DRN-5193755

The complaint

Mr M complains that HSBC UK Bank Plc ('HSBC') won't reimburse the funds he lost when he fell victim to a scam.

What happened

Mr M says that he was searching for a job when he received contact from someone who said he worked for a company I'll refer to as D. D was involved in marketing products. Mr M didn't know at the time, but this person was a scammer and D was impersonating a genuine company. The scammer offered Mr M a role which involved clicking on logos to complete sets of tasks. He would make a nominal amount for each click and if he completed tasks on consecutive days he would receive a salary.

The scammer instructed Mr M to open an account at a cryptocurrency exchange and gave him access to a platform where he could complete tasks. Mr M was also introduced to a group chat with others who were performing the role, and to a chat with D's customer services team.

Mr M began to receive 'combination tasks', which he says left his account with a negative balance which he was told he would need to clear to reset his account and complete further tasks. Each time this happened, Mr M sent money to his cryptocurrency account and transferred the USDT he bought to D's platform.

At the end of the first week, Mr M says that he could see on the platform that D had paid him his salary of 500 USDT - which he decided not to withdraw. In the second week Mr M received multiple combination tasks which became more and more expensive.

After making the final payment for a set of tasks, Mr M tried to withdraw his funds. He decided to split the payment in two in case anything went wrong in the transfer process. The withdrawal was refused, and Mr M says he was told that this was because he had made two transactions. Mr M was then required to pay a fee to withdraw his funds. He explained that he couldn't pay the amount requested and the scammer halved the figure. Mr M didn't make the payment and most of the contact he had with D ceased.

Mr M made payments to his cryptocurrency account between 4 January and 15 February 2024 which totalled over £11,000. He says he fell victim to a further scam just after this one, and lost more money. This second scam wasn't reported to HSBC, so it has not had the opportunity to investigate. This means that I am only considering Mr M's losses in the first scam involving D (up to 15 February 2024) in this decision.

Mr M reported the scam to HSBC on 16 February 2024. HSBC didn't agree to reimburse Mr M's loss. It said it wasn't liable for Mr M's loss because he transferred funds to an account in his own name. HSBC also said that after Mr M had made two transfers to the cryptocurrency exchange for £2 each it held a transfer of £2,000 to the same exchange and spoke to Mr M about it. During the call appropriate warnings were provided and the payment was reversed. Mr M's claim also wasn't covered by the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code).

Mr M was unhappy with HSBC's response and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in part. He said that HSBC didn't do enough when it called Mr M about the third payment he made (of £2,000 on 15 January 2024) but that Mr M should share responsibility for his loss with HSBC.

HSBC said that as a gesture of goodwill it would agree with his recommendation. Mr M didn't agree with the investigator's findings. He said that HSBC didn't do enough to protect him and should have had a better risk management system in place. Mr M also said that when HSBC called him, it failed to ask any questions about D and, instead, focused on the legitimate cryptocurrency exchange. HSBC also didn't provide relevant warnings.

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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

None of the transactions Mr M made are covered by the CRM Code. The CRM Code only applies to certain types of payment made to another person in pounds sterling, between accounts based in the U.K. In this case, Mr M wasn't transferring funds to another person but to an account in his own name.

Aside from the CRM Code, a bank still has wider obligations and a duty to protect its customers, as far as is reasonably possible, against the risk of financial harm from fraud and scams.

In broad terms, the starting position at law is that a bank such as HSBC is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

Taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that HSBC should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment; and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-

stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

In this case HSBC identified the first larger payment Mr M made (£2,000 on 15 January 2024) carried an increased risk and spoke to Mr M about it. I've listened to the call recording. Having done so, I consider that whilst the adviser covered some helpful points, he didn't go far enough to identify the scam Mr M was likely falling victim to, or to provide relevant warnings.

I think that when these payments took place HSBC should have taken steps to identify the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam. HSBC should have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving a victim's money across a range of different scam types, including 'romance', impersonation, and investment scams. So, HSBC should have identified which type of scam Mr M was most likely falling victim to.

The advisor Mr M spoke to on 15 January 2024 asked questions about Mr M's account with the cryptocurrency exchange, whether he had control of the account and whether he was making payments himself. Mr M was clear that the funds would be moved from the cryptocurrency exchange wallet to another platform, and also said he wasn't investing. The adviser didn't pick up on these points, or ask any questions about what the funds would be used for as I think he should have. The warnings that he then gave related to cryptocurrency being risky and to fake cryptocurrency accounts only. Mr M was also advised to try to withdraw funds from his wallet.

Having considered the details of the call I'm not satisfied the adviser asked appropriate questions to narrow down the likely scam risk and then provide warnings tailored to that risk.

In reaching my view that HSBC ought fairly and reasonably to have done more to protect Mr M, I consider HSBC ought to have been mindful of the potential risk to them of 'multi-stage' fraud – whereby victims are instructed to move funds through one or more legitimate accounts held in the customer's own name to a fraudster. The use of and risks to customers of multi-stage fraud were well known to banks by the time all the transactions I am considering were made.

Mr M says he was vulnerable at the time of the scam. As I have said above, the CRM Code doesn't apply in this case so I can't consider full reimbursement based on vulnerability, as set out in it. I can't see that Mr M made HSBC aware of any vulnerabilities or that he asked for any additional support before any of the payments were made. And I don't consider HSBC ought reasonably to have identified any vulnerabilities in its interactions with Mr M. So I can't fairly ask HSBC to reimburse Mr M on this basis.

I've gone on to consider whether intervention of the type I have set out above would have made a difference and prevented Mr M's further loss.

In his call with HSBC on 15 January 2024 Mr M answered the questions he was asked honestly. So I have no reason to believe that if HSBC had asked additional questions about how Mr M planned to use the cryptocurrency, he wouldn't have been open and honest and explained his role with D. By January 2024 task-based job scams should have been well-known to HSBC and its advisers should have been able to spot the hallmarks.

I'm also satisfied that Mr M would have accepted what HSBC, as the expert here, said and not made further payments relating to the job with D had it set out the essential features of a task-based job scam. In the call on 15 January 2024, when the HSBC adviser suggested that Mr M should try to withdraw funds from his cryptocurrency wallet, Mr M agreed that this was a good idea. He was happy for the payment to be reversed until he had done so. After this, Mr M made a small withdrawal which credited his HSBC account.

I appreciate that the £2,000 payment on 15 January 2024 wasn't made because of HSBC's interaction. But I consider that if HSBC had asked additional questions in respect of the ultimate destination of Mr M's funds, the scam would have been exposed and he wouldn't have made any further payments. In those circumstances, I am satisfied it is fair to hold HSBC partly responsible for Mr M's subsequent loss.

Should Mr M bear any responsibility for his losses from the £2,000 payment on 15 January 2024 onwards?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that there were relatively sophisticated aspects to this scam, not least a platform where Mr M was able to see his earnings. I note that Mr M also had access to a customer support team. I can imagine these features would have given some validation to the scheme.

But on balance, I consider a 50% deduction is fair and reasonable in all the circumstances of this case. The nature of the job was unusual and implausible, and I think this ought to have led Mr M to ask questions, complete some additional research and to look at reviews.

Mr M hasn't been able to provide the messages he exchanged with the individual from D who contacted him, but I have seen messages on the group chat that Mr M was added to. These said that he could earn 800 USDT for completing sets of tasks on five consecutive days. In addition to this the group discussed a 'deposit reward' and commission. Mr M has explained that the role involved clicking logos, so this is a significant amount for work that was not particularly time-consuming or arduous. And buying and transferring cryptocurrency to be paid is very unusual.

Although Mr M thought the initial contact from D related to his job search, he knew this wasn't the case before he made any payments, meaning that he received out of the blue contact about a lucrative opportunity. And Mr M wasn't given anything in writing to set out the terms of his agreement with D. I appreciate he says he thought it was more like a friend introducing him to an opportunity to get a passive income, but I don't agree.

When asked what research he completed before taking on the role, Mr M said that he used the link the scammer provided to D's website and asked questions about how he would be paid and how the model worked. I think it would have been reasonable to complete some independent research into D. When Mr M did so later, he found the website of a legitimate company with the same name as D. The genuine company displayed a prominent warning about the scam Mr M fell victim to.

Overall, I consider it fair to reduce the amount HSBC pays Mr M to reflect the role he played in what happened.

My final decision

For the reasons set out above, I uphold this complaint and require HSBC UK Bank Plc to:

- Reimburse Mr M 50% of all scam payments made from 15 January 2024 to 15 February 2024; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of each transaction to the date of settlement.

If HSBC UK Bank Plc is legally required to deduct tax from the interest, it should send Mr M a tax deduction certificate so he can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 25 April 2025.

Jay Hadfield
Ombudsman