activity on his account, and it should have provided relevant fraud warnings and asked appropriate questions which could have prevented his loss. He said he wanted it to refund the money he'd lost and pay him £500 compensation and legal costs.

Mr R's representative said HSBC should have intervened as Mr R made 14 payments to a new payee linked to cryptocurrency within the space of 8 months and this represented a missed opportunity to intervene to provide an effective warning.

The representative argued the payments were large amounts to new payees and Mr R made multiple payments in single days using funds from loans and other accounts which was clearly unusual as he primarily used the account for day-to-day payments, bill payments, direct debits and living expenses. In particular, on 6 September 2022, he sent £4,370.25 to the cryptocurrency exchange company, which should have alerted HSBC to the possibility of fraud. It should have contacted him and provided advice about the risk of scams, in response to which he would have sought to establish P was legitimate.

They said HSBC sent a text message when Mr R made the first payment. The message required to confirm the payment was genuine, after which he was able to make payments freely without any contact, effective pop-up notification or scam warnings. They argued that if it had asked him what the payments were for and the basic surrounding context, he would have fully explained what he was doing and that everything had originated from a broker. And even though he was sending money to a legitimate cryptocurrency exchange, it should have still provided a scam warning considering all the information known to banks about the increasing number of scams associated with cryptocurrency.

My provisional findings

I explained that the CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, in all but a limited number of circumstances. HSBC has had said the CRM code didn't apply in this case because the code doesn't apply to card payments, and I was satisfied that's fair.

I also thought about whether HSBC could have done more to recover Mr R'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. HSBC) 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 was satisfied that HSBC's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I was 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, Mr R is presumed liable for the loss in the first instance.

There's no dispute this was a scam, but although Mr R didn't intend his 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 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'd seen, the payments were made to genuine cryptocurrency exchange companies. However, HSBC 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 R 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 R from financial harm due to fraud.

The initial payment flagged on HSBC's systems, and he was required to confirm it was genuine before it was released. I considered the first payment in the context of whether it was unusual or uncharacteristic of how Mr R normally ran his account, and I didn't think it was. So, I didn't think HSBC needed to do anything else at that point.

The next five payments were for £4,370.25, £4,521.61, £4,375.22, £4347.45, and £2,273.92 and I considered whether they were unusual or uncharacteristic for the account. These payments were to legitimate cryptocurrency merchants, and they weren't made in quick succession. I accepted that in the period leading up to the payments, Mr R hadn't made any payments of similar value, but they weren't so large that HSBC needed to intervene based on value alone. However, I agreed with our investigator that it should have intervened on 11 November 2022 when Mr R paid £8,766.09 because this was a significant increase in spending which was unusual for the account.

I explained that HSBC should have contacted Mr R and asked some probing questions about the purpose of the payment including how he learned about the investment opportunity, whether there was a third party involved and if so, how he met them, whether he'd been told to download remote access software to his device, whether he'd been promised unrealistic returns and whether he'd been told to make an onwards payment from the cryptocurrency exchange.

I hadn't seen any evidence that Mr R was coached to lie and so if he'd been asked these questions, I thought it was likely he'd have told the call handler that he'd learned about P from someone he'd met online and that he'd been advised to make an onwards payment from the cryptocurrency exchange to a wallet address provided by the broker.

With this information I would expect HSBC to have identified the investment had the hallmarks of a scam and to have provided advice on additional due diligence and warned him that the investment had the hallmarks of a scam. There were no warnings about P on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites which would have alerted Mr R to the fact this was a scam. But I didn't think he would have gone ahead with the payment if he'd had any inkling that P was operating a scam.

HSBC had argued the fact he had engaged in another investment meant Mr R was willing to take risks and so a warning from HSBC wouldn't have made a difference. But Mr R had explained that the other investment had nothing to do with cryptocurrency and that he'd tried to trade by investing £2,500 before withdrawing the money, having made a very small profit. So, while I accepted Mr R had invested before, I didn't accept it was high risk and I didn't think it meant he'd have ignored a clear warning from HSBC that the investment was probably a scam.

Because of this, I thought HSBC missed an opportunity to intervene in circumstances when to do so might have prevented Mr R's loss, so I thought it should refund the money Mr R lost from the second payment he made on 11 November 2022 onwards.

Contributory negligence

I explained there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and I accepted Mr R was taking advice from someone he'd met online, which should reasonably have given him cause for concern. And the fact he had invested before meant he would have had some awareness of the risks involved in investing. However, I noted he wasn't promised unrealistic returns and he had explained that he checked P's website and social media pages and he saw positive reviews on Trustpilot. He also noted it was registered on Companies House with a registered office in London.

Our investigator felt it was unreasonable for Mr R to have gone ahead without some documentation from P, but I was satisfied the research he did was reasonable in the circumstances. He hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he thought he was engaged in a genuine friendship with the scammer and the fact the broker appeared to be knowledgeable about investing. So, whilst there may be cases where a reduction for contributory negligence is appropriate, I didn't think this was one of them.

Recovery

Because Mr R made the payments to an account in his own name before loading the cryptocurrency onto an online wallet, I didn't think there was a realistic prosect of a successful recovery.

Compensation

I wasn't persuaded Mr R was entitled to any compensation or legal costs from HSBC.

Developments

HSBC has made further comments in response to my provisional decision. It has said it would be willing to refund 50% from the seventh payment onwards but it maintains that if Mr R was under the spell of the scammer, a warning wouldn't have made a difference.

It has said that if Mr R had done basic searches he would have realised the investment was a scam. It has commented that he said he had carried out extensive research on P and that he recalls seeing it was registered on Companies House, with an address in London, but neither the scam company nor the version of the name referred to in Mr R's complaint letter were registered with Companies House. And a search of the scam company reveals a mobile number, which ought to have been a red flag.

It has explained that a third version of the company name was registered with Companies House, with a London address and a phone number which is consistent with a London address, but this company has no links to cryptocurrency or high-risk investments. Similarly, HSBC has argued that a search of the scam company would also have taken Mr R to P's social media page which didn't look professional and should have raised alarm bells.

It has also said that Mr R likely began researching the investment in May 2022, but at that time there would have only been one review. And he hasn't produced any evidence of the social media pages he's referred to, which might have supported that he'd done reasonable due diligence rather than simply following links provided to him by the scammer.

In further comments relating to the issue of contributory negligence, HSBC has said there's no evidence that Mr R wasn't promised unrealistic returns. It has argued that the available evidence is that the returns were too good to be true as the scammer said she was making good profits, which made the investment seem profitable. It has also argued that Mr R increased his investment from late October 2022, suggesting he was promised returns that were too good to be true.

It has further argued that in paying over £70,000 to the scam, Mr R displayed a lack of caution and that he carelessly increased his investment, paying £8,000, £16,000, and £13,000 in individual payments within a month, having received no tangible returns. It accepts Mr R's previous investment experience wasn't in cryptocurrency, but he was trading in CFDs, which is categorised as high risk. And even though he had built up what he thought was a genuine friendship with the scammer, he should have been concerned when the discussion changed to cryptocurrency.

Finally, it has argued that the payments Mr R made from 27 October 2022 were funded from his savings account, so the relevant rate of interest should be based on the rate of interest for that savings account and the award of 8% simple interest would be betterment.

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.

HSBC is suggesting that if Mr R had searched either of two versions of the name associated with the scam company, he would have discovered that neither were registered on Companies House and that this should have raised concerns. As should the fact the scam company had a mobile number and a social media page, neither of which would have seemed professional. Alternatively, if he'd searched the company that was registered on Companies House, he'd have seen it wasn't associated with cryptocurrency.

I've noted what HSBC has said about the results of searches Mr R might have done and while I accept that more thorough searches might have raised concerns, I'm satisfied he did what he understood to be reasonable due diligence. I would expect Mr R to have undertaken a google search to confirm P did exist, but I wouldn't necessarily expect this to have involved an analysis of the services it provided. And I accept the use of a mobile number would have been a red flag, but Mr R might not have noticed this or considered that the social media platform was unprofessional.

As I've previously noted, this was a sophisticated scam and I don't think it's unreasonable that he failed to differentiate between the various versions of the company name or not to have spotted red flags that are now obvious with the benefit of hindsight. So, while I accept Mr R's research wasn't as effective as it might have been, I don't think it means that he was negligent to the extent that he contributed to his own loss.

HSBC has pointed out that there was only one positive review about P at the time Mr R was likely to have checked Trustpilot, but there's no suggestion that he ignored negative reviews and I don't think it was unreasonable for him to have gone ahead with the investment having seen only one positive review.

It has also suggested that Mr R followed direct links provided to him by the scammer, but he's explained that he believed he had developed a genuine relationship with this person and in the circumstances I don't think it was unreasonable that he believed what he was told about the investment.

I said in my provisional decision that there was no evidence that Mr R was promised unrealistic returns, which is relevant to the issue of whether it was unreasonable for him to have believed what he was told by the scammer. But even if he was tempted by good profits, 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 broker in terms of the returns he was told were possible.

Similarly, I accept he made large payments to the scam, but I'm satisfied he did this in the belief that he's money was safe and that he was making significant profits which he could see on the trading platform, and in those circumstances I don't think he was negligent or that he could fairly be said to have contributed to this own loss.

Overall, I note the further comments that HSBC has made in support of its argument that the settlement should be reduced for contributory negligence, but I maintain my view that this was a sophisticated scam and Mr P had thought he was engaged in a genuine friendship with the scammer, so I don't think he contributed to his own loss.

Finally, HSBC has argued that the interest award should be based on the rate of interest for the savings account that Mr R used to fund the scam payments. But we normally award 8% simple interest per year to reflect the cost of being deprived of money and in the circumstances I'm not persuaded that it would be fair to use a different rate of interest.

My final decision

For the reasons I've outlined above, I'm minded to uphold this complaint and to direct HSBC Bank UK Plc to:

- refund the money Mr R the money he lost from 11 November 2022 (the seventh payment) onwards.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If HSBC Bank UK Plc deducts tax in relation to the interest element of this award it should provide Mr R with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr R to accept or reject my decision before 18 January 2024.

Carolyn Bonnell
Ombudsman