DRN-4515774

The complaint

Mr L complains that HSBC UK Bank Plc 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.

Mr L was looking to increase his income to pay off his mortgage and had heard colleagues discussing cryptocurrency. He had previously invested a small amount in traditional stocks and shares and had a basic knowledge of investing, so he did some research to gain a basic understanding of how cryptocurrency worked.

In November 2021, he opened an account with a cryptocurrency exchange company I'll refer to as "F" and on 5 November 2021 he paid £10 to it with no intervention from HSBC, followed by £450 on 29 December 2021.

Shortly afterwards, one of his colleagues recommended a social media account that he should follow which belonged to someone I'll refer to as "the scammer". The account provided live updates on the cryptocurrency market and included information on how different currencies were performing. The majority of the posts were based on trading and investing with the occasional personal post, so Mr L believed the scammer was an experienced cryptocurrency trader.

On 25 January 2022, Mr L responded to a post from the scammer and they began to communicate. The scammer told Mr L he would introduce him to a secret trading platform and sent him a link to a trading platform I'll refer to as "C". Mr L couldn't see any negative reviews about C and it was registered by the Financial Services in Antigua, with a company address in Florida. The website included a live-chat function, an about us section, FAQs, a 'contact us' page and a timeline showing how the company started. There was also a live market chart detailing the current trade prices, and Mr L could see it was endorsed by Bitcoin and Ethereum.

To sign up to the trading platform, Mr L had to provide his name, email address, and contact number. The scammer said he would have to buy cryptocurrency from F, before transferring the coins to a wallet on the trading platform. He explained he would guide him on how to trade, describing himself as a mentor. On 28 January 2022, Mr L made an initial payment of £300 and between 28 January 2022 and 30 March 2022 he made sixteen transfers to F totalling £35,650 from his HSBC account.

On 28 March 2022, Mr L decided to withdraw £100 from his trading account, but when he asked the scammer if he could withdraw more of his profits, he was told he would need to pay VAT. He eventually realised he'd been scammed when he still didn't receive his funds and he didn't receive a response from customer service.

Mr L complained to HSBC but it refused to refund any of the money he'd lost. It said he had access to the cryptocurrency account so it was unable to refund any of the payments and he should contact the cryptocurrency exchange as the money was lost from there. It explained its fraud detection system is based on current fraud trends, meaning not all payments will flag for additional checks, and customers should carry out their own due diligence by checking if investment companies are registered with the Financial Conduct Authority ("FCA") and seeking independent financial advice.

Mr L wasn't satisfied and so he complained to this service with the assistance of a representative. He said he received no contact from HSBC when he made the payments and he wanted it to refund the money he'd lost plus £500 compensation and any legal costs resulting from the scam.

His representative said the payments had the hallmarks of an investment scam and HSBC had missed several opportunities to intervene. They said the first payment should have been a red flag and that if HSBC had identified the payments as unusual and suspicious it would have realised Mr L was falling victim to an investment scam. They said he was transferring funds to a new payee linked to cryptocurrency and it should have asked relevant questions and advised him about the potential risks, which would have prevented him from making further payments.

HSBC confirmed there were no fraud warnings or calls because the payments didn't flag on its fraud system. It said Mr L had made payments to the payee before the scam so it would have been a trusted beneficiary at this stage.

Our investigator thought the complaint should be upheld. She was satisfied the payments Mr L made to the scam before 28 March 2022 weren't significant enough in value to have triggered an intervention. But even though F was an established payee, she thought the £7,800 payment he made on 28 March 2022 should've been blocked.

She accepted Mr L had paid out larger sums on 1 June 2021 (£4,700), 21 November 2021 (£17,878) and 27 January 2022 (£3,200), but she thought HSBC should have contacted him and asked probing questions about why he was sending such large amounts of money to a cryptocurrency merchant and had it done so, she was satisfied Mr L would have explained that he'd found a mentor on social media who had advised him to use a trading platform which was registered outside of the UK.

With this information she was satisfied HSBC would've realised there were red flags present and provided scam education which would have uncovered the scam. Because of this, she was satisfied that HSBC had failed to intervene in circumstances which could have prevented the scam and that it should refund the money Mr L had lost from 29 March 2022 onwards.

Our investigator also explained that Mr L had spoken to colleagues who had successfully traded in cryptocurrency and the scammer's social media page was recommended by someone who he knew and trusted. He was new to cryptocurrency and wouldn't have known it was important to use a platform that was registered with the FCA, so she didn't think he had contributed to his own loss. Finally, she recommended HSBC should pay Mr L £150 compensation for failing to protect him from financial harm.

HSBC has asked for the complaint to be reviewed by an Ombudsman. It has argued the payments weren't out of character as Mr L had made previous payments to F. And there were other payments of higher value, so in the context of the previous account activity, the transactions weren't remarkable and didn't warrant intervention. It has also said that even if it had intervened, Mr L would probably have proceeded with the payments as he was satisfied

that it was registered with the Financial Services in Antigua and he would have relied on his colleagues' experiences.

Finally, it has stated that if it is required to refund Mr L's losses, the settlement should be reduced by 50% for contributory negligence, arguing that he wasn't an inexperienced investor and he was probably promised returns that were too good to be true.

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 CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr L says he's fallen victim to, in all but a limited number of circumstances. But the code didn't apply in this case because Mr L was paying an account in his own name.

I'm satisfied Mr L '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 L 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'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 L 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 L from financial harm due to fraud.

The payments didn't flag as suspicious on HSBC's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr L normally ran his account and I agree with our investigator that the first ten payments weren't unusual or suspicious because Mr L was paying an established payee which was a legitimate merchant, and none of the payment were for particularly large amounts.

However, on 28 March 2022, Mr L made a payment of £7,800 to F and I agree that HSBC should have intervened at that point. This is because, even though F was an established payee that Mr L had paid on 12 previous occasions, the payment amount had increased significantly and by this time he'd paid over £19,000 to a cryptocurrency merchant in respect of which HSBC had never asked him any questions or provided any warnings. Significantly, in the previous November and December, he'd only paid £10 and £450 to F and the payments had increased in frequency and value from January to March.

I accept there were some higher value payments in the months before the scam, but the payment of £17,878 was to HMRC, and the other two payments were for a kitchen and were made nine months before the disputed payments, so I don't think the existence of those low-risk payments means the later scam payments weren't concerning.

For these reasons, I think HSBC should have contacted Mr L and asked him whether there was a third party involved and if so how he met them, whether he'd been advised to download remote access software to his device, whether he'd been allowed to make any withdrawals, whether he'd been promised unrealistic returns and whether he'd been advised to make an onwards payment from the cryptocurrency exchange.

There's no evidence Mr L had been coached to lie and so I'm satisfied he'd have told HSBC he was being advised by someone he'd met on social media who had told him to use a trading platform that wasn't registered in the UK and that he'd been advised to make an onwards payment to a wallet address provide to him by the scammer.

There were no warnings about C on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites, but I'm satisfied that HSBC would have had enough information to have identified that the investment was a scam and so it should have provided a very robust scam warning. It should also have told him there were red flags present suggesting the investment was a scam and provided advice on additional due diligence.

There's no evidence Mr L was keen to take risks with his money therefore I'm satisfied he'd have listened to this advice and done some more research which would have ultimately uncovered the scam. Because of this, I'm satisfied that HSBC's failure to intervene on 28 March 2022 represented a missed opportunity to have prevented Mr L's loss and so it should refund the money he lost from that point onwards.

Contributory negligence

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 L was to blame for the fact he didn't foresee the risk.

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 L to have believed what he was told by the scammer in terms of the returns he was told were possible. In any event, he has explained that he could see his money fluctuate with the trades the scammer was making on his behalf and that was told the more he invested, the larger the profits he would make, which I don't think is unreasonable.

Mr L was referred to the scammer's social media account by a colleague and he was satisfied it had a number of followers and appeared genuine. He was also satisfied the trading platform seemed genuine and professional and I don't think it was unreasonable for him to have believed C was regulated outside of the UK.

He has explained he had some very limited investment experience, but this was a sophisticated scam and he hadn't invested in cryptocurrency before, so I don't think he can fairly be held responsible for his own loss.

Compensation

Our investigator has recommended that HSBC should pay Mr L £150 compensation for the impact of its failure to protect him from the scam and in the circumstance I'm satisfied that's fair.

My final decision

My final decision is that HSBC UK Bank Plc should:

- refund the money Mr L lost from the first payment he made on 28 March 2022 onwards.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

- pay £150 compensation

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

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

Carolyn Bonnell
Ombudsman